Journal of Strategic Security

Volume 4
Number 2 *Volume 4, No. 2, Summer 2011: Strategic Security in the Cyber Age*

Article 6

Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy

Audrey Guinchard , Ph.D.
University of Essex, United Kingdom, abguin@essex.ac.uk

pp. 75-96

Recommended Citation
Guinchard, Audrey , Ph.D.. "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy." *Journal of Strategic Security* 4, no. 2 (2011): : 75-96.
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5
Available at: https://scholarcommons.usf.edu/jss/vol4/iss2/6

Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy

Author Biography

Dr. Audrey Guinchard, Senior Lecturer in Law (2009–Present), joined the University of Essex (UK) in October 2000 and is the co-director of the double degree LLB English and French Laws with Master 1/Maîtrise. She has a Licence en droit, an LL.M., and a Ph.D. in criminal law from the University of Jean Moulin (Lyon, France). Her current research focuses on crime and the virtual world as a starting point for a broader perspective on criminal law's ability to adapt to new technologies. In 2010, she was a visiting fellow at the Centre for Research in Arts, Social Sciences and Humanities (CRASSH) in Cambridge as part of the program on The Future University. Bringing a comparative law perspective to bear on criminal law issues, she published notably on hate crimes and on the concept of criminal charges regarding financial services, both in French and in English.

Abstract

Most of the actions that fall under the trilogy of cyber crime, terrorism, and war exploit pre-existing weaknesses in the underlying technology. Because these vulnerabilities that exist in the network are not themselves illegal, they tend to be overlooked in the debate on cyber security. A UK report on the cost of cyber crime illustrates this approach. Its authors chose to exclude from their analysis the costs in anticipation of cyber crime, such as insurance costs and the costs of purchasing anti-virus software on the basis that "these are likely to be factored into normal dayto-day expenditures for the Government, businesses, and individuals. This article contends if these costs had been quantified and integrated into the cost of cyber crime, then the analysis would have revealed that what matters is not so much cyber crime, but the fertile terrain of vulnerabilities that unleash a range of possibilities to whomever wishes to exploit them. By downplaying the vulnerabilities, the threats represented by cyber war, cyber terrorism, and cyber crime are conversely inflated. Therefore, reassessing risk as a strategy for security in cyberspace must include acknowledgment of understated vulnerabilities, as well as a better distributed knowledge about the nature and character of the overhyped threats of cyber crime, cyber terrorism, and cyber war.

Journal of Strategic Security
Volume IV Issue 2 2011, pp. 75-96
DOI: 10.5038/1944-0472.4.2.5

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy

Dr. Audrey Guinchard
University of Essex
United Kingdom
abguin@essex.ac.uk

Abstract

Most of the actions that fall under the trilogy of cyber crime, terrorism, and war exploit pre-existing weaknesses in the underlying technology. Because these vulnerabilities that exist in the network are not themselves illegal, they tend to be overlooked in the debate on cyber security. A UK report on the cost of cyber crime illustrates this approach. Its authors chose to exclude from their analysis the "costs in anticipation of cyber crime, such as insurance costs and the costs of purchasing anti-virus software," on the basis that "these are likely to be factored into normal day-to-day expenditures for the Government, businesses, and individuals."[1] This article contends if these costs had been quantified and integrated into the cost of cyber crime, then the analysis would have revealed that what matters is not so much cyber crime, but the fertile terrain of vulnerabilities that unleash a range of possibilities to whomever wishes to exploit them. By downplaying the vulnerabilities, the threats represented by cyber war, cyber terrorism, and cyber crime are conversely inflated. Therefore, reassessing risk as a strategy for security in cyberspace must include acknowledgment of understated vulnerabilities, as well as a better distributed knowledge about the nature and character of the overhyped threats of cyber crime, cyber terrorism, and cyber war.

Introduction

Ulrich Beck's *Risk Society*, published in 1986, proposed a new reading of the changes experienced by modern society since the early 1970s, grounded on his analysis of the environmental and health hazards caused by pollution and nuclear technology.[2] Twenty-odd years later, the risks and patterns of reactions he described in a world without the Internet are surprisingly apt for analyzing security issues in cyberspace. For Beck, the risks that industrialization and modernization created tend to be global, systemic with a "boomerang effect,"[3] and denied, overlooked, or overhyped.[4] The very nature of information technology, with the creation of the World Wide Web (WWW), its ubiquity, and the interconnectedness that it creates between systems heightens the possibility of "cascading effects."[5] Moreover, the narrative about cyber risks is dominated by competing expert claims, alongside a media prone to inflate cyber risks.[6] Indeed, a quick glance at the recent official reports, in the UK and internationally, reveals different perspectives on risks in cyberspace. For a few, if the use of cyber weapons "will shortly become ubiquitous,"[7] "it is unlikely that there will ever be a true cyber war" since, notably, "there is no strategic reason why any aggressor would limit themselves to only one class of weaponry."[8] For others, on the contrary, cyber war is a serious possibility,[9] if not already an entrenched reality.[10] In addition, cyber crime costs billions;[11] and its occurrence, as well as that of cyber terrorism, are doomed to increase.[12]

The media reports on the latest attacks, such as the one on the European Commission in late March 2011,[13] seem to give credit to these gloomy views. The complexity of some cyber incidents does not dispel the sensation of an undefined but serious danger. In 2007, when Estonia faced a series of distributed denial of service (DDOS) attacks against its governmental and critical private-sector IT structure, as well as the defacement of the prime minister's party's website, it first accused Russia of ordering the attacks. The attacks seemed to originate from Russian servers and computers, and there was a dispute about a Russian war memorial. However, the compromised computers thought to be Russian in the early days of the attacks could have been zombies controlled by any citizens, including Estonians. In addition, Russia denied the attacks and did not issue threats or take further action. At the end, Estonia came to the conclusion that it could not identify the attackers well enough to affirm whether it had been the victim of a skirmish ordered and supported by a nation, a terrorist organization, an organized crime group, or just a crime committed by individuals. Of course, not all cyber incidents are so complex. Nevertheless, the exact nature of cyber attacks and sometimes their scale tend to be difficult to assess; and their authors often cannot be identified.[14]

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

Cyber incidents are not always visible until it is too late, which is the very characteristic of modern risk.[15]

The proper approach is to gain a better understanding of the cyber threat, which is precisely what Beck advocated in his 1986 *Risk Society*.[16] The 2007 Estonian incident cited above triggered a reassessment of cyber risks, with nation-states and international organizations (NATO,[17] OECD) reflecting on what happened and what could happen. Knowledge is at the heart of a strategy for security in cyberspace. Otherwise, "[i]nadequate knowledge ... leads to over- or underestimating the real need for cyber security," hence "generating insecurity and fear."[18] But this knowledge must not limit itself to the illegal behaviors that can constitute cyber crime, terrorism, or war. It must also encompass the very roots of these threats. Indeed, most of the actions that fall under the trilogy of cyber crime, terrorism, and war exploit pre-existing weaknesses in the technology. Maybe because these vulnerabilities in the network, in the exploitation systems, and in applications are not themselves illegal, they tend to be overlooked in the debate on cyber security. The UK report on the cost of cyber crime illustrates this approach. Its authors chose to exclude from their analysis the "costs in anticipation of cyber crime, such as insurance costs and the costs of purchasing anti-virus software," on the basis that "these are likely to be factored into normal day-to-day expenditures for the Government, businesses, and individuals."[19] But maybe if these costs had been quantified and integrated into the cost of cyber crime, the analysis would have revealed that what matters is not so much cyber crime as the fertile terrain of vulnerabilities that unleash a range of possibilities to whomever wishes to exploit them. By downplaying the former, the threats represented by cyber war, cyber terrorism, and cyber crime are conversely inflated. Therefore, reassessing risk as a viable strategy for security in cyberspace means the acknowledgment of understated vulnerabilities as much as it means a better knowledge of the overhyped threats of cyber crime, cyber terrorism, and cyber war.

Overhyped Threats: Towards a Strategy of Knowledge

The discourse on cyber threats tends to be dominated by excessive publicity given to some threats to the detriment of others, and by exaggerated claims about the frequency and scale of the attacks. This narrative distorts the public perception of the threats and masks the need for better detection tools and information-sharing strategies. Media coverage, for example, concentrates on reporting large-scale attacks as if the bigger the attack, the bigger the threat.[20] However, cyber incidents can be less dra-

matic, more frequent, and just as serious. The last attack suffered by the EU Commission on 23 March 2011 may have been large in scale and worth an article, but as acknowledged by Antony Gravili, the spokesman for the inter-institutional relations and administration commissioner, "the commission is frequently targeted" and it "isn't unusual" to launch an inquiry to understand better what has happened and the impact of the incident.[21] Yet most times it does not hit the headlines.

To be fair, the diversity of methods used to collect information on cyber incidents can produce widely different results. Compounded sometimes with a lack of adequate statistics from official sources, this facilitates extrapolations about the scale of the problem and the cost of cyber crimes.[22] In the UK, for example, the Department for Business, Enterprise & Regulatory Reform (BERR) conducted its own survey in 2008 on *Information Security Breaches* suffered by businesses.[23] Although the information gathered is valuable,[24] the survey is based on only "1,007 computer-assisted telephone interviews, each lasting on average 20 minutes."[25] Compared with the 2.10 million enterprises registered for European Value Added Tax (VAT) and/or Pay As You Earn (PAYE) in March 2010,[26] the sample appears small, despite specific efforts to choose businesses of different sizes and best representative of their sectors. Far more problematic in terms of methodology is the 2011 report on the *Cost of cyber crime* in the UK. It claims that cyber crime costs £27 billion to businesses and citizens. Yet, the report does not use, nor for that matter discuss, any official statistics available on cyber crime, however flawed they are, as we will see.[27] Moreover, its strong focus on espionage, in a report that is supposed to embrace all cyber crimes, raises important questions about the choice of DETICA, a private corporation used to conduct the research. DETICA is a member of the BAE Systems, one of the biggest actors of the military-industrial complex and an important contractor in the United States and in the UK.[28] Its interests may not be solely in assessing the cost of *all* cyber crimes,[29] since this company recently redeployed itself into the market of cyber security as a means to compensate for the loss induced by widespread spending cuts promoted by its main States clients.[30, 31] Given the context,[32] one would have wished that the Cabinet Office had been more transparent in its reasons, never stated, for choosing DETICA, and maybe in the objectives it sought to achieve.[33] Espionage at the national level does not represent the bulk of cyber crimes, even if the risk it represents and its correlated cost can well justify its assessment. Moreover, it may require the involvement of the military and intelligence agencies, whereas cyber crime is primarily a matter for civilians. The balance between the two is at the heart of our democracies. If there is a need to review that balance, it should be done without a terminology that makes it difficult to distinguish

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

between cyber crime, cyber terrorism, and cyber war,[34] and that facilitates, without proper analysis, the involvement of the military in matters where it used not to intervene.[35]

It is true that the technology, notably the distributed nature of the Internet, can make it difficult to clearly attribute some incidents and decide whether they are criminal, terrorist actions, or acts of war. Consequently, to affirm that "the principal difference" between cyber crime, cyber warfare, and cyber terrorism, "is in the attacker's intent"[36] is far too simplistic when many cyber-attackers cannot be identified.[37] It is also quite simplistic to attribute financial motivation only to cyber criminals since terrorists can be motivated by monetary gain in order to finance their political actions in the physical world or in cyberspace.[38, 39] An added difficulty is that a pattern of cyber incidents may not reveal itself unless information is shared between the different stakeholders. For example, taken in isolation, a bank's website being temporarily unavailable may look innocuous and not worth reporting to the competent agencies. Yet, when associated with other cyber incidents in which the victims and timeframe are similar, it may reveal a concerted effort to target a particular type of business or e-government resources, a pattern of behavior that could amount to crime (fraud, espionage) or terrorism if the motive can be established. Detection thus may depend on information being shared. Hence, the importance is on promoting best practices and common practices of detection and reporting through various means. Critical Emergency Response Teams (CERTs) and Computer Security Incident Response Teams will have to develop and cooperate even more than they do at a national level, and also at an international level.[40] It is significant that one of the latest European Network and Information Security Agency (ENISA) reports, published in February 2011, is precisely a "Good Practice Guide for Incident Management" to promote better and more harmonized analysis of incidents by CERTs. When it comes to Critical Infrastructures (CI), information sharing between the public and private sectors is even more important, with the added difficulty of devising methods for civilians and the military to collaborate in times of peace.[41]

Technical detection will also have to be combined with adequate legal reporting. When it comes to cyber crime, reliable reporting mechanisms are not always available. In the UK for example, online reporting is available only for fraud, via the Action Fraud website, and child pornography, extreme pornography, and racial (but not religious or sexual) hatred via the Internet Watch Foundation (IWF). All the other online offenses, including hacking, have to be reported the traditional way, i.e., by calling

the police or going to the police station. Email addresses are rarely available since the types of offenses to be reported are usually limited to offline behavior.[42, 43]

By contrast, since 2003, the U.S. Internet Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA), offers a *single* online platform for victims to report *all* cyber crimes. Created in 2000 for fraud only, bearing the name then of Internet Fraud Complaint Center, it justifies its extension in 2003 to all cyber crimes as a means to:

> "better reflect the broad character of such matters having an Internet, or cyber, nexus referred to the IC3, and to minimize the need for one to distinguish 'Internet Fraud' from other potentially overlapping cyber crimes."[44]

The IC3 name reflects "its expanded mission in the fight against cyber crime."[45] The effect of such a system is the immediate visibility of reported cyber crimes, with information being available through one source, rather than scattered across three platforms, as in the UK (police records, Action Fraud reports, and IWF analysis). The other advantage of a centralized and online reporting system is that it encourages reporting cyber crimes, thus reducing accordingly the "dark figure" of cyber crime. The IC3, for example, experienced a 10% decrease of complaints in 2010, but a 22% increase of complaints in 2009 compared to 2008, and in 2008 a 33.1% increase compared to 2007. Since 2000, the number of complaints went from 16,838 to 303,809 in 2010. Paradoxically, this rise confirms the severe underreporting of cyber crime and the need to continue educating and encouraging end-users to do so.[46]

Companies, especially banks, do not want to appear publicly as victims of online fraud or extortion threats. Individuals tend not to disclose the loss or damage suffered, sometimes just because they do not see the importance of reporting. They are not always aware that "[cyber crimes'] seriousness [often] lies in their globalized aggregate volume"[47] rather than in the individual amount lost by the victim. Indeed, a £30 loss for one person can mean a £3,000 minimum gain to the offender, given that scams are addressed to hundreds of thousands of people online. The "419" Nigerian scammers had perfectly understood this harnessing power of the Internet. It could even be argued that cyber criminals take advantage of the chronic underreporting of cyber crimes. Crime thrives on invisibility, but reporting can break that dynamic by exposing the threats and compiling their frequency. This is why most anti-virus software

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

companies (Cisco, F-Secure, McAffee, Sophos, Symantec) publish their reports. It is also why some nonprofit organizations set up websites to report specific behavior. These efforts are laudable; but hidden corporate agendas can bring into question the objectivity of reporting, and others may drift towards a mindset of "vigilantes."[48] It is therefore essential that countries develop proper reporting tools that allow for the collection of relevant data on cyber crimes. In that respect, the IC3 experience and evolution, similar, for example, to that of the French Internet.Signalement website, shows the way forward. Hopefully the UK, as well as any country that has not yet done so, will contemplate adopting a similar approach and create a centralized organization with a correlated reporting website. The importance of such a mechanism was highlighted indirectly when, in its 2009 report, the IC3 noticed that some complaints received were outside its remits because of jurisdictional issues. If the victims felt the need to file in these complaints, it may be because of their ignorance of the jurisdictional constraints of the IC3, but it may also be because they did not find appropriate channels in their own countries to report online cyber crimes and preferred to use the IC3 website in the hope that their complaints would be transferred to the appropriate authorities in their own countries.

Furthermore, reporting tools and derived statistics should cover all victims, whether corporations or individuals, and for individuals, whatever age they are. In the UK, the British Crime Survey (BCS) and the Offending, Crime and Justice Survey (OCJS), for example, exclude corporations. The IC3 reports do not seem to make this distinction. It is thus not surprising that in the UK, the Department for Business, Enterprise & Regulatory Reform (BERR) conducted its own survey in 2008 on Information Security Breaches suffered by businesses.[49] Nevertheless, this survey cannot be a substitute for proper reporting, given that companies increasingly use the Internet to conduct more of their business and thus are more likely to be victimized. Regarding individuals, the problem may arise from age selection. The UK OCJS draws "the sample of respondents [...] from persons aged 10–25 years,"[50] leaving aside the other half of the population that uses the Internet on a regular basis. This is the same group that is often the most vulnerable to security breaches because it is the least literate about security measures in cyberspace.[51] Since the BCS reports only online fraud, the OCJS is the only one to cover victimization of all cyber crimes. In addition, the OCJS methodology and information is a bit like having statistics about theft of mobile phones for the 10–24 year-old population, but not for those aged 25 years and over.

Finally, reporting, and by extension good knowledge of, cyber crimes depends on the use of adequate terminology and classification that reflect

the diverse range of cyber crimes. In that respect, the IC3's 79 categories for classification of cyber incidents robustly covers the different types of cyber crimes. The two UK websites for online reporting are also naturally structured to classify cyber crimes according to the offenses they cover. But this visibility of cyber crimes in the institutions' reports is not always matched in the more traditional tools on which statistics are built. For example, in the UK the 2010 Counting rules for the Crime Record Survey, which comprises the police records compiled nationally, puts all Computer Misuse Act offenses (hacking and manipulation of data) under the curious heading of "Preserved Other Fraud and Repealed Fraud Offences (Pre-Fraud Act 2006)."[52] Similarly, the BCS, which estimates the number of unreported crimes by surveying households, reports online fraud under the obscure heading of "plastic card fraud," but not any other types of cyber crime.[53] The fact that in its 2004–05 report thereafter, the BCS maintained its questions about mobile phone theft, but stopped its questions on cyber crimes introduced in its 2002–03 and 2003–04 reports,[54] demonstrates that the centrality of the Internet in our daily lives has not yet been integrated in terms of security and crime. At a time when mobile phones become mini-computers with Internet access and often no proper anti-virus software, it is rather ironic that the BCS reports the theft of those phones better than the range of online offenses they can facilitate.

This issue of appropriate terminology and classification has further ramifications in terms of the visibility of cyber crimes and the readability of statistics. The IC3 tries in its 2009 report to match the categories it uses with those of the more traditional tool of reporting crime in the U.S., the National Incident-Based Reporting System, which improved the Uniform Crime [federal] Reporting in 2003.[55] More importantly, the global nature of cyber crimes calls for a terminology that would transcend the specificities of national categories and definitions of cyber crimes. The Convention on cyber crime could be used as a canvass, with countries issuing tables of equivalence between the Convention's categories and their own. This level of integration could even go deeper and in the longer term, one could imagine an online reporting mechanism at the international level that would use the terminology of the Convention on cyber crime to classify the incidents reported. The jurisdictional issues faced by the IC3 show the need for such a mechanism. The future will tell if this suggested mechanism is only a dream. Meanwhile, the terminology issue remains valid because a global vision of cyber-crime incidents would be facilitated if reporting tools were in place to filter cyber incidents according to transversal categories. Overall, better detection tools and mechanisms coupled with better communication of information on cyber threats at the international level would defuse the hype around the threat and help governments to shape adequate responses to cyber-crime trends.

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

Understated Vulnerabilities: A Strategy of Acknowledgment

"Security is only as strong as the weakest link."[56] Although cyberspace is a "constructed virtual environment within which networked computer activity takes place,"[57] its vulnerabilities are not solely inherent in the technology. Its components, computer hardware and cables, by their tangible nature and their geographical location are also vulnerable to physical attacks or incidents. They can be damaged, often permanently, by bombing or natural events such as solar flares or earthquakes.[58] Laptops with sensitive information can be stolen or lost. For example, in 2008 UK Customs lost four CDs sent by recorded delivery on which all the relevant personal data of people claiming child benefits were engraved;[59] and in 2006 the Royal Navy lost a laptop with confidential information.[60] Those incidents gave ample opportunities for both fraud and access to military databases. Similarly, insufficient screening of the physical access of "sensitive" premises can open possibilities for accessing and transferring information that should remain confidential or secret and that can be illegally exploited. The recent Wikileaks affair illustrates this point well. The cables about the United States in Iraq and Afghanistan have been disclosed on the online platform—first of all, because a young soldier was able to copy them on CDs and DVDs which he in turn smuggled out of the room without being noticed. Wikileaks did not create the security breach; it only gave it a resounding platform. Had the basics of physical security been complied with by those in charge, and not solely by a young soldier, there might have been no Wikileaks scandal.[61] In this particular case, the hype around the dangers of Wikileaks masks a more sober reality: the failure to implement routine measures to secure physical premises where secret data could be accessed.[62] The Wikileaks scandal also reveals how undervaluing those vulnerabilities intrinsic to cyberspace creates wide-ranging risks if the vulnerabilities are exploited. Instead of being overlooked or downplayed, they should be clearly acknowledged as part of a strategy of risk prevention.

Vulnerabilities that stem from technological weaknesses of software, computers, and networks are at the root of many, if not most, security problems in cyberspace. At the network level, a recent assessment of state e-government websites in the United States reveals that "although … the sites had most of their Internet ports filtered or behind firewalls, all of them had their main IP addresses detected and their port 80/tcp open, and 61% of them also had their port 443/tcp open. These findings indicate that the sites still had a few spots vulnerable to cyber intrusions and hacker attacks because having obtained the IP address of a website, cyber

intruders know how to begin to access the server of the site," which enables them to gain vital information and ultimately launch a denial of service (DOS) attack.[63]

To limit the vulnerabilities of those websites is particularly important if they are part of the Critical Infrastructure (CI) of a country since a weakness in one could spread to another or could add to another and trigger a systemic risk. Indeed, the technological vulnerabilities of critical infrastructures need to be assessed per infrastructure (finance, energy, water), but also, and more importantly, as a whole, given "the interconnectedness of various major government services and large private sector systems."[64] It is important for the different agencies involved to collaborate to identify the weaknesses in "the point of design" and reduce the "probability that a triggering event takes place."[65] The difficulty here arises from conflicting interests in managing the vulnerabilities. The privately run sector of CI will not integrate *per se* the public good in its objectives,[66] whereas any response to cyber security for CI should put the latter at its heart. The difficulty is exacerbated by the nature of the actors involved. Traditionally it falls on governments to promote the public good, with the involvement of the military in exceptional cases, and the private sector is kept at bay. This framework runs counter to the very organization of the CI, where the private sector dominates and will not naturally contact the military. Finally, these intrinsic vulnerabilities can be aggravated by extrinsic vulnerabilities not specific to cyberspace, such as difficulties in identifying communication channels and the lack of organizational structures that are competent in dealing with cyber security. Hence, the need for strong cooperation is evident instead of superficial private-public partnerships.[67] In addition, the use of simulated threats would highlight the vulnerabilities of the CI. At the national level, the UK started the Cyber Storm Exercise in 2006 (now Cyberstorm III). At the EU level, the European Network and Information Security Agency (ENISA) coordinated the Cyber Europe exercise in November 2010 which was limited to the public sector.[68] The integration of the private sector, scheduled for the next exercise,[69] will be as crucial, if not more, given that most CI remain privately owned.

Zero-Day Vulnerabilities

The importance of private companies in cyber security extends beyond the domain of CI. They are the de facto providers of software used by everyone, whether individuals, governments, or corporations. The problem is that most companies choose to release insufficiently tested software, which leaves the door open for attacks. Private companies consider that the speed of release on the market will bring global benefits that out-

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

weigh the costs of limited security because: 1) the flaws are unlikely to be discovered, and 2) the company will have time to issue a patch. However, their analysis does not correspond to the reality of cyberspace. Vulnerabilities are discovered before being patched; and patches, however regularly they are provided, do not arrive soon enough to prevent exploitation. Those vulnerabilities are even given a name: zero-day vulnerabilities. Zero-day vulnerabilities occur "when a flaw in software code is discovered, and the code exploiting the flaw appears before a fix or patch is available."[70] Such malicious codes are increasing in severity,[71] as evidenced by the frequent patches the security companies provide retrospectively.[72] Not illegal as such, the vulnerabilities discovered are part of white and black markets and can open the door to malevolent actions.[73] In defiance of the software companies' best intentions, and often with the help of rogue ISPs, they are used to spread malware, to compromise computers, and create botnets. They are the hidden face of cyber crime and cyber attacks. Their immediate impact is not necessarily easily quantifiable. Botnets, for example, are rarely noticed by the owners of the infected computers. They can slow down the bandwidth; but other factors also contribute to that result, making their detection difficult, at least by the end-user.[74] In addition, they can be dormant or they can be used for years before being detected.[75] But if botnets were to be a measure of the software vulnerabilities' impact in cyberspace, the scale of the damage would become more visible and could not be overlooked. Indeed, botnets would not be for sale on the black market if selling them did not bring profit. If they cost each a mere U.S. $0.04,[76] for instance, then profit can only be realized if there are tens of thousands of them.[77] One security company reportedly uncovered 1.9 million infected computers that at one point had been responsible for spreading most of the spam found in cyberspace.[78, 79] In other words, the economic analysis adopted by software companies does not take into account (or not sufficiently) that the costs of non-secure software are significant, that these costs will be borne by others on the network and ultimately by themselves in clean-up operations,[80] that those others are millions of people and companies because of the very nature of the Internet, and that as a consequence, the social cost of software vulnerabilities far outweighs the companies' own individual cost in delaying release to conduct further tests.[81] The calculus, which does not imply an intention of wrongdoing, does not accurately reflect the distributed nature of the Internet. In doing so, it downplays the long-term impact of current vulnerabilities.

Of course, to fix the vulnerabilities after release is laudable; it is also commendable that those companies participate in huge clean-up operations of botnets like Microsoft did in 2010.[82] However, there is nothing more paradoxical than Microsoft (and others) spending money to

circumscribe the effects of the very vulnerabilities they contributed to create in the first place. Their efforts in damage limitation should not distract from the fact that, by their business model, they allowed enough time between the release and the patch for computers to be compromised.[83] In the long run, given the security costs, one can only wonder if these companies' current economic analysis of cyber security's costs and benefits is sustainable.

What is also surprising is that we, private citizens and governments alike, tolerate these technical vulnerabilities and their consequences as the price to pay for innovation and competition in a free market. Today, we would not tolerate a car built and then driven on our networks of roads without brakes or with a feeble braking system.[84] Why then do we accept insufficient safety measures on the information highway? It may well be that we suffer from the same tendency to overlook or downplay the real costs of the risks taken in using flawed software. Indeed, many end-users do not have up-to-date software or any security software at all. The last survey of the UK Office of National Statistics (ONS) in August 2010 revealed that 7% of Internet users among the 10 to 24-year-old population in the UK still do not have any software to protect their computer and data;[85] and that among the 93% who do have one, 7% do not update it.[86] The latter said they were deterred from updating the anti-malware protection because of the perceived technical difficulties (a staggering 33% of the 7% who did not update over the past year), a belief that the risk is too low (12%), or that it is too expensive to update (9%).[87] Those last two responses show that the risks taken when going online without updated software and the costs of doing so are calculated against the immediate impact they have on the user, ignoring the effect such behavior has on the network as a whole. As a result, the risks are unwittingly downplayed.

Enhanced education programs will certainly help reduce such behaviors from end-users,[88] but they will not tackle the problem of software vulnerabilities at its source. Companies will need incentives to release better-tested software. These could come from the stock market, as a recent study shows that shareholders react positively to investments in better IT security.[89] But it will probably also have to come from governments, both as regulators and as "large-scale purchasers." Indeed, as users, governments can influence the market.[90] Some institutions, for example, decided to switch from Windows to Linux as a means to lower the costs.[91] They could take similar decisions, buying more secure software, if improvement in security and a subsequent decrease in costs were demonstrated. As increased users of Web 2.0 technologies, they may also push for better security. Indeed, the very success of Web 2.0 technology, which rests on its ability to promote sharing of information among users, is also

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

its downside. The technology encourages users to add links and click on links whose noxiousness will not be apparent and so far are rarely checked for malware.[92] The cascading effects are an increased propagation of viruses and worms on platforms such as Facebook, MySpace, Twitter, and Bebo. In an effort to woo citizens, big institutions such as the EU Parliament more frequently use the opportunities offered by social networking websites. However, there might come a point when they will be more concerned about the risks and thus more demanding about the security of the technology used.

As regulators, governments could also intervene to require changes. Yet issues arise regarding the principle and modalities of such intervention. Ideologically, Western governments, especially the United States, have been reluctant to intervene in the private sector.[93] It is only when vulnerabilities become a threat to public order, such as when spam significantly slows down Internet traffic, have governments decided to intervene. Moreover, when they do, they tend to criminalize the consequences rather than dealing with the causes, which is not necessarily an efficient approach. For spam, the United States and the EU legislated massively against spam in 2003–2004, but the decrease in spam noticed in 2004–2005 seemed not to originate from the legislation. Rather, the decrease was the result of technological change, in which the Internet Service Providers (ISP) rerouted spam emails to filter them.[94] In other words, governments may have been better inspired to regulate ISPs than to criminalize spam. This involvement of the ISPs is at the heart of some countries' policies to tackle spam.[95] For example, in 2005 the Australian Communication and Media Authority (ACMA) developed the Australian Internet Security Initiative (AISI). The AISI collects data of compromised computers and passes the information daily to the participating ISPs. The latter in turn warn their customers and advise them on how to fix the compromised machine, constraining their Internet connectivity if necessary and possible.[96]

Restricting access to the Internet may raise concerns for some, given its centrality in our lives, but nobody objects to a driver being temporarily forbidden to drive should his or her car fail the yearly road test and not be repaired.[97] So what can governments do to ensure that every user updates his or her software on a regular basis? Rather than presenting anti-spam regulations, the government could develop policies to tackle the immediate consequences of software vulnerabilities.[98] The indirect impact of such an initiative could be significant; for example, users could stop buying some IT products if their vulnerabilities lead to successive bans by the ISPs because of the inconvenience of being banned even for a limited period each time. Consequently, software companies would have to dras-

tically limit the vulnerabilities of their products if they want to keep their customers and remain competitive. In other words, they will be forced to change their economic analysis of the costs and benefits of releasing insufficiently tested software. This indirect way of fighting vulnerabilities would certainly be better than the policy of ISPs increasing their bandwidth in order to cope with the slowdowns botnets traffic creates. It will also allow for the high bandwidth used by some institutions, such as universities, to be used fully rather than for unwillingly hiding botnets.[99] In the long term, governments need to recognize the real costs of software vulnerabilities and take action rather than overlook the phenomenon.[100] Such a strategy would reduce cyber crime and save money that could be spent in education programs or in the fight against cyber threats.

Conclusion

One expert has opined that "at the dawn of the twenty-first century, the overwhelming challenge that confronts Western policymakers is the management of diverse, amorphous, and qualitative security risks, rather than the fixed, quantifiable threats of yesteryear."[101] Cyber threats, whether emanating from crime, terrorism, or war are extremely diverse. Their patterns are not always easy to sketch, given the difficulties of detecting cyber incidents, the complexity in coordinating the collection of relevant data at national and international levels, and the shortcomings of reporting mechanisms for cyber crime in some countries, like the UK. Our knowledge of those variables is often too unreliable and incomplete and therefore needs to be drastically improved. We will then avoid unnecessary media hype, as well as potentially hidden agendas in reports on cyber threats. Moreover, cyber threats should not be viewed as the only risks to security in cyberspace. Vulnerabilities of physical premises and of software constitute an important element of cyber risks. Particular attention should be given to the latter types. Although not illegal in themselves, software vulnerabilities open windows of opportunity for malevolent actors willing to exploit them.

We may have switched to the Internet being the "village" square when it comes to freedom of expression, but we have more difficulties in conceiving of the Internet as the common space where illegal activities also flourish and for which we—governments, individuals, and companies—are all responsible. This is what Beck calls the "solidarity of living things that affects everyone and everything equally in the threat." A *Risk Society* underlines that to resist recognition of risks, wittingly or unwittingly, is one way of waiving responsibility. Because cyberspace is naturally a network, all users will ultimately suffer. For Beck, society must embrace and

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

promote knowledge by self-reflection. This starts by elaborating methods and methodologies to record and report incidents in order to understand them, but the ultimate challenge will be to know what risks we accept in a democracy, including those that dissent brings.

About the Author

Dr. Audrey Guinchard, Senior Lecturer in Law (2009–Present), joined the University of Essex (UK) in October 2000 and is the co-director of the double degree LLB English and French Laws with Master 1/Maîtrise. She has a Licence en droit, an LL.M., and a Ph.D. in criminal law from the University of Jean Moulin (Lyon, France). Her current research focuses on crime and the virtual world as a starting point for a broader perspective on criminal law's ability to adapt to new technologies. In 2010, she was a visiting fellow at the Centre for Research in Arts, Social Sciences and Humanities (CRASSH) in Cambridge as part of the program on The Future University. Bringing a comparative law perspective to bear on criminal law issues, she published notably on hate crimes and on the concept of criminal charges regarding financial services, both in French and in English.

References

1 The Cabinet Office, "The Cost of Cybercrime," 14.

2 Ulrich Beck, *Risk Society: Towards a New Modernity* (London: SAGE, 1992), 20. The first edition in German dates from 1986.

3 Ibid., 23, 32.

4 Ibid., 77–78.

5 Peter Sommer and Ian Brown, "Reducing Systemic Cybersecurity Risk," Contribution to the OECD project Future "Global Shocks," 2011, available at: *http://www.oecd.org/dataoecd/57/44/46889922.pdf*.

6 See David Wall, *Cybercrime. The Transformation of Crime in the Information Age* (Cambridge: Polity, 2007), 12–23.

7 Sommer and Brown, 10.

8 Ibid, 6.

9 World Economic Forum, "Global Risks 2011: Sixth edition," 2011, 36, available at: *http://riskreport.weforum.org/*.

10 HM Government, "A strong Britain in an age of uncertainty: the national security strategy" (London: the Stationery Office, 2010), 29.

11 The Cabinet Office, "The Cost of Cybercrime," 2011, 1, available at: *http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime*. The cost of cybercrime for the UK alone is estimated at £27 billion per annum, about U.S. $43 billion.

12 Word Economic Forum, "Global Risks 2011," 36.

13 "'Serious cyber attack on EU bodies before summit," *BBC News*, 23 March 2011, available at: *http://www.bbc.co.uk/news/world-europe-12840941*.

14 Susan Brenner, *Cyberthreats. The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), 9; Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52 (2011), forthcoming, available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1670330*, 18–29.

15 Beck, *Risk Society*, 23.

16 Ibid., 77–79.

17 Following the Estonian incidents, NATO created the Cooperative Cyber Defence Centre of Excellence (CCDCOE), which has operated out of Tallinn, Estonia since August 2008.

18 Stein Schjolberg and Solange Ghernaouti-Helie, "A Global Treaty on Cybersecurity and Cybercrime," 2nd ed. 2011, 45, available at: *http://www.cybercrimelaw.net/Cybercrimelaw.html*.

19 The Cabinet Office, "The Cost of Cybercrime," 14.

20 ENISA, "Botnets: 10 Tough Questions" 2011, 5, available at: *http://www.enisa.europa.eu/act/res/botnets/botnets-10-tough-questions*. For recent examples, see EU commission and carbon emission trade, Euractiv, "Cyber attack on European Commission reported," March 24, 2011, available at: *http://www.euractiv.com/en/future-eu/*; Murray Wardrop and Duncan Gardham, "Cyber attack threat 'could be next Pearl Harbor,'" *The Telegraph*, October 18, 2010, available at: *http://tinyurl.com/389mnox (www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8070236/Cyber-attack-threat-could-be-next-Pearl-Harbor.html)*.

21 "'Serious' cyber attack on EU bodies before summit," *BBC News*, March 23, 2011, available at: *http://www.bbc.co.uk/news/world-europe-12840941*.

22 ENISA, "Botnets: 10 Tough Questions," 4.

23 Technical Report (Survey), "2008 Information Security Breaches," *Department for Business Enterprise & Regulatory Reform*, available at: *http://www.bis.gov.uk/files/file45714.pdf*.

24 It is also the ninth one, which gives an added perspective to the findings. Ibid., 1.

25 Ibid., 4.

26 (UK) Office for National Statistics (ONS), September 27, 2010, available at: *http://www.statistics.gov.uk/cci/nugget.asp?id=1238*.

27 The ONS is cited only about the Research & Development figures, *Technical Report*, 14 fn., 45–46. The police records are not referred to. The MET has not been consulted, either.

DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

28 Loreen Thompson, "British-Based BAE Systems Shifts U.S. Strategy," *Forbes*, 9 November 2010, available at: *http://tinyurl.com/6hokwhz (blogs.forbes.com/beltway/2010/11/09/british-based-bae-systems-shifts-u-s-strategy/)*.

29 Brown, on systemic. It is certainly the opinion of Peter Sommer who wrote a report for the OECD with Ian cyberrisks (supra), in Kathleen Hall, "Government's £27bn cyber crime figure slammed as 'sales promotion exercise,'" February18, 2011, available at: *http://tinyurl.com/5tz58x3 (www.computerweekly.com/Articles/2011/02/18/245505/Governments-16327bn-cyber-crime-figure-slammed-as-39sales-promotion.htm)*. Similarly, Richard Clayton from University of Cambridge, and Tyler Moor, Harvard University, in Tom Espiner, "Cyber crime cost estimate is 'sales exercise,' say experts," February 18, 2011, available at: *http://tinyurl.com/66q8jbo (www.zdnet.co.uk/news/security-threats/2011/02/18/cybercrime-cost-estimate-is-sales-exercise-say-experts-40091866/?s_cid=164)*.

30 Andrea Shalal-Esa, "BAE looks to draw government cyber work," *Reuters*, March 26, 2010, available at: *http://tinyurl.com/66y503p (www.reuters.com/article/2010/05/26/us-bae-cyber-idUSTRE64O6V720100526?feedType=RSS)*; Szu Ping Chan, "BAE Systems aims to beef up anti-fraud arm with Norkom offer," *The Telegraph*, March 30, 2011, available at: *http://tinyurl.com/4np7y8s (www.telegraph.co.uk/finance/newsbysector/industry/defence/8259050/BAE-Systems-aims-to-beef-up-anti-fraud-arm-with-Norkom-offer.html)*.

31 Sarah Arnott, "BAE warns of lower sales as UK and US cut spending," *The Independent*, February 18, 2011, available at: *http://tinyurl.com/6h7nrmw (www.independent.co.uk/news/business/news/bae-warns-of-lower-sales-as-uk-and-us-cut-spending-2218325.html)*.

32 Bearing in mind that BAE has been subjected to a serious Fraud Office's investigation for over a year. It has not been prosecuted, but it is widely accepted that the charges were dropped upon political pressure. Tim Webb, "BAE Systems hires Britain's former envoy to Saudi Arabia," *The Guardian*, February 18, 2011, available at: *http://www.guardian.co.uk/business/2011/feb/18/envoy-saudi-bae-systems*.

33 On the danger of possible hidden agendas in the same military-industrial domain, see HBGary Federal, which positioned itself against Wikileaks, an affair that involves failure of the military to secure access to its databases, but whose security measures were so weak that Anonymous was able to hack without too much difficulty into important email accounts. Peter Bright, "Anonymous speaks: the inside story of the HBGary hack," *ArsTechnica*, February 15, 2010, available at: *http://tinyurl.com/4gesrcj (arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/2)*.

34 Sommer and Brown, 6, 10, 57; Schjolberg and Ghernaouti-Helie, 45; Brian Price, "RSA conference: the Fog of Cyber-War," E-Week.com, February 17, 2011, available at: *http://tinyurl.com/5vqhjco (www.eweek.com/c/a/Security/RSA-Conference-The-Fog-of-CyberWar-521201/?kc=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+RSS%252Feweeksecurity+%2528eWEEK+Security%2529)*.

35 On the militarization of terrorism, Duncan B. Hollis, "Why States Need an International Law for Information Operations," 11, Lewis & Clark L. Rev. (2007) 1023, 1026–28. On militarization in general, Benoît Dupont "Entre militarization et judiciarisation des politiques de cyber-sécurité," 22 December 2010 (video), available at: *http://www.benoitdupont.net/node/106*. For an exploration of the collaboration between civilians and the military at time of cyber war, Susan Brenner and Leo Clarke, "Civilians in Cyberwarfare: Conscripts," 2011, available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1650743*.

36 Cabinet Office, "The Cost of Cybercrime," 6.

37 Brenner, *Cyberthreats*, 9; Hollis, "An e-SOS," 4.

38 Cabinet Office, "The Cost of Cybercrime," 6.

39 See Alexandra Frean, "'Financial terrorists' pose grave risks to US," *The Times*, 2 February 2011, 9.

40 Bauer and Van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options," *Telecommunications Policy* 33 (2009), 706, 716–17; Sommer and Brown, 75; ENISA, "Botnets: 10 Tough Questions," 15; ENISA, "Botnets: Detection, Measurement, Disinfection & Defence," 2010, 95.

41 Brenner, *Cyberthreats*, 251–279; Hollis, "An e-SOS," fn 129.

42 See, for example: *http://www.direct.gov.uk/en/Diol1/DoItOnline/DG_4019457*.

43 The MET accepts online reporting for theft, criminal damage, and hate crimes. Given that racial hate-crimes fall into the remit of the IWF, and that the MET forbids reporting crimes of sexual nature, nearly no cyber crime can be reported online to the MET; see: *https://online.met.police.uk/*.

44 Internet Crime Complaint Center, available at: *http://www.ic3.gov/about/default.aspx*.

45 IC3 Report 2010, 5, available at: *http://www.ic3.gov/media/annualreports.aspx*.

46 The findings can probably be extrapolated to other countries. See, for example, the Home Office Statistical Bulletin of December 2010 (UK) that acknowledges underreporting (p. 93), available at: *http://tinyurl.com/5u2hgo8 (www.cjp.org.uk/publications/archive/home-office-statistical-bulletin-crime-in-england-and-wales-2009-10-15-07-2010/).*

47 Wall, *Cybercrime*, 19.

48 Bauer and Van Eeten, "Cybersecurity," 712.

49 Technical Report 2008, 4.

50 Economic and Social Data Service (UK), *Guide to Offending, Crime and Justice Survey*, available at: *http://www.esds.ac.uk/support/e33360.asp*.

51 Kim-Kwang Raymond Choo, "High tech criminal threats to the national information infrastructure," *Information Security Technical Report* 10 (2009): 7.

52 "Counting Rules for Fraud and Forgery," *Home Office (UK)*, 2010, 13–14, 17, available at: *http://tinyurl.com/3vnqxs7 (www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/counting-rules/count-fraudforgery).*

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

53 Economic and Social Data Service (UK), British Crime Survey List of Datasets available at: *http://www.esds.ac.uk/findingData/bcrs.asp*.

54 Jonathan Allen, Sarah Forrest, Michael Levi, Hannah Roy, Michael Sutton, Debbie Wilson, "Fraud and technology crimes: findings from the *2002/03 British Crime Survey* and *2003 Offending, Crime and Justice Survey*," Home Office Online Report 34/05 (London: Home Office, 2005); Debbie Wilson, Alison Patterson, Gemma Powell, and Rachelle Hembury, "Fraud and technology crimes; Findings from the *2003/04 British Crime Survey*, the *2004 Offending, Crime and Justice Survey*, and administrative sources," Home Office Online Report 09/06 (London: Home Office, 2006).

55 IC3 Annual Report 2009, 16, available at: *http://www.ic3.gov/media/annualreports.aspx*.

56 Choo, "High Tech Criminal Threats," 6.

57 Wall, *Cybercrime*, 221. See also: White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" (2009), 1, available at: *http://tinyurl.com/nzdbjw (www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)*.

58 Sommer and Brown, 26–27.

59 "Court case data CDs lost in post," *BBC News*, January 23, 2008, available at: *http://news.bbc.co.uk/2/hi/uk_news/politics/7204399.stm*.

60 Ibid. Regarding businesses, the BERR considers that 22% of businesses are victims of physical theft, *Information Security Breaches Survey*, 24.

61 David Leigh and Luke Harding, "WikiLeaks: From Wales to a US jail, via Iraq, the story of Bradley Manning," *The Guardian* (London), February 1, 2011, available at: *http://www.guardian.co.uk/world/2011/feb/01/bradley-manning-wikileaks*; Ray McGovern, ex-CIA agent, "Ex-CIA agent openly supporting Assange," video-interview, TVNZ, December 10, 2010, available at: *http://tinyurl.com/6602d6d (tvnz.co.nz/world-news/ex-cia-agent-openly-supporting-assange-3962462)*.

62 To be noted also that, as far as we know, the security breach did not result in leaks to foreign intelligence agencies, but in disclosure of problematic behaviors of the U.S. army regarding compliance with basic human rights.

63 Jensen J. Zhao and Sherry Y. Zhao, "Opportunities and threats: A security assessment of state e-government websites," *Government Information Quarterly* 27 (2010), 49, 54.

64 Sommer and Brown, 22.

65 Ibid., 39.

66 Ibid., 66; Bauer and Van Eeten, "Cybersecurity," 714.

67 Sommer and Brown, 74, 83–84.

68 ENISA, FAQ Cyber Europe 2010 Final, available at: *http://tinyurl.com/5w2j88s (www.enisa.europa.eu/media/news-items/faqs-cyber-europe-2010-final/view?searchterm=cyber%20europe)*.

69 ENISA, Press Release, "Interim findings of Cyber Europe 2010," November 10, 2010, available at: *http://tinyurl.com/5u32atn (www.enisa.europa.eu/media/press-releases/cyber-europe-2010-a-successful-2019cyber-stress-test2019-for-europe/?searchterm=cyber%20europe).*

70 SANS 2009 report, available at: *http://www.sans.org/top-cyber-security-risks/zero-day.php*.

71 Choo, "High Tech Criminal Threats," 3, para. 1.2.2.

72 See the monthly bulletin of the U.S. CERT in February 2011 for a list of recently patched vulnerabilities in mainstream software (anti-virus, Adobe for pdf, RealPlayer, Microsoft for IE, Word, Exchange, Google for Chrome), available at: *http://www.us-cert.gov/reading_room/*. Similarly, see: "Top Cyber Security Risks - Application vs. Operating System Patching," SANS, September 2009, available at: *http://www.sans.org/top-cyber-security-risks/patching.php*.

73 Ian Brown, Lilian Edwards and Chris Marsden, "Information Security and Cybercrime," in *Law and the Internet*, eds. Lilian Edwards and Charlotte Waelde (Oxford: Hart Publishing Ltd, 2009), 687–689.

74 ISPs are in a better position to do so, provided they are not at the hands of malevolent actors.

75 For five years, John Leyden, "RUSTOCK TAKEDOWN: How the world's worst botnet was KO'd," *The Register*, March 23, 2011, available at: *http://www.theregister.co.uk/2011/03/23/rustock_takedown_analysis/*.

76 Sommer and Brown, 25.

77 For an estimate in 2005 of profits made, see Wall, *Cybercrime*, 154.

78 Choo, "High Tech Criminal Threats," 4, 1st column.

79 Leyden, "Rustock Takedown."

80 Bauer and Van Eeten, "Cybersecurity," 707, 714.

81 Ibid., 710, 714, 717.

82 Leyden, "Rustock Takedown," available at: *http://www.bbc.co.uk/news/technology-11531657*.

83 On the race to stay ahead of the security patch, Wall, *Cybercrime*, 154.

84 Benoît Dupont developed extensively the analogy in "Entre militarization." See also: White House, "Cyberspace Policy Review," 14.

85 ONS, *Internet Access 2010. Households and Individuals*, 7, available at: *http://www.statistics.gov.uk/pdfdir/iahi0810.pdf*.

86 Ibid., Table 17.

87 Ibid., Table 18.

88 Notably, E. Kritzinger and S.H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Computers & Security* 29 (2010), 840.

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5

89 Sangmi Chai, Minkyun Kim, and H. Raghav Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decision Support Systems* 50 (2011) 651, 659.

90 Sommer and Brown, 64–65, 82.

91 For the French Assemblée Nationale (Lower Chamber of the French Parliament) in 2007, Christophe Guillemin, "Linux à l'Assemblée nationale: un premier bilan positif," *ZDNet.fr (France)*, July 1, 2008, available at: *http://tinyurl.com/6xovwlk (www.zdnet.fr/actualites/linux-a-l-assemblee-nationale-un-premier-bilan-positif-39382082.htm).*

92 Benoît Dupont, Pierre-Eric Lavoie, and Francis Fortin, "Les crimes sur le web 2.0. Une recherche exploratoire," *Note de recherché* (2010), 8, available at: *http://tinyurl.com/66ngop2 (www.benoitdupont.net/sites/www.benoitdupont.net/files/Dupont%20Lavoie%20Fortin%20crimes%20web%202%200.pdf).*

93 Sommer and Brown, 62; Bauer and Van Eeten, 715–717.

94 Wall, *Cybercrime*, 194–196.

95 ENISA, "Botnets: Detection," 96–99.

96 Ibid., 98. See also: Australian Communications and Media Authority (ACMA), available at: *http://www.acma.gov.au/WEB/STANDARD/pc=PC_310311*.

97 This does not mean there are not other legal issues, ENISA, "Botnets: Detection," 96–99.

98 Brown, Edwards, and Marsden, "Information Security," 690–691, in particular footnote # 61; Bauer and Van Eeten, "Cybersecurity," 714–716; van Eeten, M. *et al.* (2010), "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data," *OECD Science, Technology and Industry Working Papers*, OECD Publishing, 2010/5, available at: *http://dx.doi.org/10.1787/5km4k7m9n3vj-en*; B.B. Gupta, R.C. Joshi, and Manoj Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," *Information Security Journal: A Global Perspective* 18 (2009), 224.

99 Choo, "High Tech Criminal Threats," 4.

100 Despite the recommendations of the House of Lords Science and Technology Committee in 2007, the UK government rejected most of them, HL Paper 165, Cm 7234 (London: The Stationery Office, 2007). Conversely, see: White House, "Cyberspace Policy Review," and the policies of Germany, Australia, and South Korea explained in ENISA, "Botnets: Detection," 97–99.

101 M.J. Williams, "(In) Security Studies, Reflexive Modernization and the Risk Society," *Cooperation and Conflict* 43 (2008), 57, 58.

Journal of Strategic Security

https://scholarcommons.usf.edu/jss/vol4/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.5