CYBERSECURITY RISKS: ARE THEY INFLATED?

Petr Chrapavy[†]

ABSTRACT

With various views being posed on cybersecurity, this paper examines the proposition that cybersecurity risks are inflated. Due to the complexity of the cybersecurity environment, the risks will be dichotomised into two distinct categories—those posed by cybercrime, and those classified as cyber-warfare. In relation to cyber-crime, the paper examines the rise of cyber-crime, its costs, and the views of these factors by "alarmists" and "sceptics." In relation to cyber-war, the paper sets aside the emotive issue of the consequences and focuses on the likelihood of a catastrophic attack. The paper concludes that the risk of cyber-crime is real, but the sometimes mooted existential threat poses by cyber-war is inflated. The paper argues that it is important for cyber defences to improve in line with the risks, and to do this, researchers need to work across both categories of cybersecurity.

Keywords: cybersecurity, cyber risk, cyber defence, cyber-war, cyber-warfare, cyber-terrorism, hacking

INTRODUCTION

In her summary of the most notorious cyber-attacks in 2015, Zetter (2015) points out a worrying trend in the unrelenting rise of cybercrime: "every year hack attacks seem to get worse—whether in their sophistication, breadth, or sheer brazenness" (para. 1). She illustrates this by listing the most successful attacks against high-profile targets, which ranged from the Internet's leading adultery website (Ashley Madison), defensive cybersecurity firm (Moscow-based Kaspersky Lab), offensive cybersecurity firm (Italy-based Hacking Team), to US Federal Office of Personal Management. These views are not isolated. But differing opinions are published regularly in the press and academic journals. Therefore, it is timely to review the positions taken by these authors to see if cybersecurity risks are inflated.

[†] Corresponding author: petr@riotsolutions.com.au

Of concern was the revelation that: "Juniper Networks discovered two unauthorised backdoors in its NetScreen firewalls, one of which would allow the unknown hackers to decrypt protected traffic passing through the firm's VPN/firewall" (para. 1). These devices are used worldwide by both private organisations and government agencies; thus their compromise would have resulted in an unauthorised access to some extremely sensitive information. According to Zetter (2015), what is of particular concern is that the prevailing view in the security community is that a sophisticated adversary is behind at least one of the backdoors; potentially a nation-state (para. 27).

The evidence indicates that, in general, cybercrime has been steadily rising and—despite some notable local and global law enforcement successes, shows no sign of abating (ACSC, 2015). In their first unclassified report, the Australian Cyber Security Centre (ACSC, 2015) claims "the cyber threat to Australian organisations is undeniable, unrelenting and continues to grow" (p. 2). Furthermore, the report states: "if an organisation is connected to the Internet, it is vulnerable. The incidents in the public eye are just the tip of the iceberg" (p. 3). Its key predictions for 2015, the ACSC envisaged a continual increase in the sophistication of cyber-attacks and in the number of "state and cyber criminals with capability" (p. 24). Overall, while the report highlights the high levels of risks, it also includes a warning about possible bias in statistics compiled by the Australian Signals Directorate (ASD) and Computer Emergency Response Team (CERT) Australia. While the ACSC takes cyber-attacks very seriously and considers that "destructive cyber-attacks could be considered equivalent to an armed attack, and therefore, an act of war" (p. 9), it considers such a scenario "unlikely outside a period of significant heightened tension or escalation to conflict with another country" (p. 9).

Only three months after the ACSC report was published there was a cyber-attack on the Bureau of Meteorology (BOM), which can be taken as a confirmation of the ACSC's prediction. The BOM systems might have to be entirely replaced (Uhlmann, 2015, para. 4), as their complexity, customisation and interconnectivity dependencies mean they cannot simply be shut-down in order to be cleaned. Therefore, the estimates of damage run into hundreds of millions of dollars, supporting the assertion that the risks of targeted cyber-attacks are not exaggerated.

In 2015, the European Cybercrime Centre (EC3) at Europol published *2014 Internet Organised Crime Threat Assessment* that stated: "In general, cybercrime is increasing in scale and impact … trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage" (Europol, 2014, para. 6). The current report for 2015 shows further evidence that cybercrime is not only continuing to increase, but it is becoming more aggressive (Europol, 2015).

While attackers were previously content with stealth approaches, avoiding confrontation where possible, the analysis points to a growing trend for "direct, confrontational contact between the criminal and the victim, where the victim is put under considerable pressure to comply with the perpetrator's demands" (Europol, 2015: 62). This suggests risks posed by cyber adversaries, especially organised crime, are not overstated. Moreover, due to the continuing commoditisation of cybercrime methods and techniques, specialised software products and services that are easily accessible to unskilled, entry-level cybercriminals, enable them to "launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits" (Europol, 2015: 7).

There is a mature, competitive market for crime-as-a-service products and services, and this creates a force multiplier for many forms of cybercrime (more so in the realm of cyber-dependent crimes than cyber-enabled crimes). Services such as the so-called bulletproof hosting, spam bots, and counter-antivirus, among others, are crucial to enablement of some cybercriminal offences, while not being a direct subject of criminal complaint (Europol, 2015: 63).

In 2015, there was also a marked increase in distributed denial of service (DDoS) attacks, as reported by Akamai Technologies (2015), one of the global content delivery network providers whose platform "regularly transmits between 15%–30% of all Internet traffic" (p. 60). These attacks were sometimes followed by extortion attempts, particularly when the financial and telecommunications industries were targeted (p. 24). The data for the third quarter of 2015 showed increases in attack trends for DDoS metrics when compared to the same quarter of 2014 (a 180% increase in total attacks). One type of DDoS attack particularly stood out: there had been a 462% increase in reflection attacks (p. 5). These utilise (abuse) computing resources of a potentially legitimate third party component to attack the intended victim, which allows the attackers to hide their real identity.

CYBERCRIME COSTS

Data from sources such as the European Union's law enforcement agency (Europol, 2015), Australian Cyber Security Centre (ACSC, 2015), and one of the first studies to estimate the extend of cybercrime revenue (Michigan State University, 2016) indicate that cybercriminals are certainly making vast profits. However, it needs to be noted that accurate estimates of the costs of cybercrime cannot be determined, mainly due to under-reporting and under-recording. Nonetheless, these data show that the economic damages can be substantial. This was also evident in the Ponemon Institute (2015) study of the costs incurred due to cybercrime. The report found that there were notable differences in the total costs of cybercrime among the 252 companies from seven countries that took part in the study. The report's summary stated that, "the US sample reports the highest total average cost at $15 million and the Russian sample reports the lowest total average cost at $2.4 million" (p. 2).

Even though the report was a sponsored investigation by Hewlett Packard Enterprise, and not a "independent" academic report, it nevertheless can be seen as a good indicator of the magnitude of the problem. Likewise, Australian data showed the cost of cybercrime was $3.4 million, though this amount was calculated two months prior to the successful attack against the Bureau of Meteorology systems, which was estimated to have caused hundreds of millions of dollars in damages (Uhlmann, 2015).

Under-reporting and under-recording are allied to the issue of cybercriminal operations going undetected and continuing to operate for years. One example is that of the botnet dubbed *Ponmocup*, which was one of the largest. According to van Dantzig et al. (2015, p.2, para. 2) this botnet was active for "nine consecutive years, [and was] also one of the longest running. Ponmocup [was] rarely noticed though, as the operators take care to keep it operating under the radar." Van Dantzig et al, (2015) found that the botnet's operators used techniques specifically designed to avoid detection by anti-virus software, and both automatic and manual analysis. The report's authors found that "it has infected a cumulative total of more than 15 million unique victims since 2009. At its peak, in July 2011, the botnet consisted of 2.4 million infected systems" (p. 2). While the exact amount of money earned by the botnet operators is not yet known, the authors suggest it is a successful multi-million-dollar business.

ALARMISTS

While security vulnerabilities seem to manifest everywhere on the Internet, it is the most extreme scenarios that are often cited in the media. This is illustrated in the following example from an article by Iyer (2015, para. 1):

> With the increase in hacking these days, right from infecting a computer to remotely hacking a car in motion, one may wonder what would happen if a hacker decides to compromise your bionic arm, your pacemaker, or maybe your brain implant. Thanks to some students at the University of South Alabama, we have an answer: You die!

The article refers to attempts by a group of students to exploit security vulnerabilities in a sophisticated what is termed a *wireless patient simulator* product called iStan. Many hospitals use this system "to show and explain medical school students how to carry out procedures without killing people" (Iver, 2015: para. 4). Within just a few hours the students were able to gain access to most functions of the device and demonstrate that it was susceptible to various types of cybersecurity attacks. According to the director of the simulations program, Mike Jacobs, the students were able to speed-up and slow-down the simulator's heart rate via its inbuilt pacemaker, and "if it had a defibrillator, which most do, we could have shocked it repeatedly. If it was the intent, we could definitely cause harm to the patient," Jacobs said. "It's not just a pacemaker, we could do it with an insulin pump, a number of things that would cause life-threatening injuries or death" (Iver, 2015: para. 8).

Medical devices are just one type of a spectrum of devices that are being connected to the Internet and now known as the Internet of Things (IoT), or the Internet of Everything (IoE). McAfee Labs (2015) claimed that these sensors, wearables, and other devices exposed themselves, their users, and potentially the entire system they are part of, to new cybersecurity vulnerabilities. Additionally, the report warned "every new product that connects to the Internet faces the full force of today's [risks], and we have a long way to go to keep up with the speed and complexity of attacks" (p. 21).

From a law enforcement point of view, while the IoT is seen as an emerging risk environment, Europol (2015) stated, "the rising number of smart 'things,' including smart homes, smart cars, smart medical devices and even smart weapons are a clear indication of its adoption" (p. 54). It follows that this situation will

extend to challenges for law enforcers because the IoT provides new opportunities for cybercrime (p. 8).

Technologies in the rapidly evolving Smart Home market get media attention, and in general, seem to be susceptible to cybersecurity vulnerabilities and/or exposing users to issues involving breach of privacy. The range of risks is also of concern, as Howard (2015) pointed out: "what if your home is hacked and no longer recognises you? What if a computer virus deactivates your home security system? What if a denial-of-service attack renders useless thousands of smart homes housing our aged?" (p. 13, para. 7). He also draws attention to less frequently mentioned risks of false positives that could be triggered by an attacker or by system malfunction.

Some wearable devices allow the elderly and disabled to push a button that summons medical help. But in the smart home these could be further enhanced so they can trigger other types of alarms for assistance when the sensor determines a need—potentially without the monitored person having to call for help. In case of a false alarm, when this occurs, the medical emergency responders may simply waste a bit of time. However, "when it happens at a societal level," Howard points out that if "dozens, hundreds, or even thousands of these false alarms are being triggered—the systems in place for initial public safety and health responses may be overwhelmed" (para. 9) and will fail with consequential effects.

Coming back to examples of extreme scenarios in media headlines, Rozenfeld (2015) opens the online article with a somewhat alarmist statement that cybersecurity experts consider: "a widespread cyberattack is likely to occur in the next ten years, possibly causing the theft of tens of billions of dollars' harm to a nation's security and capacity to defend itself, or a significant loss of life" (para. 1). However, the article lacks depth of analysis as it only cites the Pew Research Center survey's results that showed more than 60% of the 1,642 participating experts *thought* such attack was likely, and nearly 40% gave the chance of a major damage from a cyber-attack a low likelihood rating. This split does not indicate general consensus and lacks an evidence base for drawing such conclusions. Besides, there were those experts voicing their concern that the risks are being exaggerated to generate an atmosphere of fear, accordingly this would have the potential to generate profits for those enterprises selling cybersecurity protection services and software products.

SCEPTICS

When considering the likelihood of cybersecurity risks, one needs to be aware of potential bias in reports published by cybersecurity vendors. Yet, some vendors do critically evaluate data and avoid alarmist or sensational tones in their reports. For example, where McAfee (now a subsidiary of Intel Corporation) discuss threats to critical infrastructure, in their *2016 Threats Predictions* report (McAfee Labs, 2015, p. 37):

> If we believe the press reports coming from some security vendors, our future has become considerably more uncertain—with targeted attacks aimed at our critical infrastructure. Many of those highly publicised reports came after the 2010 attack by Stuxnet, which caused significant physical damage. However, it took years before a second successful attack against critical infrastructure appeared in the news. With only two publicly recognised instances since 2009, our 2016 predictions about critical infrastructure attacks must acknowledge that they are low-incident, but high-impact events.

The risk of devastating attacks on national infrastructure is discussed by Leyden (2015). He argues cyber-attackers "have never been credited with taking down a power grid. States themselves, which have a lot more resources behind them, have only been credited with a handful of full-on, serious enterprise attacks" (para. 20). He adds that when it comes to the risk of cyber-terror attacks against national power grids, in reality, small animals are more of a danger. He states, "squirrels have more luck sabotaging electrical systems" (para. 22) when compared to hackers because they often chew through electrical cables. He refers to data on *CyberSquirrel1.com* "a site that logs these types of incidents, reckons the rodents have been responsible for 505 such operations. Birds have reached 141, and raccoons 31. Humanity has clocked up just one" (para. 23). Leyden uses this illustration as an overstatement of worst-case scenario risks in response to the UK government's increased spending on prevention measures. In terms of attacks by rogue states and terror groups, Leyden 2015) argues "there's no evidence they have the capability and even their motivation to attack systems online is at least open to question" (para. 24).

Even the 23 December 2015 attack that incapacitated parts of the Ukrainian electrical grid for several hours (Goodin, 2016), which was highly likely to have been caused by a malware infection (Lee, Assante & Conway, 2016: 8), should be considered a statistical outlier. According to the US Department of Homeland

Security, "The threat of a damaging or disruptive cyber-attack against the US energy sector is low." DHS judged that "advanced persistent threat (APT) nation-state cyber actors are targeting US energy sector enterprise networks primarily to conduct cyber *espionage* [not sabotage]" (U.S. DHS, 2016: 2).

CYBERWAR

Discussions about cyber-attacks against national critical infrastructure and their associated activities are termed *cyberwar* (sometimes synonymously referred as *cyber-terrorism*). Schneier (2010) argues cybersecurity risks posed by a wide range of perpetrators had been mislabelled as cyberwar by the media, and that instead, those attacks were probably committed by citizen activists or organised crime. He stated that "we're not fighting a cyberwar now, and the risks of a cyberwar are no greater than the risks of a ground invasion" (para. 16). Tucker's (2015) take on the cyberwar rhetoric echoes Schneier's concerns, opining a worst-case scenario attack against critical infrastructure is a "perennial bogeyman" (para. 11). He stated that many experts consider the likelihood of a surprise attack on civilian infrastructure, aimed to cause severe economic damage and loss of life, is very low. He pointed out the tendency of some parts of the US military to overstate the level of cyber risks. As a case in point, he referred to a testimony by a retired Cyber Command commander before the Senate Armed Services Committee, where the commander considered the danger of a potentially devastating attack as *imminent*. Yet, to date no such attack has occurred.

However, even within the US intelligence community there are some moderate voices not subscribing to some version of a cyber Armageddon, a digital Pearl Harbor, or a cyber 9/11; terms sometimes seen cited in the media. In his strategic assessment of worldwide risks related to cyber-attacks, James Clapper, Director of National Intelligence, reported that "cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact" (Clapper, 2015, p. 1). Nevertheless, despite this concerning trend, the risk of a catastrophic attack against the US, orchestrated by any particular actor, was deemed as unlikely. Instead, the assessment reported that the US intelligence community envisions "an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security" (p. 1).

Five years prior to Clapper's strategic assessment, the likelihood of cyberwar was already being widely discussed. Stevens (2010) called it an

"increasingly hysterical US debate over cyberwar" (para. 1), claiming that cyberwar has been consistently portrayed to the public as an existential threat. He cited Howard Schmidt, appointed in 2009 to coordinate the development and delivery of national cybersecurity policy, as stating that "the US is not in the midst of a cyberwar" (para. 3), and then contrasts this statement with the claim made by Mike McConnell (at that time vice-president of Booz Allen Hamilton, a major defence contractor), that "the US is fighting a cyberwar today, one it is losing" (para. 4). According to Schmidt (cited in Stevens, 2010), this is inflammatory rhetoric that hides flawed reasoning. Nonetheless, Stevens (2010) added that Schmidt does not represent the view of the whole cybersecurity industry or the US security agencies that may consider "there are simply too many perceived security benefits to information technologies and billions in federal contracts to be made from them" (para. 7).

Not all cyber-attacks require the Internet as a vehicle for delivery of the "payload," though most adversaries will take advantage of the vast, global connectivity that this network of networks provides. Notwithstanding, the key Internet infrastructure itself can be a potential target in an attack designed to bring the global network down. In an aptly titled section "Fear vs. Reality: Cyber Warfare in the Press and in Reality," Shein (2013) argued that some worst-case scenarios are fallacies, including the "notion that attackers could take the entire Internet off-line" (para. 50). He concedes that, oddly enough, this scenario is actually conceivable, and cites at that time well-known hacker "Mudge" from the L0pht group, who, when testifying before the US Senate in 1999, stated that his group could shut down the Internet within thirty minutes.

His claim gained further credibility four years later, when researchers found vulnerabilities in one of the key Internet routing protocols. While arguing that it would be technically possible, Mudge posed the question as to why would anyone want do so—in effect severing their own access to valuable information and resources that could be exploited. According to Shein, "for a cyber warrior to 'take down' the Internet makes little sense; it would be like an invading army blowing up a bridge that still lay before them" (para. 51). Similarly, for a nation-state, for example in case of a denial-of-service attack against the entire United States, the backscatter traffic resulting from such an attack would likely overwhelm the rest of the Internet. He cites the economic interdependence of nations as a strong disincentive for such a devastating cyber-attack, and adds that "above all else, the cyber warfare doctrines of all companies with sufficiently

advanced capabilities to perform such an attack would instead dictate that they exploit access to resources, rather than cut off the ability to continue to do so" (para. 52).

CONCLUSION

On balance, the arguments for-and-against the risks posed by *cyber-crime* appear not to be inflated. The general view appears to support that the scale, reach, and impact of crime associated cyber-attacks are genuine. In contrast, the case for *cyberwar* appears to be overstated. This is despite a few notable cases that have occurred, such as the cyber-attack on parts of the Ukrainian power grid. In the main, catastrophic scenarios are still considered as low in likelihood.

Notwithstanding whether the two cybersecurity manifestations discussed here are overstated or not, there is little doubt that the overall risks posed by cyber disruption are a hazard for individuals, organisations, government agencies, and the economies of nations. So, what implications does this have for cybersecurity practice? One thought is that it is important for cyber defences to improve in line with the risks, and to do this, researchers need to work across both categories of cybersecurity regardless of the likelihood of an attack. This is because cyber-related risks are associated with all Internet-based systems and devices. As the Director of National Intelligence advised: "cyber threat[s] cannot be eliminated; rather, cyber risk[s] must be managed" (Clapper, 2015, p. 5). Therefore, risk management is a sensible approach to what can sometimes be a divided discourse of opinion.

ABOUT THE AUTHOR

Petr Chrapavy, Graduate Certificate in Intelligence Analysis, is a member of the Australian Information Security Association (AISA), Institute of Electrical and Electronics Engineers (IEEE), Institute of Instrumentation, Control and Automation (IICA), and Cloud Security Alliance (Australia Chapter). He has over twenty years' experience in the ICT industry, with the last eleven years spent in various roles dedicated to cybersecurity.

REFERENCES

Akamai Technologies. (December 8, 2015). Q3 2015 State of the Internet – Security Report. *State of the Internet*. Retrieved from https://www.stateoftheinternet.com/resources-cloud-security-2015-q3-web-security-report.html

Australian Cyber Security Centre (ACSC). (2015). *The Australian Cyber Security Centre Threat Report 2015*. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

Clapper, J. R. (February 26, 2015). *Statement for the Record Worldwide Threat Assessment of the U.S. IC Before the Senate Armed Services Committee*. Office of the Director of National Intelligence (ODNI). Retrieved from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

van Dantzig, M., Heppener, D., Ruiz, F., Klijnsma, Y., Zheng, Y., de Jong, E., … Haagsma, L. (November 30, 2015). *Ponmocup. A giant hiding in the shadows*. Retrieved from https://foxitsecurity.files.wordpress.com/2015/12/foxit-whitepaper_ponmocup_1_1.pdf

Europol. (2014). *The Internet Organised Crime Threat Assessment (IOCTA) 2014*. Retrieved https://www.europol.europa.eu/iocta/2014/keyfindings.html

Europol. (September 30, 2015). *The Internet Organised Crime Threat Assessment (IOCTA) 2015*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_ioctа_web_2015.pdf

Goodin, R. (January 6, 2016). First known hacker-caused power outage signals troubling escalation. In *Ars Technica*. Retrieved from http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

Howard, E. M. (December 2015). Home, Smart Home. *The Institute, 39*(4). 13.

Iyer, K. (September 8, 2015). Hackers Turn Off The Pacemaker Of A Simulated Human And Kill It. *TechWorm*. Retrieved from http://www.techworm.net/2015/09/hackers-turn-off-the-pacemaker-of-a-simulated-human-and-kill-it.html

Lee, R. M., Assante, M. J., Conway, T. (March 18, 2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Leyden, J. R. (November 24, 2015). Cyber-terror: How real is the threat? Squirrels are more of a danger. *The Register*. Retrieved from http://www.theregister.co.uk/2015/11/24/cyber_terror/

McAfee Labs. (November 9, 2015). *McAfee Labs 2016 Threats Predictions*. Retrieved from http://www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf

Michigan State University. (February 16, 2016). *Cyber thieves making millions in profits*. Retrieved from http://msutoday.msu.edu/news/2016/cyber-thieves-making-millions-in-profits/

Ponemon Institute. (October, 2015). 2015 Cost of Cyber Crime Study: Global. *Hewlett Packard Enterprise*. Retrieved from https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

Rozenfeld, M. (March 6, 2015). Should We Fear a Catastrophic Cyberattack? *The Institute*. Retrieved from http://theinstitute.ieee.org/opinions/question/should-we-fear-a-catastrophic-cyberattack

Schmidt, M.N. (Ed). (2013). *Tallinn manual on the international law applicable to cyber warfare*. New York: Cambridge University Press. Retrieved from https://archive.org/download/TallinnManual/TallinnManual.pdf

Schneier, B. (July 7, 2010). The Threat of Cyberwar Has Been Grossly Exaggerated. *Bruce Schneier* [Web log post]. Retrieved from https://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html

Schneier, B. (March 4, 2015). Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle. *Bruce Schneier* [Web log post]. Retrieved from https://www.schneier.com/essays/archives/2015/03/hacker_or_spy_in_tod.html

Shein, R. (2013). A Brief Summary of Cyber Warfare. In *Information Security Today*. Retrieved from http://www.infosectoday.com/Articles/Cyber-Warfare.htm

Stevens, T. (March 10, 2010). The US is not at cyberwar. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2010/mar/09/us-cyberwar-howard-schmidt

Tucker, P. (November 3, 2015). *US Still Doesn't Know Who's In Charge of What If Massive Cyber Attack Strikes Nation*. Retrieved from http://www.defenseone.com/threats/2015/11/us-still-doesnt-know-whos-charge-if-massive-cyber-attack-strikes-nation/123377/

Uhlmann, C. (December 3, 2015). "Classified report on Bureau of Meteorology cyber-attack recommends computer system overhaul." *ABC News*. Retrieved from http://www.abc.net.au/news/2015-12-03/report-on-bom-cyber-attack-recommends-it-overhaul/6997832

The U.S. Department of Homeland Security (DHS). (January 27, 2016). Intelligence Assessment: Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector. Retrieved from https://info.publicintelligence.net/DHS-CyberAttacksEnergySector.pdf

Zetter, K. (December 18, 2015). Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors. Retrieved from https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/

Zetter, K. (December 23, 2015). The Year's 11 Biggest Hacks, From Ashley Madison to OPM. In *Wired*. Retrieved from http://www.wired.com/2015/12/the-years-11-biggest-hacks-from-ashley-madison-to-opm/

- o O o -