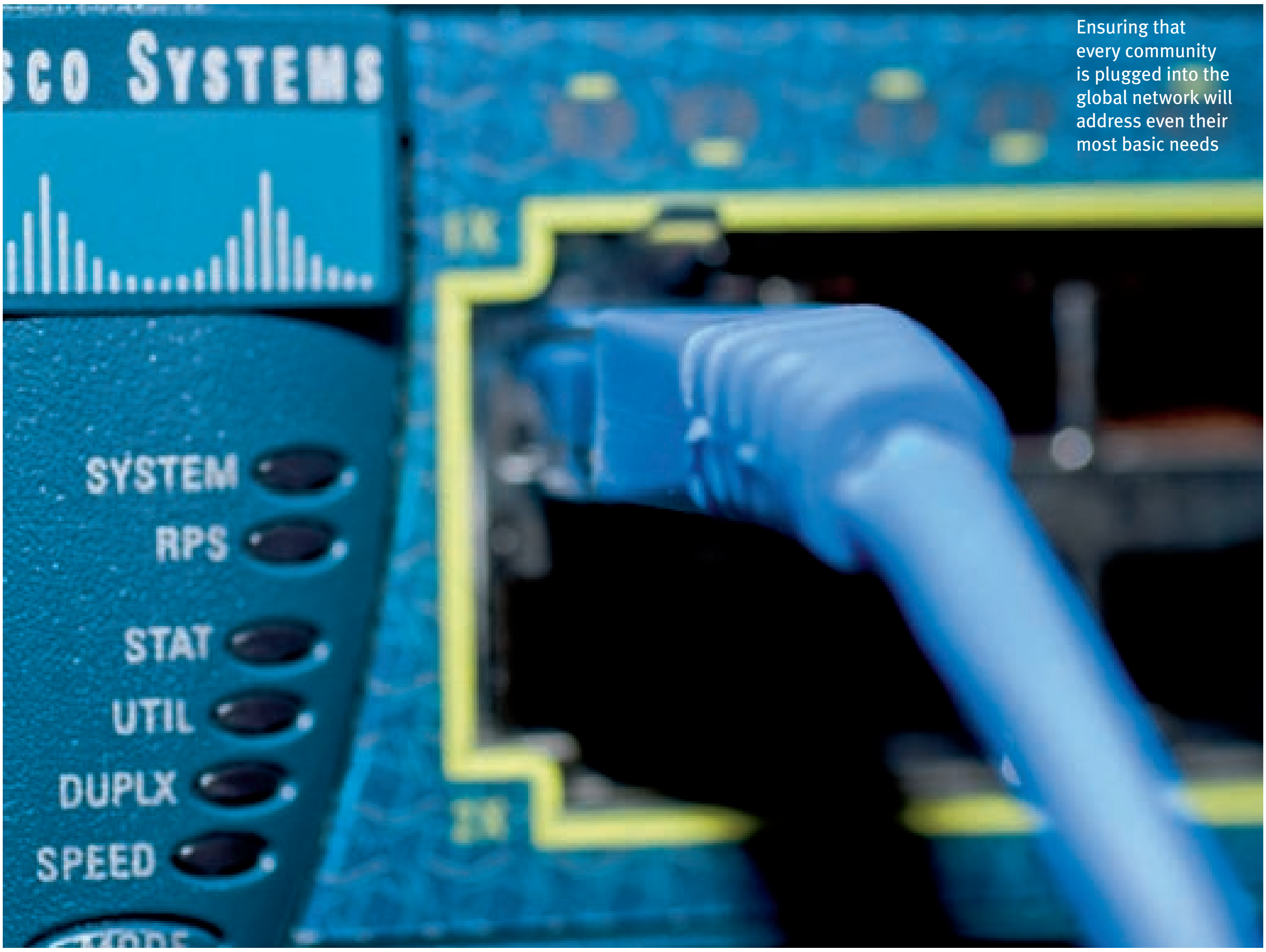


Ensuring that every community is plugged into the global network will address even their most basic needs

Positive change through better connections

The power of information and communication technologies to influence daily lives goes far beyond simply staying in touch via mobile phones or social networks. Such innovations can improve access to essential needs for developing countries

By Hamadoun Touré, secretary general, International Telecommunication Union

Today, in a world of seven billion people, current projections from the United Nations suggest that the global population will continue to grow, peaking some time mid-century at around nine or 10 billion. The Cannes Summit is, therefore, a good opportunity to look at how to address the most pressing issues facing humanity over the coming decades.

It is clear that to meet the needs of all the world's people – for adequate food and water, for healthcare and for education, to name just some of the basic essentials – the power of information and communication technologies (ICTs) must be leveraged.

There are two reasons to remain optimistic that it will be possible to do this – and to create a smarter, more equitable and more sustainable world.

First, the one inexhaustible resource in the world is human ingenuity. Over millennia, humans have been able to address and resolve complex issues because that is the way they are as a species: very good at problem-solving – which is just as well, given the problems that have needed to be solved in the past and will continue to do so in the

Students learn how to use computers aboard a ship converted into a classroom in Colombia. ICTs can connect communities in the developing world to a new wealth of knowledge

future. And, second, because ICTs by their very nature are one of the best breeding grounds for innovation.

Over the past two decades, there has been an extraordinary proliferation of ICTs in almost every domain of human endeavour. Today there are almost six billion mobile cellular subscribers and more than two billion people are already online. Everything that happens is now directly linked to – and by – ICTs.

Indeed, one thing is certain: ICTs will continue to proliferate – and I suspect that recent forecasts from Cisco and Ericsson, which predict 50 billion connected devices by 2020, may in fact be underestimates.

Thus, there is every opportunity to leverage the power of these ubiquitous ICTs to serve the needs of humanity through the 21st century, and to bring the social and economic benefits of ICTs to all the world's people, wherever they live and whatever their circumstances. Indeed, ICTs represent not just the single most powerful channel to reach out to others, but perhaps the only way to address the most pressing issues of the day – including accelerating progress towards meeting the Millennium Development Goals (MDGs).

Technology to tackle hunger

The innovative use of ICTs will be crucial in ensuring that the world's billions have affordable, equitable access to adequate food supplies, at every step of the process – from delivering the right information to farmers to help them improve yields and prices to improving supply-chain efficiencies, to ensuring that consumers understand nutritional needs, both for themselves and their children.

Similar principles apply to smart water management and distribution. Here, too, ICTs will play a vital role, as water resources become more scarce and much more valuable. Technologies such as the semantic sensor web, remote sensing with satellites and geographical information systems can be used innovatively by water authorities to obtain information in real time about water use, to track and forecast the level of rivers, and to identify new sources of fresh water.

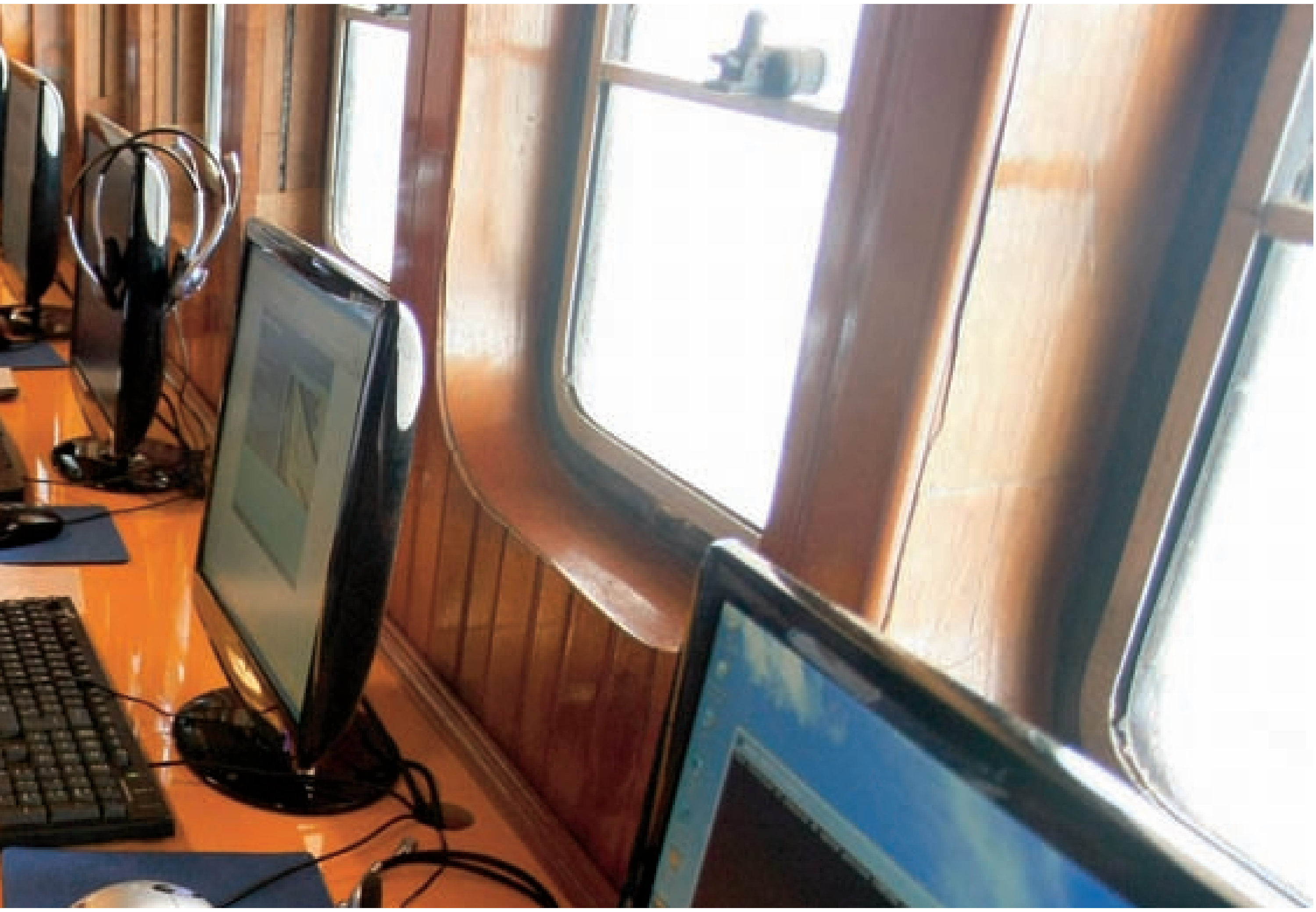
Monitoring the environment

ICTs allow water stakeholders to obtain information almost instantly about a number of physical and environmental variables – including temperature, soil moisture levels and rainfall – through web-enabled sensors and communication networks. This ability makes accurate information about the situation available (without the need to be physically present) for making forecasts and reaching decisions.

Smart metering technologies can also provide individuals, businesses and water companies with near real-time information about their own water use, thus raising awareness about usage, locating leakages and having better control over water demand.

Innovation combined with ICTs will also transform healthcare and education globally – in the developed world, as well as the developing world.

Already, mobile phones play a key role in healthcare in a growing number of countries in sub-Saharan Africa, Asia-Pacific and Latin America, where they deliver simple SMS reminders for vaccinations or antiretroviral treatments and gather grassroots information on demographics and diseases – not to mention serve as mobile information repositories for personal health records. New applications are being developed in the



thousands to help deliver healthcare to those who cannot be easily reached by medical specialists.

More advanced applications, such as 3D computer tomography, will soon allow for non-invasive internal examinations and diagnosis. Advanced data mining will allow rare and unusual medical conditions to be diagnosed and treated more quickly and effectively.

Advances in learning

In education, ICTs are already one of the main platforms for disseminating knowledge. This is perhaps the biggest shift in education since the founding of the first great higher-learning institutions, which depended on the model of 'lecturer' and 'lectured to'.

ICTs have brought two new forces to play: the death of distance and the democratisation of information and knowledge. As a result, distance learning has proliferated – so much so that the world's biggest universities are now the Indira Gandhi National Open University in New Delhi, India, which has three million enrolled students, and the Allama Iqbal Open University in Islamabad, Pakistan, which has 1.8 million students.

Through various projects around the world, including the 'Connect a School, Connect a Community' initiative of the International Telecommunication Union (ITU), computers and the internet are being brought both to those of school age and within the community as a whole for the first time. Children introduced at a young age to the vast realm of knowledge that the internet offers will stay connected as they grow.

Better-educated adults not only have families of more manageable size, but their children also have significantly improved survival rates, as well as better chances of an education, basic healthcare and stable, better-paid employment. Even simple devices like an ordinary mobile phone can have a profoundly transformational effect.

> “The innovative use of ICTs will be crucial to ensuring the world's billions have affordable and equitable access to food supplies”

Creating a sustainable world

ICTs will be critical in helping to create a more sustainable world in the 21st century. Smart grids, environmental sensors, intelligent transport systems, dematerialisation and digitalisation of goods and services, and new ways of improving energy efficiency will drive the transition to a low-carbon economy, while facilitating adaptation to the effects of climate change.

With political will, a strong social conscience and a profound desire to fulfil a humanist mandate, everyone is fully capable of making the world a better place for all. I am absolutely confident that together, by leveraging the power of ICTs and innovation, we shall do so. ◆

SPONSORED FEATURE

Mobile security: the foundation of new economic development

Research In Motion® (RIM) focuses on designing secure and efficient solutions for enterprises and consumers. BlackBerry® smartphones are available through 565 carriers in over 175 countries and there are 50 million BlackBerry smartphone users. A global presence this large requires that BlackBerry products and solutions are developed with insight into how the value of secure online communications can be achieved and applied across old and new world markets.

The topic of cyber security is predominant in discussions of the worldwide growth of mobile data and communications for consumers and enterprises. Cyber security means securing networks from all attacks, malicious or otherwise. This is best done within organisations through the application of a standard cyber-security policy that both establishes governance of issue resolution and enhances the safety of an organisation, its partners, and its customers through the timely and appropriate notification of security vulnerabilities, thereby minimising the risk of exposure and possible exploitation and maintaining valuable brand credibility. The term that signifies the cumulative measures that individuals and organisations take to protect their network assets (personal computers, mobile phones, servers, and so on) is cyber defence. To understand the impact of cyber security and cyber defence in the global conversation, the progress of ecommerce in all aspects of global economies, and the concerns of everyday citizens and governments alike, we must understand the value of security in mobile communications.

Mobile tools can foster economic growth and stability

Communications today have reached unprecedented levels with information that is readily accessible in electronic forms and that can be easily transferred, duplicated and shared. Smartphones, portable computers and tablets are increasingly being used by people to access the internet, and particularly in emerging or developing economies, providing the sole connection to the internet.

As the G20 addresses the financial crisis and the need for growth of agricultural sectors, the new growth in mobile technology has put unprecedented access to information in the hands of independent business people, including farmers. The G20 proposal of a database providing access to comprehensive, reliable and regularly updated information for agricultural markets can be more fully realised with securely managed smartphones and tablets running applications that connect to such a database.

With up-to-date information right at their fingertips, the appropriate people can receive proactive wireless notification about evolving situations, verify issues with colleagues, and take action quickly. Mobile communications technology, provided with the right level of data security, enables a previously unforeseen potential to ensure safety and quality and simultaneously protect government and public interests. For example, a BlackBerry application developed for LILA Asturias in Spain allows dairy farmers real-time access to LILA's complete analysis of variables in dairy samples.The security of documents sent and received on BlackBerry smartphones is recognised under the UNE-ISO 17025 standard and fulfills LILA's certification requirements. This validation of the BlackBerry solution allows all stakeholders to benefit from increased quality and efficiency, and hence profitability. For more information, see uk.blackberry.com/newsroom/success/LILA-Asturias-(UK).pdf

The economic dependency of G20 members on communication infrastructures will be shared more and more by developing countries. Globally, people from all walks of life are communicating, buying and selling on mobile devices as part of their daily lives, and the need is stronger than ever for any device or system that transmits data to protect confidentiality in both fixed and mobile environments. Small and large businesses and public-sector organisations alike need to keep their own product-related data private but are also responsible for protecting personal information that they store about customers, partners and employees.

> **People from all walks of life are communicating, buying and selling on mobile devices, and any device that transmits data must protect confidentiality**

The value of security

Individuals and organisations can employ a variety of solutions, including antivirus software, firewalls and encryption, to help protect personal information on desktop platforms. Making these tools available to mobile platform users is a fundamental part of protecting their privacy and earning their trust. To meet the public demand for secure personal and business information, communication solutions need to provide built-in security features that allow users to manage their privacy protection easily and consciously.

Security should enhance consumers' choices and be a market differentiator. Consumers must be educated to select solutions that best meet their communications and security needs, and that limit their total cost of owning and configuring a mobile device by providing security features that are both inherent and usable. For example, on BlackBerry® smartphones, a free mobile application for consumers called BlackBerry® Protect allows customers to remotely back up, restore, and locate their BlackBerry smartphones from wherever they are via their computer. Vendors must develop products with security features and technology that appeal to consumers and offer them security at no additional cost, freeing them to focus on their personal and business endeavours.

Securing the information that people store on their smartphones is a fundamental part of protecting their privacy. The security of a mobile platform should also allow organisations to extend their own data and systems to mobile applications. Mobile business solutions for the public sector must protect information but allow mobile personnel wireless access to case files and associated records, emergency operating procedures, alert notifications, timely analysis and reports – all at the point of need.

Conclusion

Security certifications assure people and organisations that the technology they choose is trusted and suitable for use by some of the most security-conscious organisations in the world. The assurance that the information of a business, however large or small, established or entrepreneurial, is secure is an essential cornerstone in developing trust and confidence in the online economy and its established and emerging brands. As citizens merge their private and business lives on their mobile devices, this principle becomes essential to their safety and livelihood.

It is challenging for private citizens to independently verify the security of the mobile technologies they use. To confidently measure and evaluate a mobile solution's security model, many individuals and organisations – including governments and military organisations – look to trusted third parties that have independently verified and certified a technology for use. Vendors that work to certify their mobile solutions through trusted validation programmes provide assurance to governments and consumers.

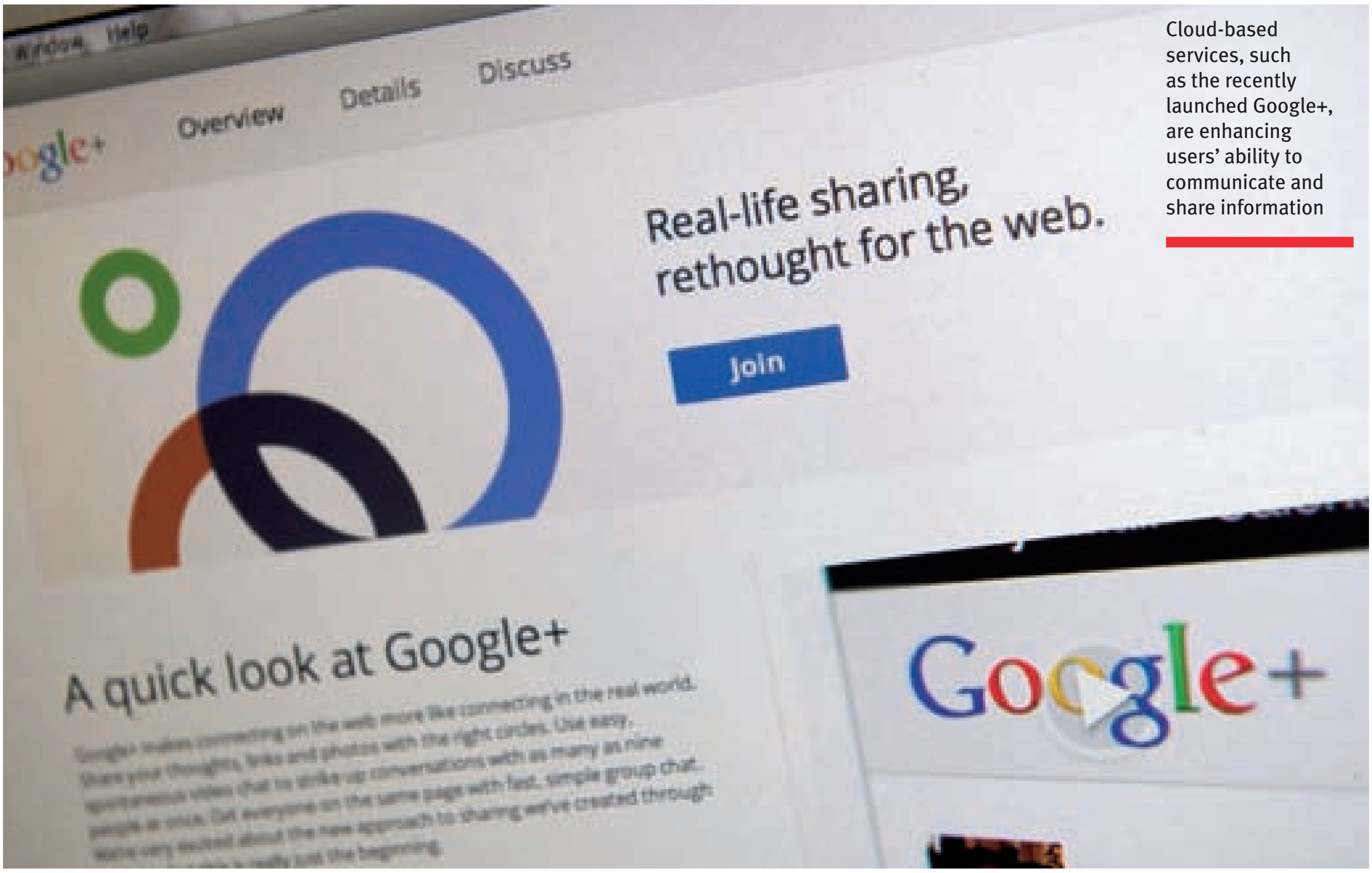
About BlackBerry security

RIM has long been a leader in mobile communications and has a history of integrating security features into its products. The company firmly believes that security technologies are an important foundation for a digital economy and for the protection of governments and citizens. BlackBerry products and solutions have received more security accreditations globally than any other wireless solution. The BlackBerry solution has been approved for level EAL 4+ of the Common Criteria for Information Technology Security Evaluation (CC), the highest level attained by any mobile internet solution designed for civilian use. The BlackBerry® PlayBook™ is the first tablet approved under the FIPS (Federal Information Processing Standard) certification from the National Institute of Standards and Technology (NIST) for use within the United States federal government.

Built-in security features in BlackBerry products include the use of encryption technology and security features to protect stored data and allow individuals to use these same privacy protections for their personal data and the information they choose to allow applications to access. If a device is lost or stolen, encrypted data cannot be read by an unauthorised person. Application controls prevent malware from accessing sensitive personal information. The BlackBerry Enterprise Solution also includes policy controls designed to give organisations the ability to balance individual and enterprise use of BlackBerry smartphones.

BlackBerry®

www.blackberry.com/security



Cloud-based services, such as the recently launched Google+, are enhancing users' ability to communicate and share information

Questions of trust as we head into the 'cloud'

As growing numbers of internet users migrate their data from their own devices to the servers of 'cloud-computing' providers, issues of policing, privacy and human rights are coming to the fore, not least in states where democracy is lacking

By Ronald Deibert, director, Canada Centre for Global Security Studies, Citizen Lab, Munk School of Global Affairs, University of Toronto

Though barely noticeable, a major tectonic shift has happened in global communications. Data previously stored only on desktops, on hard drives and in filing cabinets has evaporated into the 'clouds'.

'Cloud computing' refers to the delivery of software and other services as a utility over computer networks. But the cloud has become a metaphor for the way today's digital lives have been dispersed into a globally distributed mist.

Whereas, before, the internet was a self-segmented network distinct from other means of communication, such as television, telephony and radio, all these media have become integrated into a single system of planetary communications called cyberspace. This has happened at the same time as business models and service-delivery mechanisms for information and communications have changed fundamentally, with the rise of social networking, mobile connectivity and cloud computing (referred to together here as the 'cloud').

For large organisations, such as businesses and governments, the cloud provides a major cost-cutting solution. For individuals, it is convenient, reliable and fun. For the companies that support the cloud and the various products, services and devices that connect to it, it is an attractive source of growing revenue and innovation.

But there are dark sides. The shift to the cloud represents a paradigm shift in communications, which has upset the principles, norms and rules of what used to be just the internet. Under the internet's operating paradigm, the companies that ran the infrastructure took a 'hands-off' approach to the content that flowed through their networks, a principle known as 'network neutrality'. Today, data is entrusted to vast transnational information

empires – such as Google, Facebook and Amazon – that act as gatekeepers of what gets communicated and what is accessible. Market considerations can easily outweigh privacy and other rights concerns.

The rapid shift to an entirely new ecosystem has also opened up unforeseen insecurities that are systematically harvested by opportunistic actors, including criminals, unethical businesses, and military and intelligence agencies. Whereas at one time people's data was only as secure as they could protect it behind closed doors in their offices and filing cabinets, today it is only as secure as the companies that host it. In principle, entrusting data to third parties should actually enhance security because security is delegated to professionals that should have the ability to keep up with the latest threats. But studies have shown that cloud-computing companies are far less concerned with security than the bottom line. Some spend less than 10 per cent of their information technology resources on security.

Not surprisingly, there has been a growing rash of major security breaches across governments and the private sector. According to Privacy Rights Clearinghouse, nearly 600 million records have been breached due to the roughly 2,670 data breaches made public since 2005, in the United States alone. Included among these was the breach of Epsilon systems, resulting in a loss of more than 60 million email addresses from more than 50 companies. A breach of Sony servers in April 2011 resulted in the exposure of the private data of more than 100 million people. Major US defence contractors have also now admitted to persistent breaches and attacks.

Although many of these breaches appear to be mostly opportunistic hacks by anti-authoritarian groups intending to wreak havoc against 'the system', a growing number have sophisticated political and economic motivations. Research by Citizen Lab and the SecDev Group has uncovered cloud-based espionage networks emanating from Chinese, Iranian, Syrian, Burmese and other national jurisdictions pursuing numerous high-profile government, military, political, opposition and human-rights targets across Asia, Europe and North America.

One overarching characteristic is that the trade craft employed by the perpetrators is usually indistinguishable from that used in the ecosystem of cybercrime. As cyberspace becomes an object of geopolitical contests and a political battlefield among authoritarian regimes and their adversaries, clouds will become vectors for cyber-espionage and politically motivated attacks.

> As cyberspace becomes an object of geopolitical contests, clouds will become vectors for cyber-espionage and politically motivated attacks

Transcending jurisdictions

The shift to the cloud has also created new governance issues. While the notion of the cloud may seem ephemeral and be experienced by users as a virtual mirage, the infrastructure in which it is embedded involves a complex material, logistical and regulatory infrastructure that can span multiple political jurisdictions, from the local to the national to the international. While the text, the image and the video all may still seem within our immediate grasp, on our desktops and handheld devices, they are not. Data that we handle – that we assume is in our possession – is transported in an instant over cables and through radio waves from arrays of servers, many of which are far away in another political jurisdiction. And almost all of it is owned and operated by the private sector.

Governments looking to control cyberspace must therefore enlist the private sector that owns and operates the cloud to 'police the internet', through laws, regulations, incentives or other types of pressures. For example, in Canada, the government has introduced a crime bill that would require internet service providers (ISPs) and telecoms companies to retain user data, process the data for law enforcement and intelligence consumption, and share it with law enforcement representatives – all without judicial oversight. Such arrangements are not uncommon. Telecom carriers and ISPs not only facilitate access to information for law enforcement, but also actually derive revenues from doing so, and there is extensive variation among them on how exactly they go about doing so. As a result, citizens using different communications services can live in entirely different universes of rights.

The downloading of policing functions to the private sector – a phenomenon known as 'intermediary liability' – extends to the protection of intellectual property. It is considered standard practice for large carriers to 'clean their pipes' of malicious networks and traffic associated with file sharing or other activities deemed copyright-infringing. In the United States, several ISPs and carriers have already taken on this responsibility as a voluntary arrangement. The bottom line of business now demands it.

Manipulation by non-democratic states

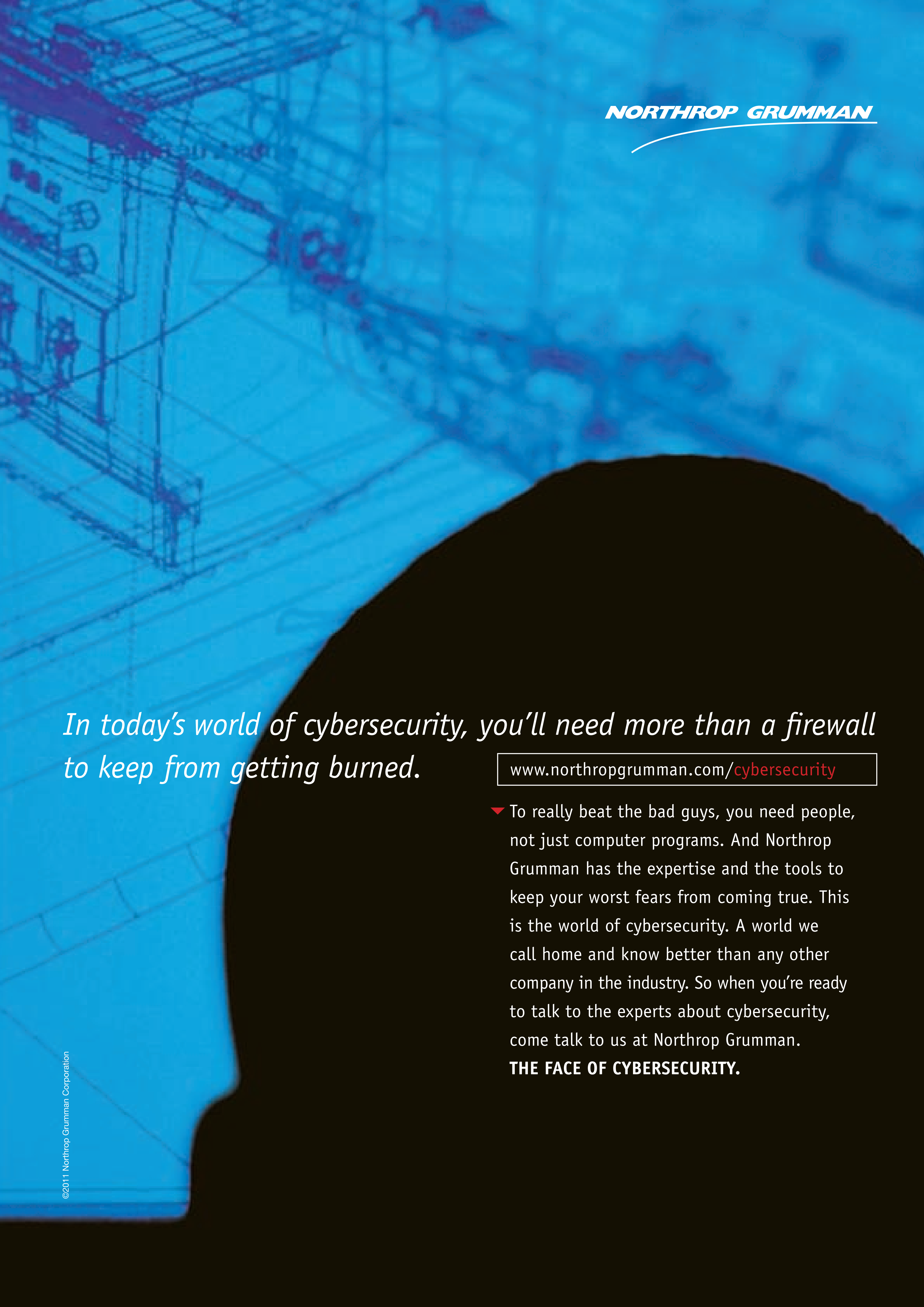
Of course, what is considered intermediary liability or a market imperative in Canada and the United States differs quite fundamentally from the situation in Belarus, Iran, Vietnam or China. In non-democratic countries, ISPs, telecom carriers and mobile operators are asked to police political content, track dissidents, identify protestors, send threatening messages over their networks and disable certain protocols used by adversaries – as part of the next-generation controls emerging in cyberspace. During the Arab Spring, for example, the Egyptian government forced ISPs to shutter the internet and required the country's main mobile phone operator, Vodafone, to send mass text messages encouraging pro-regime sympathisers to take to the streets to counter the protestors.

Citizens can find themselves hamstrung in jurisdictional confusion. When the US-based son of an Iranian activist, arrested presumably after his cell phone records were turned over to Iranian authorities by his provider, filed a lawsuit against Nokia-Siemens in an American court, the company argued that it was the wrong case in the wrong jurisdiction, and that it was merely following local law. The suit was eventually withdrawn.

In Canada, the Rogers Yahoo! internet privacy policy states that "personal information collected for the Internet Service may be stored and processed in Canada, the United States or other countries and may be subject to the legal jurisdiction of these countries". Users might well ask which countries and whose laws. As people's data evaporates into the clouds, so seemingly do their rights.

The trend towards the clouds may be irreversible, but its direction can be shaped in ways that mitigate some of its more serious dark sides. The private sector that owns and operates the clouds should be required to spend as much, if not more, effort protecting users' privacy and data as it does policing the internet for law-enforcement and intelligence agencies and copyright holders. If market forces are not enough, data-breach and privacy-by-design laws should be introduced, both domestically and through global cyber-security forums. Civil-society networks, including university researchers, play an important role as well, monitoring the private sector, uncovering and exposing security flaws and other forms of corporate negligence, and educating users on best practices.

More broadly, there needs to be a reinvigorated discussion of what public transparency and accountability mean as data levitates to the clouds and private authority in cyberspace becomes the norm. There is an urgent need to strengthen the protections against when data can be shared with third parties without users' knowledge or permission. Private forms of authority should be subject to the same type of rigorous checks and balances as is public authority, especially as their operations can span political borders where rights protections diminish. Until such time, dark clouds will continue to grow more ominous on the horizon, threatening to diminish human rights. ◆



Building international cooperation in cyberspace

The speed with which information technologies are shaping the modern world has left governments, industry and individuals exposed to fast-evolving cyber-threats. Countries should come together to ensure a safe and secure online environment

By John Lyons, chief executive, International Cyber Security Protection Alliance

Cyber-crime in all its facets is rapidly coming to define the 21st century. Whether it is Anonymous and its hacktivist friends taking down another website, financially motivated cyber-criminals stealing banking data or state-sponsored hackers pilfering intellectual property, such behaviour is now sadly the rule and not the exception.

But it should not come as a surprise when the latest cyber-attacks are played out in the daily paper or online news. During the Industrial Revolution, the world experienced tremendous innovation – a monumental upheaval in human life, powered by machinery. From that revolution sprang modern shipping and the rail industries, followed later by the automotive and aircraft industries, all growing and developing at a much more genteel pace than today's information revolution. That pace allowed for supporting infrastructure to grow and for people to become accustomed to such innovations. There was time to educate the public and train those who wanted to work in these developing industries.

Even with slow evolution and gentle maturation, many major accidents and incidents claimed lives. Legislation and regulation – or the threat of such – were needed along the way to improve safety and security. Seatbelts had to become compulsory in cars and manufacturers had to introduce quality assurance and certification for their products before they could be fitted and used in vehicles.

It should come as no surprise, then, that the rapid, chaotic acceleration of the information technologies of today has left governments, citizens and business caught on the back foot. Without the time to develop at a more sedate pace, the result is dangerous gaps in several areas, gaps that have been greedily exploited by what can be broadly termed cyber-criminals. Now is a good time to pause, therefore, and rethink what structures are needed to safeguard businesses, citizens and their governments in this very fast-moving, internet-enabled age of communication and technological advance.

> At a time of economic austerity and uncertainty, governments need assistance to develop a toolkit of best practices

Urgent need for global cooperation

Governments, of course, should continue to look within their own borders to tackle cyber-crime and to introduce measures to protect their critical national infrastructures. But it is also imperative that they start looking outwards at greater cooperation on a legislative and regulatory basis. A welcome development has been the two-day International Cyber Conference, hosted by the UK's Foreign and Commonwealth Office on 1 November, in order for governments, international organisations, non-governmental organisations and businesses to discuss cooperation across sectors and geographical boundaries. Five streams formed the agenda: economic growth and development, the social benefits of the internet, international security, cyber-crime, and safe and reliable access.

A new era of connectivity

When it comes to international security and cyber-crime, the Cold War days of mutually assured destruction are over. Everyone lives and works in an incredibly interconnected world – one look at the global financial crisis and how it reverberated with frightening speed across the planet reveals just how interconnected people are. Indeed, the successes of the Arab Spring might not have occurred had it not been for the ability of citizens to support one another online and through social media.

Those suggesting that western countries need to up their offensive cyber-war capabilities should tread carefully. In the physical world, air strikes can be carried out with a minimum of collateral damage – unmanned airborne raids in Afghanistan are carefully engineered to limit civilian casualties. However, this degree of surgical precision cannot be possible with any degree of confidence in cyberspace.

An act of cyber-war against a government department could well cause significant damage to non-related vital services. A denial-of-service or similar attack may, in a worst-case scenario, take out related healthcare or other networks that are plugged into the same backbone. Jeopardising the safety of innocent civilians and harming a country's growth and prosperity in a way that is disproportionate to the transgression that began the exchange is dangerous, given the globalised and interdependent nature of world economies.

At a time of economic austerity and uncertainty, governments – especially those in developing countries – more than ever need assistance to develop a toolkit of best practices. But this needs to go further and aim for international harmonisation of legislation and regulation, while providing the law-enforcement agencies tackling cyber-crime with the capability and capacity they badly need. This work is of paramount importance to build a more safe and secure internet-engaged global marketplace – not by regulating content, but by addressing specifically internet crime and security threats and risks.

Whether they are cyber-intrusions or cyber-attacks by 'botnets', carried out by rogue elements or government-sponsored hackers, cyber-attacks could ultimately lead to trade sanctions against a country that permits or, indeed, sponsors them, not to mention damage to its economy. Everybody would lose. This requires attention at senior

Inside the Global Response Centre of the International Multilateral Partnership Against Cyber Threats, based in Malaysia. Joint international efforts are necessary to fight cyber-attacks

governmental level, even by officials who would rather keep their collective political heads in the sand.

Russia and China, in particular, must be part of this debate. Both are prolific actors in cyberspace and on the world stage, and are thus fundamental to progress towards a safe and secure internet. There is little point in the Chinese government heralding its stand against spam email originating within its borders without acknowledging the threat posed by the groups operating there that attack other states. The same could be said about organised criminals within Russia. This type of state-endorsed cyber-crime damages these countries' standing on the world stage, harms their economic stability, and strains diplomatic and economic ties.

An inclusive approach

These countries must be part of the solution. The G20 Cannes Summit represents a wonderful opportunity to build upon the work of the UK conference and on the important work of other intergovernmental groups. This includes the Commonwealth Secretariat's proposal on cyber-crime, currently being considered by the Commonwealth heads of government.

Agreements are needed on how to proceed into a new era of political cooperation on the internet. Financing is necessary, of course, but difficult decisions must not be ducked because of a lack of investment. The world's citizens and businesses deserve to know that governments enable and support the sustainable economic development presented by the internet and by the huge innovation now possible by mobile smart devices. Some of the poorest countries can skip the significant infrastructure expense of fixed-line communications and jump straight to a mobile environment that can deliver new prosperity to those who are most in need.

At a fundamental level, governments around the globe must take the lead in ensuring that the security of today's communications and technology revolution is safeguarded for everyone. There has been much progress since the Industrial Revolution, but leaders must look to the future if this new revolution – of a very different kind – is not to spiral out of control into lawlessness and mutual distrust. ◆

Advancing international cybersecurity through strategy and partnership

Scott Charney
Corporate Vice President,
Trustworthy Computing,
Microsoft

Cyberattack joins terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts nation-states at risk. To be clear, there are risks to cyberspace other than those related to security; for example, the increasing number of machines and applications creates a very complex environment with challenging reliability issues, and nations' increased dependence on information technology makes the availability of systems a national and international imperative.

National governments confront many challenges in cyberspace. These include:

- Reliance on interdependent, interconnected global networks;
- The misuse of information technologies to enable extremists to engage in acts of violence;
- The ability of any individual to employ cyber tools to perpetrate actions that in the physical world would normally be limited to nation-states (such as espionage and other significant attacks that, if conducted by a nation-state, could be considered acts of warfare); and
- The ability of any nation, regardless of traditional measures of sophistication, to gain economic and military advantage through cyber programmes.

In addition to these challenges, the internet citizen – the individual who uses cyberspace for social and commercial interactions – is critically relevant to any solution. Unsecured computers can turn everyday users into a launch platform for attacks, and user fear about online security and availability can have sweeping economic consequences. Trust in cyberspace, on the other hand, can create new opportunities, markets and possibilities.

Nations must plan, organise and act accordingly to develop national cyberspace security strategies that can address these challenges. Historically, national security strategies have been characterised by their employment of all elements of national power – economic, diplomatic, law enforcement, military and intelligence. Comprehensive cyberspace security strategies must include these elements and articulate how they will be employed to ensure national security and public safety, ensure economic prosperity, and assure delivery of critical services to the public. Such strategies must also recognise the ever-mounting importance of economic security. In the industrial age, power was generally based on physical might; in the information age, power is derived from information, knowledge and communications.

Articulating and advancing a clear understanding of *norms, attribution,* and *deterrence* in the context of cybersecurity can dramatically improve the national and international cyberspace ecosystem.

Norms

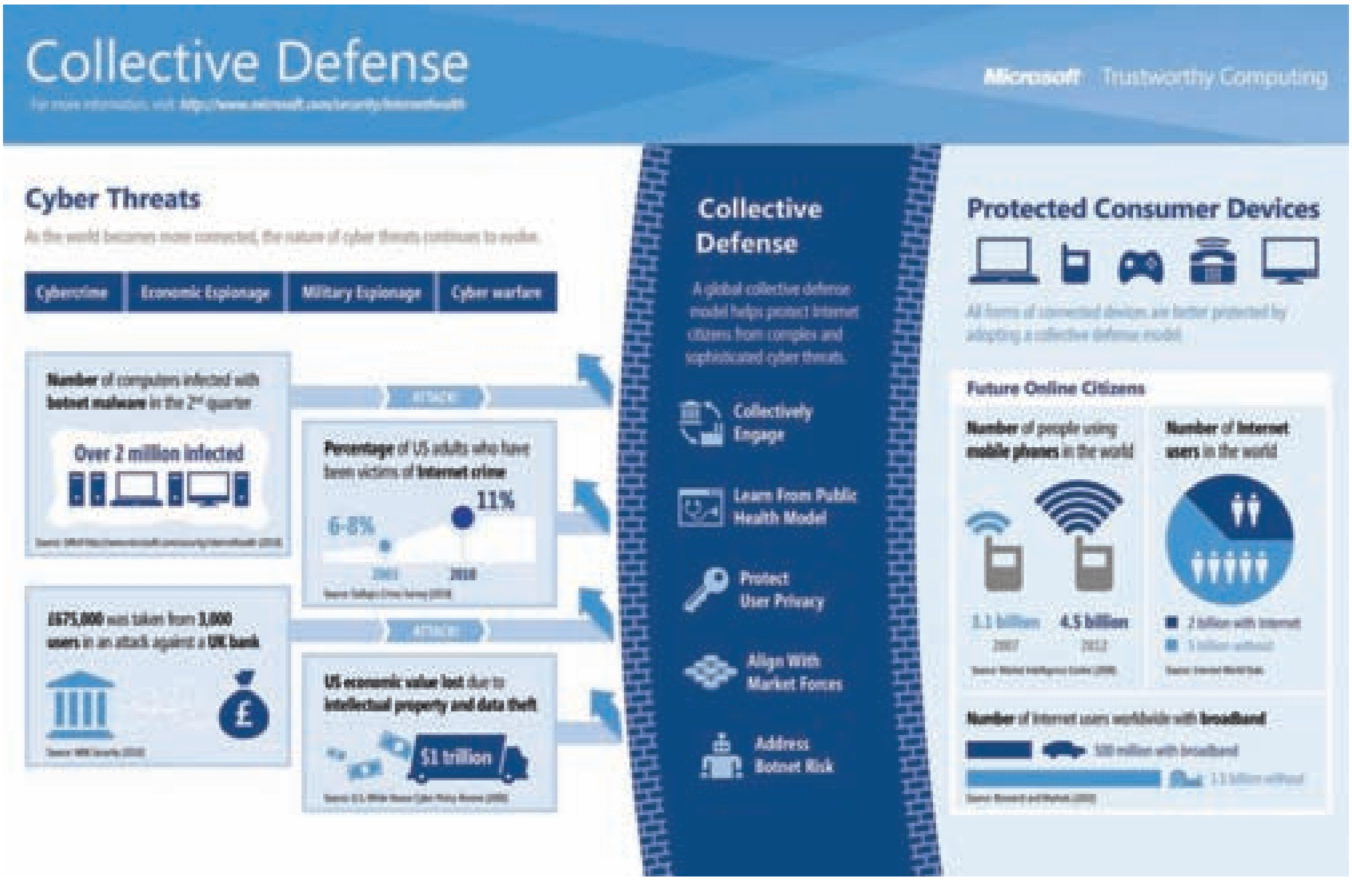
Foreign policy and diplomatic engagements on issues related to cyberspace security are not as focused as our efforts to combat terrorism or stem the proliferation of nuclear weapons. I believe that nation states should marshal their diplomatic skills and expertise to advocate cyberspace security and increase multilateral cooperation. I would caution that advocacy and cooperation are not goals in themselves. We need to focus advocacy and cooperation efforts towards specific outcomes. For example, working with like-minded nations to articulate clearly defined norms of nation-state behaviour in cyberspace could help to deter state support for cyberattacks, or hold nation-states that support such efforts accountable for their actions.

Attribution

Attribution of cyberattacks is one of the most fundamental challenges facing the international community. The inability to attribute attacks can greatly impede the effectiveness of a nation's response. Too often, valuable time is lost trying to determine if an attack or penetration of a system was an isolated criminal incident or one perpetrated by a foreign intelligence organisation. Attributing the source is essential to ensuring the appropriateness of response – criminal prosecution or military/diplomatic measures. Absent strong attribution abilities, international and national strategies to deter acts will not be taken seriously by the community of attackers who thrive on this diagnostic weakness, or by criminals who prey on citizens' inboxes and online accounts. Thus, we must focus on identity and authentication in cyberspace and enhancing swift international cooperation on cyberattacks. We must also recognise that while greater attribution will not ensure attribution in all cases, it will help to ensure that the number of incidents where attribution is difficult is reduced dramatically.

Deterrence

Deterrence did not happen overnight in the Cold War; the concept and strategy took several years to develop. Deterrence in the information age is perhaps even more complicated owing to the lack of attribution and the inability to identify strong mechanisms to prevent hostile actions. But nations can learn


Collective Defense
Microsoft Trustworthy Computing
Cyber Threats
As the world becomes more connected, the nature of cyber threats continues to evolve.
Cybercrime
Economic Espionage
Military Espionage
Cyber warfare
Number of computers infected with botnet malware in the 2nd quarter
Over 2 million infected
ATTACK!
Percentage of US adults who have been victims of Internet crime
6-8%
11%
2010
£675,000 was taken from 3,000 users in an attack against a UK bank
ATTACK!
US economic value lost due to intellectual property and data theft
$1 trillion
Collective Defense
A global collective defense model helps protect Internet citizens from complex and sophisticated cyber threats.
Collectively Engage
Learn From Public Health Model
Protect User Privacy
Align With Market Forces
Address Botnet Risk
Protected Consumer Devices
All forms of connected devices are better protected by adopting a collective defense model
Future Online Citizens
Number of people using mobile phones in the world
3.1 billion
4.5 billion
2007
2012
Number of Internet users in the world
2 billion with Internet
5 billion without
Number of Internet users worldwide with broadband
500 million with broadband
1.5 billion without

Governments and private sector shareholders must articulate a new philosophy that starts with a simple premise: government and private sector efforts should be synergistic and efficient

important lessons from the nuclear experience. In the Cold War, nations kept sensitive information secret, but disclosed enough about their strategy and capabilities for allies and adversaries alike to understand the commitment to national security and nations' ability to protect it. We must do the same for cyberspace.

Deterrence is very difficult when adversaries and bad actors are motivated and persistent. In order to improve cyberspace security in a meaningful way, deterrence requires a clear and unambiguous commitment by nations and an understanding by the spectrum of bad actors – from cybercriminals, to organised crime and nation-states – that violations of national cybersecurity have consequences. What makes deterrence successful is commitment, broadly known and broadly felt.

Cyberspace security is a shared challenge and requires government and the private sector to work together.

The private sector designs, deploys and maintains much of each nation's critical infrastructure. However, the private sector faces unique challenges because its customer base and supply chains are global. It also builds commercial products that can be targeted by sophisticated advisories, including nation-states. Private sector firms are increasingly being forced to think about security challenges that cannot reasonably be mitigated by commercially realistic development practices, especially as users remain price-sensitive.

Governments also face challenges. Unlike certain other traditional aspects of national security, cyberspace cannot be secured by the government alone; it requires a coordinated effort involving the owners, operators and vendors that make cyberspace possible. The bifurcation of responsibility (governments must protect national security) and control (they do not customarily manage the assets or provide the functions that must be protected) dictates the need for a close partnership, with clearly defined roles and responsibilities, that optimises the capabilities of participating stakeholders.

Governments and private sector stakeholders must articulate a new philosophy for collaboration, one that starts with a very simple premise: government and private-sector efforts should be synergistic and efficient. This requires that governments and the private sector: (1) identify those security requirements that will be fulfilled by the market; (2) identify national security requirements; and (3) identify how the gap between market security and national security can be filled. This effort must be focused on protecting functions (such as communications) as opposed to simply physical assets. Moreover, we must build operational partnerships that let us effectively mitigate and respond to threats.