The Undiscussed Civilian Victims in the Crossfire of Cyberwarfare

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Samuel Y. Ahn

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

The Undiscussed Civilian Victims in the Crossfire of Cyberwarfare

When asked about cybersecurity, the common person may think of malicious software, or malware, such as adware or ransomware—devious cyberattacks from smaller groups to exploit victims that cannot defend themselves—use them as an asset to gain unauthorized access for financial gains; however, scarcely do people think of the further sinister cyberattacks conveyed by heavily funded, strategically organized, and scientifically innovated malware developed by government-backed entities to carry out the agenda of a nation-state. This is natural behavior, as when governing bodies carry out organized cyberattacks or cyberwarfare, the main target is often government organizations and not civilians, and these cyberattacks of this scale are often kept classified and unspoken. Despite this, there are cases where cyberwarfare between nation-states hinders daily lifestyle and breaks the sense of safety civilians have when interacting with the technological world as bad actors use civilians as vectors for their malware—either by explicit intention or complete accident.

In the quickly advancing modern era of glass and silicon, everyone has an electronic device; often one with a computer able to connect to the internet as well as other devices. A tech-savvy person may have up to 10 devices in their home with three devices always on their person, a highschooler may have a laptop and smartphone they need with a four-year-old sibling that frequently borrows a tablet for entertainment, and people going through financially difficult times may find themselves valuing their smartphone more than a meal. With computers developing very quickly and integrating within a large amount of previously non-technical innovations, some people may not realize that they are growing more connected to the world of cyberspace. Homeowners may equip their houses with a myriad of smart devices and appliances—each device with the ability to connect to the local home network of computers that

are often running operating systems. As people continue to advance the technologies that make life more effective, convenient, and exciting, more of their lifestyles and livelihoods grow further interconnected and dependent on computers, each of which potentially creates more vectors for malicious actors to exploit.

Every device capable of connecting to the internet or a local network of devices are all potential nodes for a bad actor or "hacker" to reconnoiter, infiltrate, and exploit to progress their personal agenda. The term "hacking" originated as a term describing, "putting together a rough solution for a problem", but as cybercriminals began to hack up methods of cyberattacks, the term adopted a new meaning: the unauthorized access and exploitation of a computer or network. With the devices that are prominent in people's lives, they are left vulnerable to exploitation by hackers. Usually, this is through basic cyberattacks that exploit uninformed users for illegitimate monetary benefit. Occasionally, groups of cybercriminals may band together to form larger, more organized groups to simultaneously target many people. As these groups form, greater feats are imagined and performed, from assaults on highly secure corporations to steal huge sums of money, to activism on the internet through illicit means; otherwise known as "hacktivism". The capabilities and reach of organized cyberattacks have been recognized since the advent of hacking, and as such, governments have focused on its importance and the creation of their hacking groups in confidence. These covert units have been used by the government as a tool of warfare with espionage, sabotage, and coercion whether it is during peacetime or wartime.

With cyber-offensives and cybersecurity at the pioneering forefront of modern warfare, the effects of cyberwarfare begin to have very physical impacts on active battlefields, but a topic that remains scarcely considered is the impact of these operations on citizens caught in the crossfire. What do civilians within warscapes weather if they even go through anything at all?

Do these cyberattacks even touch civilians, and if they do, how are they executed? To which extent are civilians impacted, and are they put in danger like how civilians are when caught in the crossfire of traditional kinetic warfare? If governments primarily conduct cyberwarfare pinpointed targeted at other governments with the effects limited to government-related organizations and the military, how are civilians a part of that crossfire? When civilians are directly affected by cyberwarfare, they can see their machines infected and unwillingly used by bad actors, or they can be influenced by flooding social media networks with propaganda and misinformation. However, it is often the case that most cyberwars conducted between two countries do not directly affect civilians by infecting civilian computers, but despite that, cyberattacks still greatly impact civilians indirectly through the services that civilians utilize, policies codified to dictate regulation, economic impacts derived from losses, and major paradigm shifts and development of both rational and irrational cyber-paranoia.

Methodology

To explore these topics, two in-depth historical case-studies such as NotPetya and WannaCry are used to understand the similarities and differences between cyberattacks, the full breadth of the attacks, and the extent of the civilian impact, while separate concurrent cases are reviewed more generally to highlight different aspects such as changes in behavior caused by threats, political turmoil, persistent threats, and active use in conjunction with traditional kinetic warfare. The case studies and research cover the attack methodology and the outcome of the attacks, reinforced with qualitative data. The data is collected from primary sources and literature from academic journals, news media coverage, and firsthand interviews, and are supplemented by secondary sources on human-technology relations in cybersecurity through academic and literary publications.

Brenner and Clark (2010) explore what it means for civilians to suffer casualties when caught in cyberwarfare:

> Firstly, a civilian can be a direct target of a cyberwar attack because an attack on the civilian would directly accomplish a strategic or tactical goal of the aggressor…
>
> Second, the civilian could be a target because it is a means of attacking others…
>
> Third, a civilian can be an indirect victim…
>
> Fourth, a civilian can become a victim not of a cyberwar attack, but of its own government's response to the attack. (Brenner & Clarke, 2010, pp. 251–252)

With a focus on these rules, the collection of evidence will be based on cyberattacks that have been claimed by credible sources to be sponsored, politically supported, or implicated to be affiliated with governing bodies of nation-states. As the target of the research is the human-technology interaction between civilians, evidence will consist of qualitative and quantitative data for government bureaucratic actions, damage caused by cyberattacks, changes in the mindset of civilians, and economic impact as a metric for determining the social impact of civilians.

The government actions of interest are the policies and procedures established due to direct and indirect consequences by both victims and bystanders. Although this research is not focused on government impacts, changes in governing bodies can affect civilians by the enforcement of policies and procedures that may inhibit or complicate civilians through personal internet use, additional security requirements for services, and limits to technologies put in place by the government.

Another metric for the impact of cyberwarfare would be damages that are directly inflicted onto civilians through the destruction or non-consensual manipulation of personal

devices or damage that indirectly disrupts civilians as a consequential effect of a different instance of damage. For the extent of this research, damages to a civilian can include physical damage to property, disruption of lifestyle, psychological harm, financial losses, and other losses of value.

Outside of damage to property and lifestyle, but slightly connected to influence on the government would be the psychological impact of cyber events that significantly change the ideas of the individual and society. The worldview of civilians and potential paradigm shifts after understanding and experiencing a cyberattack may impact how civilians trust and interact with technology. Cyber events may affect personal ideas of safety, instill rational and irrational fears and paranoia, and move political ideas and movements forwards.

The final metric for the impact of cyberwarfare is the financial consequences of cyberattacks. In the context of this research, financial consequences will not be for the individual but of the society; individual financial losses will be covered in personal damages whereas large losses of money that impact entire societies will be the focus. Financial consequences can take the form of large monetary losses from corporations, organizations, and governments, and losses in large-scale products and services.

Results

As cyberwarfare continues to develop and be used during wartime and peacetime, it is found that many civilians are impacted either as collateral damage from the attack or intentionally through targeted cyberattacks. There are few anthropological works found that diligently scrutinize the physical and psychological impacts on these civilians with little quantitative data on how the lifestyles of civilians are affected by cyberattacks. However, the data that is present indicate that civilians have their lives changed by cyberwarfare events

through drastic changes in lifestyle through the services they consume, necessary goods for survival, economic shifts in society around them, and paradigm shifts on the safety and security in personal technology to the systems and agencies responsible for governing their lives.

Background

With the onset of computer innovation, societies became heavily intertwined with computers for every aspect of life, and for nation-states, that includes the defense and offense of war. Physical weapons and mechanism now relied on computer chips, communications were no longer only over radio, and power grids and infrastructure all became linked to a computer network. This meant that every part of warfare became potentially vulnerable to cyberattacks.

The Actors and Their Scripts

Every nation began equipping itself with the newest weapon in warfare; nation-sponsored hacking groups rose with every country. Even today the Tailored Access Operations (TAO) group, now named the Computer Networks Operations (CNO), resides as a part of the United States of America's NSA., Cozy Bear and Fancy Bear are claimed to be state-sponsored hacking groups, while the Sandworm group resides within the GRU behind the Russian Federation, Volt Typhoon in the People's Republic of China, the Lazarus Group or "Zinc" as the sole profitable enterprise of Democratic People's Republic of Korea (CISA, n.d.).

Each of these groups have their own sets of tools for use in cyberwarfare, most of which are classified and unavailable to the public. From cyberweapon programs that utilize zero-day exploits, cyber vulnerabilities that are not yet revealed to the public, covert field agents responsible for delivering cyberattack mediums to target sites of foreign nations, and gadgets developed through government research and development with sci-fi-like technology.

The NSA developed a set of zero-day exploit hacking scripts such as EternalBlue, a powerful tool for gaining unauthorized access to computers running Windows operating systems. The vulnerability within built-in Microsoft software was discovered by the NSA, and EternalBlue was developed by them to exploit it. The NSA then proceeded to use this exploit as one of their cyberweapons and the exploit was not made public until an organization self-proclaimed as "The Shadow Brokers" were able to gain unauthorized access to these confidential NSA tools and released them to world. This leak enabled every nation-state to utilize dangerous exploits, such as the EternalBlue exploit, as a part of cyberwarfare, even in the following case studies (Fox-Brewster, 2017).

Case Study I: WannaCry

One month after the leak of the EternalBlue exploit by The Shadow Brokers, it is speculated that the allegedly North Korean hacking organization, the Lazarus Group, was behind the propagation of WannaCry, a ransomware worm—"ransomware" being malware that encrypts a computer, locking it and making it unusable unless the victim pays a fee to the distributors of the malware to obtain an unlocking key, and a "worm" being a specific type of virus that self-propagates through a network that connecting computers to an infected vector (Malwarebytes, n.d.; U.S. Department of Justice, 2018). Due to the EternalBlue exploit being kept secret before the leak, many Windows computers were not able to update and patch the vulnerabilities in time to defend against malicious actors that immediately seized the opportunity to wreak havoc. WannaCry would demand Bitcoin ransom payments while promising an exchange for the key to unlock afflicted computers, usually to no avail (Samantha Donaldson, 2017).

WannaCry attacked roughly 230,000 computers all over the world, targeting organizations that were the most vulnerable to ransoms with outdated systems, urgent need for

computers, and poor cybersecurity responses, such as the one-third of the hospitals within the United Kingdom's National Health Service (Fox-Brewster, 2017). The machines responsible for running the hospital were compromised, leading to ambulances being rerouted, patient systems being inaccessible, making important test results impossible to store, and 19,000 appointments being canceled (He et al., 2022; Kaspersky, 2024). WannaCry was also responsible for disrupting essential services like Telefonica telecoms, Gas Natural utility service, railway ticket stations, Renault car manufacturers, FedEx delivery company, and more (BBC News, 2017). For a cyberattack that had its effects felt for roughly four days worldwide, WannaCry cost the world $4 billion dollars in damages, from lost profit in corporations, to the ransoms paid by individual elderly citizens (Kaspersky, 2024).

WannaCry is a case of financial espionage where the object of the malware was to gain as much money as possible, making for a potent and indiscriminate design specifically targeted at the general populus. Civilians were primarily the target of the malware with most of the damage coming from public services, private corporations, and the technologically uninformed public. The disruption of critical services affected anywhere from a person's daily lifestyle with a lack of gas limiting their car drives, to putting people requiring urgent care at significant health risk. Governments across the world responded to this attack to protect civilians from future attacks; one such event was the United States government under the Trump administration releasing its official statement to improve cybersecurity policy with a framework to strengthen networks and implement guidance (NIST, 2017; Trump White House Administration, 2017).

Case Study II: NotPetya

Petya, discovered in 2016, is the name of ransomware—a malware that encrypts a computer, locking it and making it unusable unless the victim pays a fee to the distributors of the

malware to obtain an unlocking key—that was responsible for infecting around 200,000 computers across many countries, primarily Russia, Ukraine, India, and Taiwan (CISA, 2018). NotPetya is a variant of the Petya virus, disguising itself as Petya. The term NotPetya was coined by Kaspersky Lab as people began to discover that NotPetya was not just a ransomware that Petya was, but instead a wiping malware that destroys all the contents of a computer. NotPetya, first appearing in June 2017, would render the computer unusable after a set amount of time where it would gather money from fake ransoms, attempt to gain administrator access, propagate itself into other computers through the network using EternalBlue, and eventually be responsible for shutting down a large portion of computers in Ukraine, disrupting public services, technological infrastructure, and essentially shutting down the country for three days, and feeling residual effects for weeks following the incident (Kaspersky, 2017).

Where WannaCry spread and locked computers indiscriminately across the world, NotPetya was a wiper malware that targeted specifically designated targets. NotPetya infects specifically Ukrainian targets indiscriminately from individual civilians to public services. NotPetya does this by targeting customers of a Ukrainian tax service called M.E. Doc, attempting to mitigating the reach of the virus to within Ukraine (but failing to do so with huge third-party victims), while still rampantly gaining access to as many Ukrainian computers as it can.

This led to significant damages to critical infrastructures and organizations such as banks, power grids, postal services, newspapers, Chornobyl nuclear power plant, metros, airports, and government buildings within Ukraine, and as well as unintended exterior victims including a large port in Mumbai, FedEx subsidiary TNT Express in the Netherlands, manufacturer Reckitt Benckiser in Britain, Saint-Gobain construction in France, and the Danish global pharmaceutical

and shipping giant, Maersk (European Repository of Cyber Incidents, 2023; Zaheer Merchant, 2022). Financial damages worldwide reached $10 billion dollars in damage with Maersk suffering an estimated $1.4 billion dollars on its own from destroyed global computer networks, lost shipments, and rebuilding.

As IT professionals were staying long hours at work to mitigate the effects of NotPetya, citizens of Ukraine found themselves restricted in basic routines, unable to get from place to place, withdraw money from banks, and scurry in a panic, from physical concerns like stocking up on food, to emotional changes from the disruption of daily life and a paradigm shift in security that affects a sense of safety (Greenberg, 2019; Jack Rhysider, 2022). NotPetya became the most devastating cyberattack in history attributed to Sandworm, a cyber division of Russia's GRU intelligence unit. The people of Ukraine found themselves questioning if their way of life was safe when so much technology that dictates it is vulnerable to such catastrophic collapse, and for a country in the middle of a conflict with Russia, it also made them question their physical safety. The people were aware that large cyberattacks could affect the important infrastructures before NotPetya, but it wasn't until after NotPetya that it was successfully executed.

Cyberwarfare and Traditional Kinetic Warfare: Escalation of the Russo-Ukrainian War

The NotPetya cyberattack had dire implications. The virus was able to abruptly disrupt the entirety of Ukraine, causing standstills and chaos after spreading to thousands of computers in moments. Questions arose on the motive behind the attack and how such a dangerous cyber weapon would be used in conjunction with other forces such as a coordinated kinetic attack. In hindsight, NotPetya seemed to be an experiment run by the Russian government to determine potential impacts of large-scale cyber weaponry.

After the re-escalation of the Russo-Ukrainian war in February 2022, Ukraine saw the emergence of a new type of hybrid warfare utilizing both kinetic traditional warfare paired with cyberwarfare offensives. A series of malware would be used to disable telecommunications systems and prevent third-party humanitarian aid from reaching civilians caught in the crossfire. One such set of malware is currently known as the HermeticSuite including HermeticRansom, a ransomware, HermeticWiper, a wiper or type of malware that wipes the data from a computer to destroy it, and HermeticWizard, the software that deploys and executes all these malwares once inside of a target system (CyberArk Blog Team, 2022; ESET Research Group, 2022; Knapczyk, 2022; Walsh, 2022).

The usage of the HermeticSuite in the Russo-Ukrainian war is one of the first large scale uses of cyberwarfare alongside traditional kinetic warfare. With the conditions of combat, there is a greater emphasis on using cyberwarfare to damage and sabotage modern cityscape battlegrounds. With the goal of taking more territory in Ukraine's cities, major hacks have been reported to hit and hinder humanitarian aid going to trapped civilians near the frontlines as well as refugees (Beyer, 2023). In the same way as NotPetya, Sandworm attacked critical infrastructure, this time affecting how Ukrainian military communicates and how civilians live close to the battlefield with no electricity.

With cyberwarfare now entering the world stage as more than just an information threat, the world now sees the extent of how cyberwarfare assists in traditional warfare, but it is becoming increasingly important seeing how cyberwarfare affects civilians. Cyberwarfare can now be directly correlated to the endangerment to people. In the case of the Russo-Ukrainian War, cyberwarfare is no longer just about exfiltration of data or sabotage of communications, but the choking out of critical humanitarian resources and critical infrastructure responsible for the

sustenance of civilians trapped close to the frontlines in the battle for attrition between the two military forces.

Cyberwarfare That Changes Thinking: Panic, Paranoia, Propaganda, and Politics

Cyberwarfare is not only used to damage machines and steal information, but it can also be used to sway the thoughts of the people. Acts of sociopolitical cyberwarfare might include the spread of misinformation or propaganda and the tampering of political processes. On top of changing how people think, the negative consequences of successful cyberattacks often change how people feel and believe.

WannaCry showed the world how powerful a single hacker entity can be, using nation-state grade cyber weapons to sweep over international society and sabotage essential services. NotPetya showed that with government backing and a targeted country, an entire society can be shut down and destabilized at a nation-wide scale. For the Ukrainians, it deeply realized the fear of cyberwarfare potentially used in tandem with kinetic warfare. After the escalation of the Russo-Ukrainian War, Ukraine barely holds together cyber infrastructure through constant hacks while the world watches as they themselves prepare defenses in cybersecurity while developing their own cyber weapons.

Political manipulation is another way cyberwarfare changes the minds of people. One cyberattack, led by the Russian Cozy Bear and Fancy Bear, was the phishing hack on the email systems of the Democratic National Committee, exposing the emails of DNC candidates (Fidler, 2016). Then, botnets, or a network of many machines used to hack, would flood social media with misinformation and propaganda to sway the opinion of the public (Johnny Harris, 2024). During the actual vote on election day, voting machines were easily susceptible to physical hacking (Steve Friess, n.d.).

Through the social engineering of DNC committee members, to the electorate through online media, and the potential vulnerability of the voting machines themselves, the opinions of the people, question of legitimacy of elections, and the political representatives in office are vulnerable to cyber espionage.

Governments primarily responded to events in cyberwarfare through the creation of official cybersecurity organizations and standards of implementation and guidance with stricter policies on compliance with such standards (EU Parliament, 2022; Serpanos & Komninos, 2022). Another way governments respond is by furthering their control of information through surveillance, which affects the privacy of the observed civilians.

Conclusion

Cyberwarfare is becoming more relevant with the advent of godlike technology engrained into every aspect of modern society. As such, it is not just governments, but the people themselves are vulnerable to the effects of cyberwarfare. With the emergence of this new idea in human-technological interaction, a widely unexplored field of anthropology is revealed where the direct impact of cyberwarfare on societies and civilizations are lacking focus, observation, and research, overshadowed by the more technological and political impacts, and limited by the stealth and unknown factors of cyberwarfare.

It is becoming apparent that cyberwarfare has significant and drastic sociopolitical effects that sway the psychology and lifestyles of the people and even their physical welfare. Cyberwarfare, an extremely quickly developing technological force, needs scrutiny to deduce the impact on the individual civilians and prevent a new type of catastrophe as nation-states enter an arms race in cyberweapons as a safeguard and deterrent, that unlike nuclear weapons, is directly implanted into the necessary machines of society at home.

Future Work

To further the research into the civilian impact of cyberwarfare, more work must be done to observe and collect data on the extent of personal damage done to civilians. Work on how cyberwarfare is perceived by laypeople and how it affects their psychology, confidence in government protection, and overall awareness of cybersecurity and cyber threats. More research needs to be done as classified evidence and outcomes of cyberattacks declassify in the coming years.

References

BBC News. (2017, May 12). Massive ransomware infection hits computers in 99 countries. *BBC News*. https://www.bbc.com/news/technology-39901382

Beyer, J. (2023, August 7). The Ukraine War & Cyberattacks Targeting Refugees and Humanitarian Organizations. *The Henry M. Jackson School of International Studies*. https://jsis.washington.edu/news/the-ukraine-war-cyberattacks-targeting-refugees-and-humanitarian-organizations/

Brenner, S. W., & Clarke, L. L. (2010). *Civilians in Cyberwarfare: Casualties*. *13*(3), 249–282.

CISA. (n.d.). Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA. Retrieved May 11, 2024, from https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.

CISA. (2018, February 15). *Petya Ransomware | CISA*. https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

CISA. (2024, February 7). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CyberArk Blog Team. (2022, February 24). HermeticWiper: What We Know About New Malware Targeting Ukrainian Infrastructure (Thus Far). *The CyberArk Blog*. https://www.cyberark.com/resources/blog/hermeticwiper-what-we-know-about-new-malware-targeting-ukrainian-infrastructure-thus-far

Dipert, Randall R. (2010). The Ethics of Cyberwarfare: Journal of Military Ethics. *Journal of Military Ethics*, *9*(4), 384–410. https://doi.org/10.1080/15027570.2010.536404

ESET Research Group. (2022, March 1). *IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine*. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

EU Parliament. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

European Repository of Cyber Incidents. (2023). *Major Cyber Incidents—NotPetya*. https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf

Fidler, D. P. (2016). *The U.S. Election Hacks, Cybersecurity, and International Law*. *110*, 337–342. https://doi.org/10.1017/aju.2017.5

Fox-Brewster, T. (2017a). An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak. *Forbes.Com*.

Fox-Brewster, T. (2017b). Watching The Awful WannaCry Ransomware Scourge Hit Doctor's Surgeries IRL: Forbes.com. *Forbes.Com*, 13–13.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

He, Y., Maglaras, L., Aliyu, A., & Luo, C. (2022). Healthcare Security Incident Response Strategy—A Proactive Incident Response (IR) Procedure. *Security & Communication Networks*. Complementary Index. https://doi.org/10.1155/2022/2775249

Jack Rhysider (Director). (2022, December 15). *Russia vs. Ukraine: The Biggest Cyber Attack Ever 🎙Darknet Diaries Ep. 54: NotPetya*. https://www.youtube.com/watch?v=N20q-ZMop0w

Johnny Harris (Director). (2024, February 14). *Why Hacking is the Future of War*. https://www.youtube.com/watch?v=15MaSayc28c

Kaspersky. (2017, June 27). *New Petya / NotPetya / ExPetr ransomware outbreak*. https://usa.kaspersky.com/blog/new-ransomware-epidemics/11710/

Kaspersky. (2024, March 21). *What is WannaCry ransomware?* Usa.Kaspersky.Com. https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry

Knapczyk, P. (2022, August 18). *Overview of the Cyber Weapons Used in the Ukraine—Russia War*. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

NIST. (2017). Bolstering Government Cybersecurity Lessons Learned from WannaCry. *NIST*. https://www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry

Samantha Donaldson. (2017, May 19). *WannaCry Ransomware: Who It Affected and Why It Matters*. Red Hat Developer. https://developers.redhat.com/blog/2017/05/19/wannacry-ransomware-who-it-affected-and-why-it-matters

Serpanos, D., & Komninos, T. (2022). The Cyberwarfare in Ukraine. *Computer*, *55*(7), 88–91. https://doi.org/10.1109/MC.2022.3170644

Steve Friess. (n.d.). *Hacking the Vote: It's Easier Than You Think*. Alumni Association of the University of Michigan. Retrieved May 8, 2024, from https://alumni.umich.edu/michigan-alum/hacking-the-vote/

Trump White House Administration. (2017). *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – The White House*. https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

U.S. Department of Justice. (2018, September 6). *Office of Public Affairs | North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions | United States Department of Justice*. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Walsh, J. (2022). Another Round Of Malware Attacks Hits Ukraine As Russia Crisis Intensifies: Forbes.com. *Forbes.Com*, N.PAG-N.PAG.

WannaCry. (n.d.). Malwarebytes. https://www.malwarebytes.com/wannacry

Zaheer Merchant. (2022, March 4). *NotPetya: The cyberattack that shook the world*. The Economic Times. https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms