Cyberspace – Empowered or vulnerable?

March 2013:

Cyberspace is the world's newest toy. It's a playground where almost everything is possible. The upside: It is a free-for-all world that offers the opportunity to empower more people and enrich more societies that ever before. The downside: As we transform our physical and tangible world into this digital and intangible universe we expose ourselves (and our personal information and behaviors) in new ways, leaving us more vulnerable. We are increasingly building our lives around wired or wireless networks making it possibly to live our lives in real-time, 24/7. The shift is not just in our personal lives. Businesses are becoming more and more networked and dependent on cyberspace and technology. So too are nations. The time of the Cold War with superpowers constantly on alert and building physical presence everywhere is long gone, with technology increasingly coming to the fore, for example remote-controlled drones.

For many years we have felt reasonably safe on our new playground. However, as an exploding amount of information moves into and is stored in the digital world, cyberspace is becoming the new frontline for security. A new kind of warfare is emerging with increasing numbers of targeted and malicious cyber attacks shaking up governments, businesses and consumers around the world. Knowledge and information is a source of competitive advantage, for organizations, nations and individuals. But it's also a growing challenge to retain control as mobility and the democratization of everything (commerce, politics, and societies) increases. Cyberspace is here to stay and we want our digital freedom. But how do we keep ourselves safe once we have it? The costs are rising, not only in terms of deploying protective systems and approaches, but in the rising tide of litigation, policies and regulation that could potentially transform our world into a "big brother" society in the quest to fight these new types of security threats. Are you ready to defend your business and your personal information?

The realm of cyberspace

The internet was first built as a knowledge sharing network; now massive increases in computer power and ever-faster communications infrastructure mean it is a phenomenon that we take for granted, for information at our fingertips from news updates, to scientific developments or celebrity gossip. Today over 34% of the world's population has access to the internet and it is being used diligently. Daily we create and store information, privately, for work or just for fun, and everyday ever more of it ends up in cyberspace making it grow with unimaginable speed. According to some experts the internet is actually growing at a rate of one exabyte a day – an exabyte equals 250

million DVDs. In the digital universe, 60% of the information in 2012, was created and consumed by consumers – watching digital TV, interacting with social media, sending camera phone images and videos between devices and around the internet, and so on. Yet businesses are still responsible for nearly 80% of the information in the digital universe. They need to deal with issues of copyright, privacy, and compliance with regulations even when the data zipping through their networks and server farms is created and consumed by consumers. (Source: IDC/EMC)

In Action!

So much information: Look and you will find. What cannot be found on the internet is probably not worth looking for. The internet is growing with unimaginable speed. IDC/EMC predicts that the digital universe will grow from 130 exabytes in 2005, to 2,837 exabytes in 2012, to 8,591 exabytes in 2015 and 40,026 in 2020. Cisco predicts that by 2016 data centers will be sending more than than 1.3 zettabytes of data (a zettabyte is approximately 1000 exabytes – or 250 billion DVDs) across the internet every year – in 2011 no single data center could hold a zettabyte of information. The age of the zettabyte is dawning already, as one thing is for sure, the amount of data being created is speeding up (Sources: Business Insider and IDC/EMC)

Mobile land: 2009 was the year that the world saw more data traffic than voice traffic being transmitted over the mobile network. Since then, data traffic has doubled every year. Today there are about 1.1 billion smartphones across the world and Ericsson's forecast is that by 2018 that number will triple to 3.3 billion. Cisco predicts that by the end of this year the number of mobile connected devices will be more than 7 billion, accelerating to 10 billion by 2017. The hike in mobile data traffic is already tremendous and is not expected to slow down. In 2012 global mobile traffic was 885 million gigabytes of data per month and is expected to reach 11,200 million gigabytes of data per month in 2017 (Source: BBC Future)

Look Out For...

Living in the cloud: Dropbox, Amazon, Verizon Terremark and VMware just to mention a few**.** Cloud computing is growing rapidly. The Digital Universe Study from EMC and IDC estimates that by 2020 close to 40% of the information in the digital universe will be "touched" by cloud computing and perhaps as much as 15% will be maintained in a cloud. According to the study corporate spending on third-party-managed and public-cloud environments is expected to grow from US$28 billion in 2011 to more than US$70 billion in 2015. However McKinsey Quarterly points out that this number is indeed much higher as it does not reflect what businesses spend on their private-cloud environments. (Source: McKinsey Quarterly, EMC and SC Magazine). Virtualization, connectedness and storing of data in the cloud makes todays companies increasingly open and distributed as well as less secure than yesterday's companies. The question is to what extent these shifts compromise security.

The rise of the machine: It is not the first time we have mentioned "the internet of things." New communications and connectivity technologies are turning dumb objects into smart objects. We experience this growing, often invisible machine economy as smart meters, online check-in and fridges that let you know when you need to buy more milk. While the rise of the machine may seem to be off to a slow start (often because much is invisible), it is accelerating. Now Ericsson and MegaFon in Russia have teamed up to use the Ericsson Device Connection Platform, a cloud-based connectivity platform, to cost effectively manage a large number of connected devices. Ericsson believes that by 2020 more than 50 billion connected devices will be found globally making the machine-to-machine (m2m) segment a huge unexplored market. (Source: Ericsson)

The deep web: While we did say above "Look and you will find," that's not the whole picture. Beneath the standard search engines, a deep and also in many cases a much darker internet is hidden. It is a world thousands of times larger than the indexed surface internet that most of us know and is generally inaccessible to uninvited guests. This web of hidden data includes information such as financial information, shopping catalogs, flight schedules and medical research in organization's own systems and stored in databases that remain largely invisible to search engines. Some of this information – if publically available and accessible – could offer insights and opportunities for companies. However, the deep web

has a much darker side, which poses significant risks. Lurking in its depths are thriving market places where criminals and terrorists are trading everything from arms to drugs to whatever information they can lay their hands on. As technologies advance, expect more of the deep web to become more widely accessible – but explore with caution. To learn more about the deep, dark web visit New York Times and KPMG.

Empowered to seize new opportunities

"The internet is becoming the town square for the global village of tomorrow" (Bill Gates).

The digital world has wrought significant changes in societies, individual lives, business and education. The way the world communicates has change radically. It has empowered innovation, revolutionized economies and transformed daily lives. It has opened up new markets and industries and as information flows more freely there are opportunities to further strengthen and transform our societies and businesses. Big data – the data found everywhere in cyberspace, e.g. cellphones, purchase transactions, social media sites, digital pictures and videos etc. – is making it possible to tap into heart of cyberspace. However these data and technologies can only empower and strengthen us and our businesses if we can translate data into insights, understanding and opportunities.

In Action!

Tapping into the global brain: Cyberspace increasingly allows us to tap into the global brain through crowdsourcing, open-source movements and open innovation. Organizations and individuals are turning more and more to these collaborative networks to find, create and leverage knowledge and expertise, faster and at lower cost. Kimberly-Clark did just that and has reduced the time it takes to bring out new products by 30 percent through open innovation, while Innocentive connects companies with a global network of scientists and experts who can help solve challenging problems.

Knowledge and expertise available anywhere, anytime: These days we do not really need our financial advisors any more – or at least not as much -- because we can fill out our taxes online, pay them via our mobile phone and access government records, banking, mortgage, pension information online and in real-time. If we need advice or information we tap into the global brain using real-time information tools like Wikipedia, Twitter, social networks, LinkedIn discussion boards and other community based networks. Need to vote – it is also possible online at least in some countries. Cyberspace is our playground and our standards for what we do, where and how to get reliable information and expertise are continuously changing especially as the ne(x)t generations explore and populate the digital world!

Look Out For...

Envision the future of free information: With the internet came Wikipedia, a big step towards enlightenment of the "masses." Then Ivy League universities such as Harvard, MIT, Stanford and Princeton opened up platforms making it possible for the masses to obtain Ivy League education level for free – or almost for free. Now the academic publishing game is changing. The British government has revealed a plan to make publicly funded scientific research available for anyone to access and read for free by 2014. According a study from the Finnish researchers Laasko and Björk close to 17% of the world's research papers are now published in open source journals and this trend is showing no signs of slowing down. (Source: The Guardian). It seem like we can look towards a future of more free information for everyone. The important question is how can we best use it?

Tracking every step: 770 million U.S. smartphones are GPS-enabled and that is only in the U.S. From 2011 to 2012, smartphone ownership among adults in that country rose from 35% to 46%, which means the overall proportion of U.S. adults who get location-based information has almost doubled during that time period (23% in May 2011 to 41% in February 2012). What exactly does that mean? One implication is that it gives businesses unprecedented possibilities to collect and use consumers' personal information to generate new revenue streams and sources of profit. It is an easy way for brands to connect with

consumers and form meaningful relationships. However, although location-based technology has been around for a while it is still not fully understood by the consumer. Only 50% of consumers are aware that their personal information is collected for commercial purposes. But the reasons why, how or exactly what it is used for are obscure to most. (Source: Ericsson and ODM Group). Maybe it is time to enlighten the consumer about what exactly their information is being used for, in order to make more consumers interested in using location-based services!

Being vulnerable in cyberspace

Transnational crime is growing, benefitting from globalization and, in particular, technology advances. The global cost of crime and corruption runs into trillions of U.S. dollars, including illegal trade in drugs, arms and humans, cybercrime and money laundering, with criminal organizations controlling significant financial assets. Many factors are increasing criminal organizations' reach and organizational flexibility while reducing society's ability to detect and punish crimes. These include: Increased and low-cost travel, burgeoning trade, a globalized financial system, the global transfer of knowledge, mobile communications and increasingly powerful computers. These factors also allow more individuals to access crime, threatening social beliefs and values as well as economic growth, and potentially raising geopolitical tensions. Lately we have seen a wave of cyber attacks directed in large part at American news corporations, financial institutions, businesses and the American government which are widely believed to have originated in China. But these organizations are not the only ones at risk. About every 60 seconds, malware infects 232 computers and chances are that it is yours or that of someone you know well! Even the hackers are feeling the heat, with the Twitter account of the Anonymous group recently taken over for a short time.

In Action!

Global threats – did you know: Only about half the information that *needs* protection *has* protection. This may improve slightly by 2020, as some of the better-secured information categories will grow faster than the digital universe itself, but it still means that the amount of unprotected data will grow by a factor of 26. (Source: The Digital Universe in 2020). While no one really knows the correct number McAfee has estimated the annual cost of cyber crime worldwide at US$1 trillion (Source: Computerworld). Symantec's Norton group has released another cyber crime study finding cyber crime has cost consumers about US$110 billion in the last 12 months, affecting more than 556 million people. There is no doubt that cyber crime, cyber espionage and acts of cyber war are happening every day but the exact scale is unclear and the financial costs are difficult to calculate as solid data is hard to get. How ready are you and your business for the world of cyber crime?

Where is privacy? It is thought-provoking that, according to a recent Ipsos study, 45% of U.S. adults feel that they have little (33%) or no (12%) control over the personal information that companies gather while they are browsing the web or using online services such as photo sharing, travel, or gaming. Only 21% say that they have a significant amount of control over such personal information, while 34% feel that they have moderate control. 85% have taken steps to protect their privacy such as deleting cookies (65%), opting out of targeting advertising (44%), uninstalling an app (41%), request that websites don't track them (39%), stopped using an online service (21%) and changed to a different website or online service (20%). 15% say that they have not taken any of these actions to protect themselves. (Source: Ipsos) Is it even possible to be in cyberspace and not be tracked?

Look Out For...

Getting more malicious and targeted: Cyber crime is increasingly dangerous for governments, businesses and ordinary people alike. As the malware Flame was discovered, the UN urged co-operation and peaceful resolutions among countries to prevent a global cyber war. Symantec is predicting that 2013 will be the year where cyber conflicts become the norm with nations, organizations, and individuals increasingly involved. Also expect more targeted attacks on individuals and non-government organizations. Ransomware will be the new scareware. Mobile adware, or "madware," will be a nuisance

that disrupts the user experience and can potentially expose location details, contact information, and device identifiers to cybercriminals.

Challenging our financial system: Trillions of dollars' worth of transactions occur every day in cyberspace around the world, whether corporate or private, the big guys on Wall Street or you buying groceries. However these can come with an unwelcome price tag. As banking becomes increasingly electronic, hacker attacks on the financial system are rising. In the last couple of months some 30 large global banks, mostly American, have been hacked, shutting down their websites. The threat is evolving and one can only imagine what massive and potentially long-lasting consequences a crippling hacker attack against the financial system could have: disrupting stock and commodity markets as well the flow of money among banks, businesses and consumers around the world – and massively damaging trust. Such hacker attacks ultimately have the potential to disrupt economic growth and threaten societies. (Sources: The Economist and WSJ)

The internet's weakest links: How vulnerable is your organization to being disconnected from the world wide web? Perhaps more than you think, depending on your location. If you are in Belarus or Iran, it's time to think about Plan B if there's a connection hitch, while in war-torn Afghanistan your vulnerability to disconnection is about the same as if you are in the populous democracy of India. In 2012 Renesys, a consultancy focused on risks to connectivity, created a map ranking every country's risk of internet disconnection. One metric is critical – the number of "frontier" internet service providers in a country, which are those that have gateways to the global internet, not just to domestic networks. Afghanistan because of necessity has a huge range of different modes of connection to the internet at large, while in Belarus the state-owned telecoms entity "owns" the country's only connection to the world. However, even in countries deemed to be at low risk of disconnection, such as China, which has many frontier ISPs, there are still questions about the ability of the state (or potentially criminals) to shut down (or slow down) access to the internet – while it could take time to close all the gateways, recent history suggests that it is not impossible. So time to figure out how connected your location really is. (Source: BBC)

Protecting ourselves, our businesses and governments – responding to the challenges of cyberspace

As vulnerabilities and cyber attacks are becoming the new "normal," tackling the challenge will demand new forms of cooperation, risk management and deterrence between nations, intergovernmental, governmental, security and business organizations. Individuals and communities will also have to step up their awareness of and preparedness for security threats. Cybercrime is dangerous for governments, businesses and ordinary people alike. But it's not a simple debate, because it's not just the "bad guys" at it: cyber warfare, as well as less aggressive disruption and information gathering (even espionage) activities in the pursuit of "home" security interests, are increasingly being deployed by nations, sometimes even by businesses. With the rise in targeted attacks and malware like Stuxnet, DuQu, Flame and Gauss there is likely to be an increasing debate around the line between the legitimate pursuit of national security interests and criminal activity.

In Action!

Are we prepared at all? According to the report "Cyber-security: The vexed question of global rules," from the security and defense think-tank SDA with the support of McAfee, 57% of global experts believe that an arms race is taking place in cyberspace; 36% believe cyber security is more important than missile defense; and 43% identify damage or disruption to critical infrastructure as the greatest single threat posed by cyber attacks with wide economic consequences. 45% of respondents believe that cyber security is as important as border security. However, the state of cyber readiness of the United States, Australia, UK, China and Germany all ranked behind smaller countries such as Israel, Sweden and Finland (23 countries ranked in report).

Balancing regulation and free speech: In the Philippines a controversial cyber crime law has been suspended after a public outcry. It was initially put in place to protect against Internet crimes like hacking,

identity theft, spamming, and online child pornography. In January 2012 a similar public outcry swept the Internet and shook the power structure of Washington, D.C. aiming to stop PIPA (Protect IP Act) and SOPA (Stop Online Piracy Act). According to Freedom House recent revisions to the United Arab Emirates' cyber crime law will not only restrict internet freedom but are in violation of citizens' rights to freedom of expression. (Sources: Global Post and Freedom House). The need for cyber crime laws is clearly rising. In most countries cyber laws are meant to protect citizens and organizations, but many believe a proliferation of regulation could stifle free expression and speech.

Look Out For...

The "big brother" society: You are being watched! Ever more of our daily lives is being recorded and stored. Think about it: how many of your actions and whereabouts are not being watched? Yes, it is a little creepy! Today, high-tech cameras can be found in buses, schools, train stations, banks, airports, hospitals, street corners, some workplaces, to name but a few locations. Don't think you can escape online: your "like" and "dislike" reactions are being tracked when shopping, and if you are on some sites long enough this will trigger an offer of a personal helper to find what you need. And by the way, the ads you see next time you are surfing will reflect your latest searches (or perhaps those of your friends). Is this what we want, a big brother society watching us, recognizing us everywhere? Facial recognition software are gaining traction, even as nanosensors that could enable organizations to monitor their employees around the clock, recording where they visit, whom they talk with, and what they consume are under development. What about a human-implanted nanochips that able to track an individual's location and possibly, what that person consumed (drugs, junk food; etc.)? this is not a bad sci-fi movie – it is more realistic than you think. (Source: Institute for Ethics & Emerging Technologies) Using it to get the bad boys will be great but what about you. How much privacy are you willing to give up – and how much do you realize that you are already giving up?

Protecting nations: As cyber security breaches increase and cyber attacks intensify, more and more governments are proposing initiatives to restrain and fight cyber crime. The EU, for instance, is proposing new cyber crime rules that could require more than 40,000 companies, including energy providers, banks and hospitals to report cyber-break-ins. (Sources: BBC). In his recent state-of-the-union message, President Barack Obama unveiled an executive order intended to plug the gap left by the failure of Congress to pass cyber-security legislation to match the growing threat. The executive order focuses on sharing information about threats between government agencies and the private sector. (Source: The Economist)

In March: Look out for trends in action on Realizing the promise of new geographic markets!