Cybersecurity Futures: How Can We Regulate Emergent Risks?

Benoit Dupont

> *When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is very probably wrong.*
>
> Arthur C Clarke (1917–2008)
> Science-fiction writer, futurist, and inventor

This article reviews nine socio-technical trends that are likely to shape the cybersecurity environment over the next decade. These nine trends have reached various levels of maturity, and some – such as quantum computing – are still theoretically contentious. These trends are: cloud computing; big data; the Internet of Things; the mobile Internet; brain–computer interfaces; near field communication payment systems; mobile robots; quantum computing; and the militarization of the Internet.

What these nine trends have in common is that they will be instrumental in generating new opportunities for offending, which will result from an exponential increase in the quantity of data, number of connection points to the Internet, and velocity of data flows that irrigate the digital ecosystem. As a result, more opportunities for malicious exploitation will be available to attackers, "security by design" will be harder to achieve in such a fluid and dynamic environment, and the performance of control mechanisms is likely to erode significantly.

Technical solutions to address these challenges are already being developed by computer scientists. This article focuses on a different and complementary approach, finding inspiration in the work of regulatory scholars who have framed promising theories such as regulatory pluralism and responsive regulation to explore options for the necessary institutional adaptation to these future changes.

Introduction

The current threat landscape that characterizes computer networks and critical infrastructures is already so saturated with complex risks that it seems futile to extrapolate what the future of cybersecurity will look like 10 years from now. Indeed, Napoleon Bonaparte once said that "simpletons talk of the past, wise men of the present, and fools of the future" (tinyurl.com/7yhoexj). However, a number of information technologies have disrupted existing economical, social, political, and legal arrangements, and it is likely that similar transformations will repeat themselves at regular intervals. The term "disruptive technology" was first used by Clayton Christensen (1997; tinyurl.com/7onvohk) to analyze innovations that do not simply improve the performance of existing technologies (these innovations are called sustaining technologies), but that instead define entirely new products or services to meet unsatisfied needs, and consequently make a lasting change in the technological landscape into which they fit. However, criminals are also very ingenious innovators who take advantage of disruptive technologies to open “breaches”, which can be defined as “sudden new opportunities for offending that opened as a result of changes in the technological or social environment” (Killias, 2006; tinyurl.com/m6qmdz5). These breaches are often the result of a defective legal or regulatory coverage and provoke rapid increases in offences, before the breach is closed and offenders move on to the next opportunity. In such a rapidly evolving context, it therefore becomes crucial to anticipate what breaches are likely to open as the result of technological innovations, so that policies and regulations can be developed proactively in order to minimize their impact on Internet users.

Current cybersecurity discourses focus on national security threats such as destructive cyberattacks against critical infrastructures or cyberspying campaigns targeting valuable intellectual property and sensitive strategic information (Brito and Watkins, 2011: tinyurl.com/mtmv7xy; ONCE, 2011: tinyurl.com/638opk9; Gendron and Rudner, 2012: tinyurl.com/lbn2yxm). However, more mundane cybercriminal risks receive considerably less attention and investments from governments, despite the fact that they already affect a much larger share of the population than their national-security counterparts. According to recent Canadian victimization statistics, cyberfrauds represent roughly one-third of all property crimes and significantly outnumbered car thefts, burglaries, and vandalism incidents in 2009 (Perreault and Brennan, 2010: tinyurl.com/lnhlg4a; Perreault, 2011: tinyurl.com/mwae6m6), in line with similar patterns observed in the UK (Anderson et al., 2012; tinyurl.com/csnqtkr). Yet, the majority of police organizations remain under-resourced to address this issue, policy makers are still in the process of developing effective cybercrime control mechanisms, and many private actors keep on marketing equipment, applications, and services whose security remain problematic.

This article sketches the contours of the cybersecurity challenges that are likely to emerge over the next decade and to analyze their security and regulatory implications, so that more effective systems can be designed to monitor and close breaches. In the first section, I introduce the nine disruptive technological trends that forecasters predict will most radically alter the Internet ecosystem over the next 10 years. In the second section, I examine the six cybersecurity implications of these trends and discuss potential breaches that could open if the *status quo* is maintained. Finally, in the third section, I consider what regulatory adaptations could deal more effectively with future cybersecurity problems.

Nine Disruptive Socio-technical Trends

The nine socio-technical trends that are discussed below and are most likely to have an impact on the cybersecurity environment over the next decade were identified and described by the author in a report commissioned by Public Safety Canada Cybersecurity’s Directorate and are available online (Dupont, 2012; tinyurl.com/kqqd39f). Because this list includes trends that have reached various stages of maturity, there is unfortunately a strong bias toward technologies that are already commercially available or are reaching the “peak of inflated expectations” in Gartner’s “Hype cycle” (Fenn, 2010; tinyurl.com/msw6vn2).

1. Cloud computing

The consulting firm IDC estimates that, in 2020, one-third of computer data will be stored in or will transit through systems administered in the cloud, and that the explosion of this market could generate revenues in excess of one trillion dollars by 2014 (Gantz and Reinsel, 2010: tinyurl.com/m8curcy; Nash, 2011: tinyurl.com/k3egchu). The unparalleled flexibility of cloud computing that promises reduced costs to companies that use it make it an irresistible proposition, particularly in these turbulent financial times (IBM, 2011; tinyurl.com/l7o23cb), and even individuals become avid consumers of cloud services such as Dropbox or Netflix.

2. Big data

The term big data reflects the appearance in recent years of datasets containing gigantic volumes of unstructured or disparate information. The units of measurement used to describe these volumes of data are no longer the gigabyte or the terabyte, but the peta , exa-, or even zettabyte (10^{21} bytes). IDC estimates that, in 2011, the worldwide quantity of information created and exchanged on digital media (the digital universe) was approximately 1.8 zettabytes, and that it would be multiplied by 20 by 2020 to reach 38 zettabytes (Gantz and Reinsel, 2011; tinyurl.com/3f56u9t). The volume and diversity of the data processed prevent traditional analysis techniques from being used, and specialized solutions that are based on cutting-edge computer tools and statistics (such as Hadoop MapReduce programming [tinyurl.com/qqjot] and R language [tinyurl.com/yp9y64] for statistical analyses and visualization) are deployed on infrastructures specially designed for such uses.

3. The Internet of Things

This term refers to the growing interaction between the physical and digital worlds through sensors and data-capture devices integrated into the objects around us (from cars to pacemakers to refrigerators to smart meters). These objects gain the ability to communicate wirelessly with computer networks through the Internet. The massive flow of data produced by these objects allows for their operations and the environments in which they operate to be more effectively monitored and managed (Chui et al., 2010; tinyurl.com/mqa7942). There are already more objects than computers connected to the Internet (Fenn and LeHong, 2011; tinyurl.com/7a577pl), and Cisco predicts that over 50 billion objects will be connected to the Internet by 2020 (Evans, 2011; tinyurl.com/88uhsx3).

4. Mobile Internet
The concept of mobile Internet or mobile computing designates all technologies that provide full or partial access to the Internet using mobile devices such as smartphones or tablets. In 2012, worldwide sales of mobile Internet devices reached 850 million units, whereas desktop and laptop PCs barely moved 350 million units. The growth rate for tablets and smartphones is evaluated at 174% and 110% respectively over the next four years (IDC, 2013; tinyurl.com/ck2aoxj).

5. Brain–computer interfaces
Brain–computer interfaces are technologies used to directly connect external computer devices to the human brain. These devices allow individuals to interact with computers by thought. These technologies are currently used in medicine to compensate, assist, or augment the cognitive and motor functions of individuals with physical or psychological disabilities. These previously costly technologies that were restricted to the world of research are appearing in consumer electronics and will gradually replace the keyboard and mouse as humans' preferred ways to interact with machines (Yuan and Barker, 2011; tinyurl.com/mkgxm4s). Significant advances have been made in this field, and for the past few months Emotiv (emotiv.com) has been marketing a $300 wireless neuro-headset to capture and process brain signals.

6. Near field communication (NFC)
This is a form of payment that uses various wireless communication technologies related to radio-frequency identification (RFID; tinyurl.com/82u9a) chips to facilitate financial transactions at points of sale. This technology is primarily installed on payment cards and on mobile phones, which can carry out a transaction if placed a few centimetres from a properly-equipped receiver. This technology considerably accelerates the point-of-sale process (Tata, 2011; tinyurl.com/nywjbqx) and is intended to compete directly with traditional payment methods such as cash or credit cards (Ondrus and Pigneur, 2009; tinyurl.com/la3xq9b).

7. Mobile robots
Multi-jointed mechanical systems that are able to travel autonomously or semi-autonomously and that have the ability to influence their immediate environment are known as mobile robots. Some of these robots also have wireless communication functions that allow us to consider the concept of collaborative robots (MEFI, 2011; tinyurl.com/lf5jywj). Mobile robots can be found in a growing number of sectors, such as manufacturing, but also service industries, the health sector, and any occupation where humans accomplish dangerous tasks. Japan and Germany are the most advanced countries in the development of civilian mobile robotics, while the United States and Israel dominate the military robotics market. France's ministry of the economy estimates that the robot market could represent $30 billion by 2015 (MEFI, 2011; tinyurl.com/lf5jywj).

8. Quantum computing
This branch of computer science is still at a very embryonic stage of development but nevertheless suggests revolutionary applications in terms of calculating power and therefore security. Quantum computing uses the laws of quantum mechanics to process large volumes of information much more efficiently than traditional computing. Very specialized quantum cryptography solutions are already on the market, and some large organizations such as IBM, HP, Microsoft, Google, NASA, and Lockheed Martin, as well as startups such as D-Wave Systems in British Columbia, are investing large sums in quantum computing to accelerate the development of machines for practical applications.

9. Militarization of the Internet
In the past few years, military doctrine has changed to make control of the Internet not only an internal security issue but also a national security issue, with a sharp increase in the resources devoted to the development of offensive and defensive capabilities (Deibert, 2010; tinyurl.com/l96vzk7). At least 33 states (including Canada) have explicitly acknowledged developing offensive and defensive operational capabilities in cyberspace (Lewis and Timlin, 2011; tinyurl.com/mpfw7cv). The Pentagon spent just over $3.2 billion USD in 2012 on its defensive and offensive efforts in the cybersecurity domain (Sternstein, 2011; tinyurl.com/k9kbaes).

Six Cybersecurity Challenges

The trends outlined in the previous section will all create specific cybersecurity issues, which I examined at length in my full report (Dupont, 2012; tinyurl.com/kqqd39f). However, one important dimension to consider is their high level of integration. These nine trends are technically and socially interdependent, and some even have symbiotic relationships with each other (such as the mobile Internet and NFC payments). Other trends will converge to provide new services to individuals and businesses, such as the Internet of Things, which will benefit from scientific advances in big data to improve business productivity. Figure 1 maps a subjective sample of the interdependencies identified in the full report, and makes no claims to be exhaustive, in that new links will certainly appear as hard-to-predict disruptive innovations occur.

These interdependencies illustrate the growing number of ties linking technologies that used to be considered separately. In such a tightly coupled system, it becomes counterproductive to think about cybersecurity in narrow terms and a high-level, whole-system approach is essential in order to facilitate the emergence of effective policies and regulatory mechanisms. In this perspective, six broad security challenges can be anticipated.

1. More data
The huge quantity of information produced and stored by the vast numbers of machines that will be connected to the Internet will require the development of security technologies that remain efficient at this scale and that can detect potential risks among an ever-expanding constellation of unstructured and highly heterogeneous datasets. Given that even the smallest organizations will amass large amounts of information, the organizational capacity to keep the safe custody of such large datasets will be in question (Lane, 2011; tinyurl.com/p3y9lba).

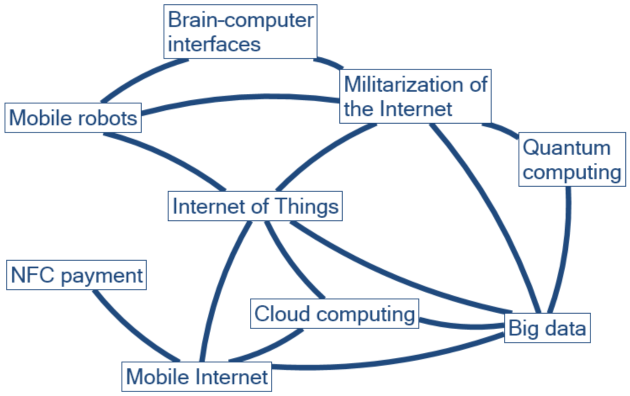

Figure 1. Key interdependencies between socio-technical cybersecurity trends

2. More connections
Each new object connected to the Internet will represent an additional entry point to the digital ecosystem that will have to be secured. This will prove particularly difficult for autonomous machines such as robots and smart meters that operate in public spaces and can be easily tampered with, or for devices that are produced in such large quantities that security features need to remain rudimentary to keep costs down (Roman et al., 2011; tinyurl.com/nqgl9qn). The proliferation of connected devices and objects will also increase surveillance capacities to an unprecedented level, and will allow malicious actors to surreptitiously collect contextual personal data that had never been available before such as geographical coordinates, on-the-fly biometric information, sounds, smells, chemical compositions, etc.

3. More movement and flows
The oceans of data generated by mobile devices, objects, and sensors will circulate in the digital ecosystem at high velocity in order to be stored, shared, and analyzed by organizations trying to discover hidden opportunities. Each movement will leave behind data traces and residues that could be exploited by malicious actors if treated carelessly. The escalation and acceleration of data flows may lead to a dilution of security responsibilities if adequate regulatory obligations are not developed and implemented.

4. More opportunities for malicious exploitation
The expansion and diversification of the digital ecosystem, which is unlikely to slow over the next decade, will benefit criminal offenders and various categories of attackers whose range of suitable targets will increase exponentially; this is a classical application of Cohen and Felson's (1979; tinyurl.com/pml7vcq) routine-activity theory. Low-skill hackers will statistically find more unprotected machines available online, while high-skill hackers will leverage these new opportunities to create larger botnets and launch more damaging and unpredictable attacks.

5. Less security by design
The "security by design" movement, which was initially inspired by C. Ray Jeffery's (1971; tinyurl.com/pdzyvox) work on crime prevention through environmental design, has now expanded beyond buildings and spaces to include objects, machines, and applications. Com-

panies and inventors are encouraged to consider how they can reduce offender opportunities early enough in the design process by undertaking research, observing users, and interviewing stakeholders (Alliance Against Crime, 2011; tinyurl.com/p3v9t2d). This long and complex method, which can be applied to software design (Gegick and Barnum, 2005; tinyurl.com/oy5fe7e), is unfortunately incompatible with faster innovation cycles where new products are brought to market as soon as possible to prevent competitors from achieving a dominant position. In contrast with other industrial sectors such as car, plane, or toy manufacturing, very limited enforceable security standards are in place to offset the absence of economic incentive in marketing safe products.

6. Less control

The growing complexity inherent to a digital ecosystem relying on highly diversified technologies that were not necessarily developed to be used by such a large proportion of the population or in an integrated manner creates technical and regulatory challenges that delay the implementation of effective control mechanisms. Legacy technical protocols and existing government institutions are not well prepared to deal with this new reality and apply industrial-era answers to digital-era problems. The case of privacy is a good example. The traditional privacy-control mechanisms that organizations, individuals, and regulatory authorities currently have available become particularly difficult to use, if not obsolete. This is because the mix of big data, cloud computing, mobile Internet, NFC payments, and the Internet of objects technologies will automatically and constantly generate huge personal data streams shared by a myriad of organizations. In such an environment, how can one ascertain what types of data are collected and retained, with what degree of accuracy and reliability, or what data retention, exchange, marketing, and destruction policies are implemented? Moreover, every disruptive technology causes the appearance of new actors in the digital ecosystem. From a cybersecurity perspective, this instability makes coordination efforts more difficult by constantly introducing new organizational actors whose abilities and willingness to contribute to the security of the ecosystem as a whole are difficult for their partners and the regulatory authorities to assess and mobilize.

Regulatory Options to Increase the Digital Ecosystem's Resilience

While computer scientists are actively working on technical fixes to solve the six challenges listed above, the nature of the debate among social-science scholars has been much more cautious and skeptical. Efforts to design and implement regulatory mechanisms that could enhance the safety of online users have more or less explicitly been associated with governmental attacks eroding the Internet's core values of freedom and openness (Zittrain, 2009: tinyurl.com/qb9blmc; Deibert and Rohozinski, 2010: tinyurl.com/l96vzk7; Mueller, 2010: tinyurl.com/qdgkqbx; Palfrey, 2010: tinyurl.com/m5sxsja). So, while the digital ecosystem is expanding and integrating, regulatory theory remains fragmented and reluctant to offer new alternatives to address existing and future cybersecurity challenges. If we return to the diagram of interconnected trends (Figure 1), we would ideally need to map a corresponding diagram representing links between regulatory regimes that should be reflecting these changes. This second diagram would represent the linkages that should be established between various fields of regulation (such as banking regulations, health, law, and medical ethics – for brain computer interfaces, criminal law, traffic regulations – for mobile robots, the law of war, privacy regulations, international industrial and security standards, telecom regulation, etc) in order to move toward a regulatory model that could harness this plurality instead of being constrained by it.

The concept of “regulatory pluralism” recognizes that regulation has become dispersed and that many institutions (including private actors) and tools beyond the state from a broad range of fields can be mobilized to achieve outcomes aligned with the public good (Grabosky, 1995; tinyurl.com/lk7vkkp). What characterizes regulatory pluralism is the belief that, by relying on diverse, complementary, and self-reinforcing regulatory instruments, policies can be implemented in a manner that is more responsive to the specific context, resources, and constraints of a particular sector (Crawford, 2006; tinyurl.com/lshb4wv). In other words, regulation becomes focused on hard problems to solve and outcomes to achieve instead of being obsessed by compliance to a narrow set of prescribed behaviours. In his influential book on cyberspace regulation, Lessig (2006; tinyurl.com/lf5zrfb) outlines four types of regulatory constraints that can be leveraged separately or in combination to tackle complex problems: the law, social norms, market forces, and technological architecture. Countries such as Japan, South Korea, Australia, and Germany are already experimenting with this regulatory pluralism approach to combat botnets by forging alliances of state regulators, Internet service providers, and anti-virus companies to persuade (or in some instances compel) computer users to clean their infected machines (Dupont, 2013: "An International Comparison of

Cybersecurity Futures: How Can We Regulate Emergent Risks?

Benoit Dupont

Anti-Botnet Partnerships", Public Safety Canada: Ottawa). Without any need to legislate and with limited public monies, these initiatives are achieving promising outcomes through innovative regulatory approaches that harness the four levers described by Lessig.

The question then becomes how to ensure optimal and consistent participation when regulation is entrusted to a large extent to private actors. In other words, can a diversity of actors operating in a pluralistic regulatory environment be effectively incentivized and choreographed without building a large counterproductive bureaucracy (Grabosky, 2012; tinyurl.com/mwrbf8t)? In trying to answer this question, Ayres and Braithwaite (1992; tinyurl.com/muyrh78) suggest that the concept of "responsive regulation" may offer an innovative and cost-efficient alternative to the dichotomy of state-regulation versus self-regulation. Their theory rests on the core principle of the "benign big gun", where escalating enforcement practices are deployed in order to individualize the regulatory activity's intensity to the regulated actors' behaviour. The default strategy in this context is non-intrusive and delegated regulation, which is more likely to generate cooperation and innovation among private actors by allowing them discretion in deciding how best to achieve regulatory goals. For private actors that are unwilling or unable to implement effective strategies (i.e., in a case of market failure), the state retains the ability to escalate its level of interventionism by shifting to command-and-control regulations that involve various forms of punishment. Responsive regulation principles are inherently compatible with the need to preserve the innovative potential of Canadian companies in a highly competitive business context, by letting key stakeholders find optimal solutions suited to their particular needs and capacities before state interventions become escalated to more coercive and costly approaches.

Conclusion

The gap between the anticipated evolutions of the digital ecosystem and the regulatory tools that are being currently forged by regulatory authorities seem to comfort Killias' (2006; tinyurl.com/m6qmdz5) general theory of crime and security breaches. However, the major difference with Killias' historical examples of mass production of spirits, consumer goods, or the emergence of the banking system, is that the current wave of techno-social innovations is unfolding on many different fronts and that the resulting interdependencies introduce an unmatched level of complexity. We tend to think about new trends in isolation; in this article, I argue for a more holistic approach. I have sketched how nine techno-social trends will shape the digital ecosystem, and how new cybersecurity challenges and requirements will emerge as a result. Without a concerted and integrated regulatory strategy to guarantee the security and stability of the digital ecosystem, Canada's technological capacity may erode and fall behind its global competitors. Some countries such as Australia, Japan, and Germany, among others, are already experimenting with multi-stakeholder or nodal regulatory schemes to manage complex digital risks such as botnets (Dupont, 2013: "An International Comparison of Anti-Botnet Partnerships", Public Safety Canada: Ottawa). Other fields of regulation have also witnessed the emergence of ingenious initiatives that may also be transferrable to the cybersecurity environment (Braithwaite and Drahos, 2000; tinyurl.com/msp2xu5). But, expecting that the status quo or laissez-faire solutions will miraculously produce enhanced cybersecurity in this fluid environment is clearly not a sustainable option.

Acknowledgments

This article is based on two reports prepared for Public Safety Canada's National Cybersecurity Directorate. The author wishes to thank Public Safety Canada for the support provided to complete this research.

About the Author

Benoit Dupont is the Canada Research Chair in Security and Technology at the Université de Montréal, where he is Professor of Criminology and Director of the International Centre for Comparative Criminology. Professor Dupont researches the coevolution of crime and technology, focusing on offences such as identity theft, bank fraud, computer hacking, and telecommunications fraud. His political science background also leads him to examine emerging cybersecurity policies and what forms of regulation can be developed to address the new risk landscape.

Citation: Dupont, B. 2013. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review*. July 2013: 6–11.

Keywords: cybersecurity, technological trends, forecasting, emerging risks, digital ecosystem, cybersecurity policies, regulation