CHAPTER 3

WannaCry as a Creeping Crisis

Maria F. Prevezianou

Abstract This chapter deepens our understanding of cyber crises with the help of the creeping crisis concept. The chapter shows that although emerging technologies make malicious activities in cyberspace more sophisticated, vulnerabilities enabling such threats have been inherent in cyber assets for a very long time in the form of creeping crises. The question is: was WannaCry the acute crisis or just a precursor event to a bigger explosion? It is argued that the WannaCry ransomware attack in 2017 should be considered a wake-up call. The chapter demonstrates how the cyber threat was lurking in the background, gradually evolving in time and space in a non-linear fashion and receiving varying levels of attention.

Keywords Creeping crisis • Cyber-attacks • Cyber security • WannaCry • IT security

M. F. Prevezianou (✉)
Swedish Defence University, Stockholm, Sweden

Secana Omegapoint, Stockholm, Sweden
e-mail: maria.prevezianou@fhs.se

A. Boin et al. (eds.), *Understanding the Creeping Crisis*,
https://doi.org/10.1007/978-3-030-70692-0_3

3.1 Introduction

"Oops, your files have been encrypted!". In May 2017, a large number of users booted their computers only to find this message on their screens. The message was accompanied by a set deadline of three days: the user had to pay 300 USD ransom in the Bitcoin cryptocurrency to have their files decrypted. If users did not meet the deadline, the ransom would double; if the payment was not made within seven days, the decrypted files would be deleted (Symantec, 2017a).

These users had fallen victim to a ransomware "cryptoworm" now known as WannaCry, which allows hackers to encrypt user data. The worm replicated itself within networks without user interaction (Europol, n.d.). This "distributed denial-of-service" attack affected multiple systems across the world. Hospitals and clinics in Britain were forced to turn away patients due to a lack of access to patient information. Red pop-up windows covered announcement boards at Deutsche Bahn stations. The multinational shipping company FedEx experienced widespread service delays. The Russian interior ministry, railways, banks and phone operators all found themselves battling ransom demands (BBC, 2017). These are just a few of the major implications of the WannaCry attack.

No matter how many security systems we install in our homes, our banks and our businesses, there will always be the risk of criminal activity. Cyberspace is not an exception to the rule. As in the physical world, cyberspace can never be entirely secure. This is a key point in understanding how the situation got out of control during the 2017 WannaCry attack. Software contains bugs and errors that can have serious security implications, since cyber criminals can exploit these bugs to gain unauthorized access to, and control over, a computer. As Middleton (2017) argues, "[…] we need to keep doing the same things we have been doing for many years in the realm of physical security. You don't want to let your guard down there" (p. x). Standing still, we might say, is falling behind in the pursuit of cyber security.

This chapter demonstrates our shallow understanding of cyber crises. With WannaCry as an indicative example, the chapter shows how cyber crises are "hiding in plain sight", to quote the title of this volume. It makes use of the "creeping crisis" concept introduced in the first chapter, a concept that helps to reveal dimensions of cyber crises that are often overlooked or misinterpreted. Most analyses on the matter focus on cyber

crises' unprecedented speed, unpredictability, and delimitation in time.[1] Drawing from the creeping crisis conceptual framework, the chapter argues that, despite their seemingly speedy and temporally delimited nature, cyber crises do not have a clear beginning or ending and may keep simmering long after the "hot phase" of the "crisis" is over (Boin, Ekengren, & Rhinard, 2020, p. 5). In contrast to conventional wisdom, cases like WannaCry are not exceptional events delimited in time and space, but rather permanent global threats that manifest themselves as seemingly acute crises (cf. George, 1991). Due to their highly complex nature, they receive varying levels of attention from different actors. Above all, these events demonstrate the need for a better understanding of the long-term processes that give rise to cyber crises.

3.2 Precursor Events

Major cyber-attacks are often preceded by a chain of events and disturbances which, from a creeping crisis perspective, can be seen as precursor events and indicators of a deeper problem. One reason these precursor events occur is rather straightforward. In order to prevent software bugs and errors from posing a serious threat to our computers and networks, software vendors release security patches to fix emerging problems. Those patches signal problems that, before the patch is installed, can be momentarily exploited by hackers. To add to the problem, when state interests come into play, the situation becomes more complex.

For instance, a few years before the WannaCry attack in 2017, the US government is believed to have discovered a security vulnerability in Microsoft's Windows operating system. The US National Security Agency (NSA) had two choices at the time: it could either keep the vulnerability a secret and use it for offensive purposes of national interest, or encourage Microsoft to issue a patch to fix the vulnerability quickly.[2] According to the so-called NOBUS concept ("nobody but us"), the NSA estimates whether it is the sole actor aware of a certain vulnerability, or if other actors could have already found it (Peterson, 2013). By choosing to keep

[1] Cyber crises are most commonly examined from a strictly linear perspective with the use of traditional crisis phases such as a pre-crisis, crisis, and post-crisis phase. See for instance Chorąś, Kozik, Flizikowski, Holubowicz, and Renk (2016, p. 146).

[2] Parts of the empirical section on WannaCry presented here draw on my earlier work of conceptualizing cyber crises (Prevezianou, 2020).

the vulnerability a secret, the NSA estimated that the benefits of exploiting the error, in order to weaponize it, would outweigh the broader security risk. This estimate would later prove inaccurate.

The hacking tool developed by the NSA (Nakashima & Timberg, 2017) targets the Microsoft Windows operating system and infects vulnerable computers remotely. The Agency had been using the tool for five years before alerting Microsoft of its existence (Burdova, 2020). Although Microsoft swiftly issued security updates for all Windows versions, (Microsoft, 2017), individual users, companies and public institutions failed to install the updates. As a result, the threat potential accumulated unbeknownst to users, politicians, and crisis managers everywhere. A vast number of users all over the world had left—and, as of today, continue to leave—the door opens to a threat with a potential to erupt at any point in time.

Demonstrating the complex temporal aspect of creeping crises, at an unknown point in time a malicious hacker group called the Shadow Brokers started taking advantage of the security vulnerability, too. The group first appeared in the summer of 2016 and began promoting itself through social media, where it claimed to have compromised the "Equation Group," a sophisticated cyber-attack group allegedly linked to the NSA (European Union Agency for Cybersecurity [ENISA], 2016). To prove their claim, they started disclosing some of the group's hacking tools for free and later auctioned the rest to the highest bidder. In the midst of intense speculation regarding the true origin of the leaks, analysis conducted by security researchers suggests that the exposed data and tools were valid and even dated back to as far as 2013 (Suiche, 2016). The disclosed files revealed vulnerabilities in known vendors' devices, including public agencies, which could be used by any malicious actor wishing to exploit them.

The Shadow Brokers continued to engage in a series of leaks during 2016 and 2017. In April 2017, as part of their fifth effort to disclose vulnerabilities, they leaked several hacking tools and exploits, including the NSA's EternalBlue. On May 12, 2017, using the EternalBlue tool, hackers unleashed the WannaCry ransomware cryptoworm, which cracked vulnerable systems remotely through Internet scanning and replicated itself to spread from one vulnerable computer to the next (ENISA, 2017). The ransomware spread at a rate of 10,000 devices per hour, infecting over 230,000 Windows PCs across 150 countries in a single day (Burdova, 2020).

The WannaCry crisis exposed the multi-domain nature that is familiar to scholars of creeping crises. A cyber crisis can—and will—activate crises in multiple domains and affect a variety of actors, from individuals and private companies, to political institutions and critical infrastructure operators (Prevezianou, 2020). WannaCry demonstrates how cyberspace is used as a tool to simultaneously trigger crises across sectors and showcases how the negligence, or even inability, of policy-makers to map these sectoral interconnections and establish adequate crisis management mechanisms can allow a potential threat to lurk in the background.

Policy-makers and regulators, largely divided over responsibility and goals, had a difficult time managing the crisis. Considering that the attack could have been prevented, or at least had a less significant impact, if individual users and organizations had installed the security patches released by Microsoft two months prior to the attack, it is now evident that a severe lack of "cyber hygiene", combined with a lack of a "shared responsibility" amongst individuals, the government and the private sector contributed to the accumulation of threat potential (Smith, 2017). Securing our systems needs to be a common effort. Practicing good cyber hygiene is the users' responsibility, especially when the user is a national authority or organization. The interconnectedness of cyberspace, authorities working at cross purposes, and the lack of individuals' cyber hygiene resulted in a dangerous combination that fueled the problem.

3.3 A Tipping Point

The onset of the WannaCry attack proved a tipping point that spilled over into multiple, additional crises.

3.3.1 Diffuse Effects

The spill-over was unprecedented. Many individual users and organizations across the globe were hit by the attack, including critical infrastructure operators, manufacturers, and service providers. Their systems were set to stop functioning—unless they paid the ransom. Even then, no one could guarantee that the systems could be recovered after the ransom was paid. A few significant examples of organizations hit by the attack were (BBC, 2017):

- Britain's National Health Service
- The Russian Ministry of Interior, several banks, and MegaFon, Russia's second largest mobile phone operator
- German railways
- The Spanish phone operator Telefonica, power firm Iberdrola, and utility provider Gas Natural
- The French car manufacturer Renault, which was forced to halt production at many sites
- Chinese universities
- 600 Japanese companies
- Indonesian hospitals
- Andhra Pradesh Police in India

This disruption of services caused major economic losses, which were estimated to reach 8 billion USD (Barlyn, 2017). The impact was not just economic. The attack was a wake-up call, since it revealed how a crisis creeping in cyberspace can have a major spill-over effect in the "real world" and affect our daily lives in unexpected ways. A clear example was Britain's National Health Service. Hospitals were unable to access patient data, thousands of operations and appointments were canceled, vital medical equipment had to be taken off-line and ambulances were diverted to other, unaffected hospitals (BBC, 2017).

The private sector led the response effort. Microsoft immediately released emergency security patches after the attack (Microsoft Security Response Center Team, 2017). Apart from users of in-support versions of Windows, who would be automatically protected provided that they had the "automatic updates" function enabled, Microsoft moved one step further by issuing patches for out-of-support systems including Windows 2003 and Windows XP (Misner, 2017). At the same time, international organizations, together with so-called computer emergency response teams (CERTs) and large cybersecurity companies, issued guidelines that users should follow in response to the attack, regardless of whether they had been hit or not. Cybersecurity experts advised users against paying the ransom and urged them to update their systems as soon as possible in order to ensure their protection (Baraniuk, 2017).

The attack's expansion was halted in a surprising way. Marcus Hutchins, a British computer security researcher, also known by the pseudonym "Malware Tech," accidentally discovered a "kill switch" by registering a

domain name that tracked the spread of the ransomwear and, in the end, halted it (Malware Tech, 2017). By slowing down its expansion, it allowed for the implementation of further protection measures. However, it could not reverse the damage that was already done.[3]

3.3.2 Limited Attention, Limited Response

The deeper problems signaled by the WannaCry attack were hardly new. Cybersecurity experts have been raising the alarm for a long time—unfortunately without attracting the necessary level of attention from authorities or individual users. Attention is a core factor in understanding the response to a creeping crisis: "if political elites, media and the public do not collectively share a sense of crisis, it is hard to speak of a crisis" (Boin et al., 2020, p. 7). Without attention, remedial action is unlikely. Connecting this argument to WannaCry, it does not come as a surprise that a collectively shared sense of an emergent crisis was mostly absent. It alarmed experts, and some individuals sought to raise the alarm, but somehow this major, emerging threat failed to attract political and public attention.

For instance, about a month before the attack, private researchers announced they had identified computers compromised by the same hacking methods used by the NSA. Experts from several security firms warned their clients who practiced poor security practices. The fact that these methods originated from an intelligence agency was a sign to the researchers that this hacking tool was more likely than others to prove highly effective. Matthew Hickey, co-founder of Hacker House in Britain, said his teams issued ever-heightened warnings of a "Microsoft apocalypse" (Dave, 2017). "It's highly likely what we saw were precursors to WannaCry," said Govshteyn, Alert Logic's co-founder, when referring to the NSA leak warnings (Dave, 2017).

National politicians displayed little awareness of the impending threat. The term crisis was avoided, and public authorities seemed to rely on the private sector to deal with the issue. In the case of the UK, the Department of Health was warned about the risk of cyber-attacks on the NHS a year earlier. The Secretary of State for Health did ask the UK National Data

[3] The investigations conducted traced the attack to the Lazarus Group, cyber affiliates of the North Korean government (Symantec, 2017b).

Guardian and the Care Quality Commission (CQC) to undertake reviews of data security. These reports were published in July 2016 and warned the department that cyber-attacks could lead to patient information being lost or compromised and could jeopardize access to critical patient record systems. They recommended that all healthcare organizations provide evidence that action was being taken to improve cybersecurity, including moving off older, legacy operating systems. Although the department and its arm's-length bodies were working to improve cybersecurity in the NHS, it did not publish its formal response to the recommendations until July 2017 (National Audit Office, 2018, p. 5).

In March and April 2017, NHS Digital (the IT arm of the National Health Service), issued critical alerts warning organizations to patch their systems to prevent WannaCry. However, before May 12, 2017, the department had no formal mechanism for assessing whether NHS organizations had complied with its advice and guidance. Prior to the attack, NHS Digital had conducted an on-site cybersecurity assessment for 88 out of 236 NHS trusts (local governance regions), and none had passed. But NHS Digital could not mandate a local body to take remedial action even if it had concerns about its vulnerability (National Audit Office, 2018, p. 6).

Many individual users remained unaware of the severity of the problem. There are still many users who have not patched their systems against the EternalBlue vulnerability. Even after the crisis, more than two years following the global outbreak, the WannaCry ransomware was still spreading and sometimes still successful at infecting users. Some people still paid the ransom in a futile effort to retrieve their encrypted data (Mackenzie, 2019). Not only did this put them at risk of falling victim to WannaCry, but they are also at risk of other attacks which have emerged since EternalBlue wreaked havoc. For instance, according to the UK National Audit Office:

> WannaCry was the largest cyber-attack to affect the NHS, although individual trusts had been attacked before 12 May 2017. For example, two of the trusts infected by WannaCry had been infected by previous cyber-attacks. One of England's biggest trusts, Barts Health NHS Trust, had been infected before, and Northern Lincolnshire and Google NHS Foundation Trust had been subject to a ransomware attack in October 2018, leading to the cancellation of 2800 appointments. (National Audit Office, 2018, p. 5)

This statement showcases the severity of the problem. The precursor events were insufficiently addressed, and little political attention turned toward the problem; all which in turn led to further accumulation of threat potential. This is not the only example. In May 2019, two years after WannaCry, thousands of computers in the US city of Baltimore's city government were frozen after their files became digitally scrambled by hackers with the help of the EternalBlue fault (BBC, 2019). This led to local residents being unable to pay utility bills, parking tickets and taxes, while at the same time the staff could not send or receive emails.

Elsewhere in the world, the situation was similar. In Russia, where WannaCry affected the country's banking system, the central bank claimed to have sent recommendations to Russian banks to update their Windows software only a month before the actual attack and few took heed even then (Winning and Stubbs, 2017). Consequently, there seems to be a pattern of authorities not addressing the matter sufficiently and not taking the necessary action, even though experts and Microsoft had stressed the urgent need to keep our systems updated in order to prevent not only that particular attack, but also future attacks that could come from the same systemic weakness (Pope, 2019).

Governments failed to elevate the issue to the crisis level (by not taking measures and addressing it with the same intensity as the private sector), while the private sector was leading the management efforts and security experts were warning—and continue to warn—of a massive cyber crisis if the focus remains on managing manifestations instead of addressing the root of the problem and understanding the long-term threat accumulation. This varying sense of urgency among different actors is further deepened by a lack of ownership. Creeping crises can be addressed successfully only through cross-sectoral and cross-border cooperation, which is hindered by uncertainty, shifting national interests and varying degrees of political will (cf. Blondin & Boin, 2020).

3.4 From Creeping Crisis to Crisis: A Discussion

The fact that a computer worm managed to spread all over the world within a few hours, with limited resources, and cause such a major disruption is highly alarming. This is especially true if we consider the devastating impact the attack could have if the hackers were to target more critical societal functions. This chapter clarifies the need to understand this highly interconnected threat landscape.

The WannaCry ransomware attack was a wake-up call, since it revealed the devastating potential of cyber threats. EternalBlue, the bug that opened the door to WannaCry, still fuels an endless infection cycle and its legacy lives on. Soon after the WannaCry ransomware campaign, a new type of malware, Petya and its variant NotPetya spread through the same vulnerability, although this time the malware was much more sophisticated and deliberately malicious in character, as it entered the network through unpatched Windows-operated machines, stole passwords, gained administrator access and spread itself over the entire network (Hern, 2017). These ransomware attacks, like those before them, spread across the world (Greenberg, 2018).

Cases like WannaCry are great examples of a new type of crisis that develops in a dynamic threat environment and, despite widespread impact at a societal and political level, does not attract the same level of attention among different stakeholders as we might expect using a traditional crisis perspective.

The case also generates a tricky question for the creeping crisis research agenda, which distinguishes between precursor events and future, major crises. Was WannaCry a creeping crisis that developed into an acute full-blown crisis when the cryptoworm spread itself across the globe? Or was it a mere manifestation of a creeping crisis in cyberspace, whose acute phase is yet to be revealed? This chapter argues that, despite the fact that WannaCry constituted a tipping point in the development of a creeping crisis into a major crisis, the ransomware explosion in 2017 remains a symptom of an underlying and much more serious problem that may take us all by surprise in the future.

This is not to say that we should expect a cyber doomsday—although such scenarios are often posed by experts—or even examine other vulnerabilities that could be exploited by cyber criminals. This is a creeping crisis that is still developing in full view. Manifestations are numerous and sometimes resemble "big bangs." Yet decision-makers seem to be taken by surprise every time, while experts constantly raise the alarm and warn of a more devastating impact. Individual users are mere spectators in this vicious circle, but they have much to lose. There is a potential for a full-blown cyber crisis that has not yet been witnessed.

After the WannaCry attack, Brad Smith, the President of Microsoft, demonstrated the severity of the issue from a national security perspective:

> […] this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action. (Smith, 2017, p. 1)

There is more to cyber crises than traditional crisis approaches allow us to see. A focus on how "sudden" or "fast" a cyber incident is will result in a rather shallow understanding of the situation, which, in turn, leads to bad decision-making. As demonstrated by WannaCry, the cyber threat lurks in the background and develops across temporal and spatial boundaries, suddenly manifesting itself through tipping points. It receives varying levels of attention, which leads to a lack of a collectively shared sense of an ongoing crisis. This in turn leads to further accumulation of threat potential due to an insufficient response. The vicious circle goes on and on. Effective responses, supported by insightful research, need to acknowledge that in an interconnected world we cannot manage crises without mapping the interconnectedness of critical systems, without understanding how different actors and different conditions interact and without understanding what consequences this interaction generates. The need to go beyond the traditional temporal crisis perspectives and look at the broader, systemic picture is more pressing than ever. The creeping crisis perspective takes some useful steps in this direction.

References

Baraniuk, C. (2017, May 15). Should you pay the WannaCry ransom?. *BBC News*. Retrieved November 19, 2020, from https://www.bbc.com/news/technology-39920269

Barlyn, S. (2017, July 17). Global cyber attack could spur $53 billion in losses: Lloyd's of London. *Reuters*. Retrieved November 19, 2020, from https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

BBC. (2017, May 15). Ransomware cyber-attack: Who has been hardest hit?. *BBC News*. Retrieved November 19, 2020, from https://www.bbc.com/news/world-39919249

BBC. (2019, May 27). Baltimore ransomware attack: NSA faces questions. *BBC News*. Retrieved November 19, 2020, from https://www.bbc.com/news/technology-48423954

Blondin, D., & Boin, A. (2020). Cooperation in the face of transboundary crisis: A framework for analysis. *Perspectives on Public Management and Governance, 3*(3), 197–209. https://doi.org/10.1093/ppmgov/gvz031

Boin, A., Ekengren, M., & Rhinard, M. (2020). Hiding in plain sight: Conceptualizing the creeping crisis. *Risk, Hazards & Crisis in Public Policy, 11*(2), 116–138. https://doi.org/10.1002/rhc3.12193

Burdova, C. (2020, June 18). What is EternalBlue and why is the MS17-010 exploit still relevant?. *Avast Academy*. Retrieved November 19, 2020, from https://www.avast.com/c-eternalblue

Choraś, M., Kozik, R., Flizikowski, A., Holubowicz, W., & Renk, R. (2016). Cyber threats impacting critical infrastructures. In R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the complexity of critical infrastructures: A modelling and simulation approach* (Studies in Systems, Decision and Control, No. 90) (pp. 139–161). Springer Open. https://doi.org/10.1007/978-3-319-51043-9

Dave, P. (2017, May 17). They predicted the 'WannaCry' ransomware cyberattack, so how come few listened? *Los Angeles Times*. Retrieved November 19, 2020, from https://www.latimes.com/business/technology/la-fi-tn-ransomware-warnings-20170516-story.html

ENISA [European Union Agency for Cybersecurity]. (2016, October 5). The "Shadow Brokers" story. Retrieved November 19, 2020, from https://www.enisa.europa.eu/publications/info-notes/the-201cshadow-brokers201d-story

ENISA [European Union Agency for Cybersecurity]. (2017, May 15). WannaCry ransomware outburst. Retrieved November 19, 2020, from https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

Europol. (n.d.). Wannacry ransomware. Retrieved November 19, 2020, from https://www.europol.europa.eu/wannacry-ransomware

George, A. (Ed.). (1991). *Avoiding war: Problems of crisis management*. Boulder: Westview Press.

Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. Retrieved November 19, 2020, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hern, A. (2017, June 28). Ransomware attack 'not designed to make money', researchers claim. *The Guardian*. Retrieved November 19, 2020, from https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia

Mackenzie, P. (2019, September 18). The WannaCry hangover. *Sophos*. Retrieved November 19, 2020, from https://news.sophos.com/en-us/2019/09/18/the-wannacry-hangover/

Malware Tech. (2017, May 13). How to accidentally stop a global cyber attacks. Retrieved November 19, 2020, from https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

Microsoft. (2017, March 14). Microsoft security bulletin MS17-010—critical. Retrieved November 19, 2020, from https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

Microsoft Security Response Center Team. (2017, May 12). Customer guidance for WannaCrypt attacks. *Microsoft TechNet*. Retrieved November 19, 2020, from https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Middleton, B. (2017). *A history of cyber attacks: 1980 to present*. Oxfordshire: Taylor & Francis Group.

Misner, P. (2017, May 12). Customer guidance for WannaCrypt attacks. *Microsoft Security Response Center*. Retrieved November 19, 2020, from https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nakashima, E. & Timberg, C. (2017, May 16). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *Washington Post*. Retrieved November 19, 2020, from https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.f3dca304670a

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*. Report by the Comptroller and Auditor General for the Department of Health. London: National Audit Office.

Peterson, A. (2013, October 4). Why everyone is left less secure when the NSA doesn't help fix security flaws. *The Washington Post*. Retrieved November 19, 2020, from https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/

Pope, S. (2019, May 30). A reminder to update your systems to prevent a worm. *Microsoft Security Response Center*. Retrieved November 19, 2020, from https://msrc-blog.microsoft.com/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/

Prevezianou, M. F. (2020). Beyond ones and zeros: Conceptualizing cyber crises. *Risks Hazards and Crisis in Public Policy, 12*(1), 51–72. https://doi.org/10.1002/rhc3.12204.

Smith, B. (2017, May 14). The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. *Microsoft*. Retrieved November 19, 2020, from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Suiche, M. (2016, August 15). Shadow brokers: NSA exploits of the week. Retrieved November 19, 2020, from https://blog.comae.io/shadow-brokers-nsa-exploits-of-the-week-3f7e17bdc216#.48e51dl00

Symantec. (2017a, October 23). What you need to know about the WannaCry Ransomware. Retrieved November 19, 2020, from https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

Symantec. (2017b, May 22). WannaCry: Ransomware attacks show strong links to Lazarus group. Retrieved November 19, 2020, from https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Winning, A., & Stubbs, J. (2017, May 19). WannaCry cyber attack compromised some Russian banks: Central bank. *Reuters*. Retrieved November 19, 2020, from https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V