NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

POTENTIAL EMPLOYMENT OF OFFENSIVE REVERSIBLE CYBERATTACKS FOR STRATEGIC AND ETHICAL PURPOSES

by

Zoe M. Swiatlowski

June 2023

Thesis Advisor: Neil C. Rowe
Second Reader: Wade L. Huntley

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE POTENTIAL EMPLOYMENT OF OFFENSIVE REVERSIBLE CYBERATTACKS FOR STRATEGIC AND ETHICAL PURPOSES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Zoe M. Swiatlowski	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Reversible cyberattacks are similar to ransomware and can provide a new capability in cyber warfare. They can be effective strategically and often ethically superior. Providing incentives in an attack like returning a system to its prior state can encourage a country to comply with demands by the attacker. This research discusses the types of cyberattack that can be effectively reversed, addressing their structure and capacity for reversibility. Traditional cyberattacks and reversible cyberattacks are compared, considering strategic advantages and ethical obligations and when each would be superior. Other issues addressed are the effects of backup methods, the kinds of collateral damage that cannot be reversed, and the need for a second cyberattack to accomplish reversal.

14. SUBJECT TERMS cyber warfare, cyberattack, reversible cyberattack, strategy, moral obligation	**15. NUMBER OF PAGES** 45
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

POTENTIAL EMPLOYMENT OF OFFENSIVE REVERSIBLE CYBERATTACKS FOR STRATEGIC AND ETHICAL PURPOSES

Zoe M. Swiatlowski
Ensign, United States Navy
BS, Eastern Michigan University, 2022

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2023

Approved by: Neil C. Rowe
Advisor

Wade L. Huntley
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Reversible cyberattacks are similar to ransomware and can provide a new capability in cyber warfare. They can be effective strategically and often ethically superior. Providing incentives in an attack like returning a system to its prior state can encourage a country to comply with demands by the attacker. This research discusses the types of cyberattack that can be effectively reversed, addressing their structure and capacity for reversibility. Traditional cyberattacks and reversible cyberattacks are compared, considering strategic advantages and ethical obligations and when each would be superior. Other issues addressed are the effects of backup methods, the kinds of collateral damage that cannot be reversed, and the need for a second cyberattack to accomplish reversal.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

APT	advanced persistent threat
DoS	denial-of-service
DDoS	distributed denial-of-service
IDS	intrusion-detection system
LOAC	laws of armed conflict
MitM	man-in-the-middle
OS	operating system
RDP	remote desktop protocol
ROE	rules of engagement

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to extend my sincere appreciation for the people listed below. Each has helped me significantly and this would not have happened without them.

To begin, I would like to thank the faculty at the Naval Postgraduate School for their guidance and help with my academics which made this thesis possible for me to write. I would specifically like to thank my advisor, Dr. Neil Rowe, for his patience, insight, and support for me while I was writing this thesis. I would also like to thank my second reader, Dr. Wade Huntley, for his inquisitive nature which caused many new areas of thought for this thesis. Your guidance and kindness have helped me greatly.

My sincerest thank you to my friends and family for your constant support throughout this journey. While having struggles, I could always count on them to help me and encourage me. It has not been easy, and you all are greatly appreciated.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Cybersecurity is a critical type of international security today. Cyberattacks are evolving to increase damage and leave more lasting effects on a country's population and infrastructure. Cyberattacks are also an increasingly large part of warfare and work within cyberspace, for which the boundaries are indefinite and not contained to physical locations. Due to the size and complexity of cyberspace and the variety of possible cyberattacks, preventing cyberattacks from succeeding has been difficult despite the many security measures in place to protect organizations and their systems (Rowe, 2010). Since we cannot prevent cyberattacks entirely, their use for counterattack is important, and reversible cyberattacks could be desirable. Military reversible attacks could temporarily cause all the damage of a traditional cyberattack but allow the attacker to simply undo it; it will use methods similar to a ransomware attack and would have ransom of a specific military or political action. A country can use a reversible cyberattack to prevent offensive actions by disabling attack capabilities of an adversary.

Reversible cyberattacks, using methods developed for ransomware in particular, could allow a new approach to warfare. When reversing the damage left to infrastructure is impossible, ethical boundaries like the rules of engagement (ROE) and the laws of armed conflict (LOAC) are introduced to give standards to limit the damage that could be inflicted because they require the attack be proportional to the threat. Cyberwarfare should have rules of engagement like all warfare, as it can cause permanent damage (Kehler, 2017). A cyberattack with a reversible agent can bypass some lasting effects, resulting in only temporary direct effects which could make them the ethical standard.

A. RESEARCH QUESTIONS

This thesis will investigate how specific types of cyberattacks can be reversed to reduce the amount of residual harm they inflict and to provide a strategic benefit to the attacker. The research questions are:

- When would reversible cyberattacks be preferable to defensive measures in preventing an adversary cyberattack?
- What types of cyberattacks are reversible? What properties determine this?
- Why and how could reversible cyberattacks offer a strategic advantage?
- When should people be morally obligated to use a reversible instead of non-reversible cyberattack?
- How could reversibility be effectively implemented?

B. METHODOLOGY

A reversible cyberattack could be offensive action taken by the United States and allies, an offensive action taken by an adversary, a defensive action taken by the United States and allies, and a defensive action taken by an adversary. This thesis will focus on offensive reversible cyberattacks used by the United States and their allies. These techniques also make it difficult for victim to remove or modify the attacker's software through it is not difficult for the attacker. This means the most attack effects will persist until either the victim meets the attacker's demands or the victim follows the time-consuming process of restoring their system from backups. Nonetheless, there can still be permanent effects such as loss of opportunities from any attack, including the ones we refer to as "reversible" in this thesis.

This work should aid the military, U.S. government, and civilian organizations that could benefit from cyberwarfare that is more controllable, following guidelines and methods we suggest for reversible cyberattacks. This thesis will include distinguishing the main type of cyberattacks and their suitability for use and reversal. Once cyberattacks are deemed suitable for reversal, we will investigate methods used in these attacks to address properties that permit reversibility.

C. THESIS ORGANIZATION

This thesis is organized into five chapters. Chapter II evaluates previous work on cyberattacks, ransomware attacks, and strategic uses for reversible cyberattacks. Chapter III focuses on details of a reversible cyberattack, with what types of attacks it would be effective, how they could work, and possible targets. Chapter IV evaluates the details of how to reverse a cyberattack, addressing security systems and how they would work as well as evaluating the ethics and morality of using reversible cyberattacks. Chapter V discusses implementation issues and why reversibility could become standard practice.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PREVIOUS WORK

Cyberattacks have been increasingly used in warfare for twenty years. They have replaced traditional military operations in many instances although policies for their use are much debated (Albahar, 2019). In the United States military, cyber warfare is now preferred in doctrine sometimes instead of traditional warfare methods (Geiss & Lahmann, 2013; Robinson et al., 2015). A reversible cyberattack might still be more preferable to a traditional cyberattack since an outcome could be achieved more ethically than previously possible. We will discuss why only some types of cyberattacks can be reversed and all reversible attack use methods similar to ransomware because of its similarities to a potential reversible cyberattack and its core structure of reversibility.

A. CYBER WARFARE REPLACING TRADITIONAL WARFARE

Cyber warfare has developed with cyberspace (Tabansky, 2011). Attacks that happen in cyberspace, or cyberattacks, have been developed in the world's militaries as well as by criminals (Albahar, 2019). Cyberattacks are popular because most of the world relies on digital technology for critical infrastructures and cyberattacks threaten them. This reliance, while it has made many aspects of life easier, has permitted cyberattacks to emerge with great effectiveness. Often cyberattacks are more effective ways to attack a county and their civilians than traditional warfare.

Damage in traditional warfare is generally limited by rules of engagement and the laws of armed conflict (Faix, 2014; Boddens Hosang, 2020, Chapter 1). Rules of engagement are particularly important for weapons of mass destruction, like chemical and atomic weapons whose effects can last decades after the original attack (Hirschfelder, 2015). An example is the use the chemical weapon Agent Orange by the United States in the Vietnam War, in which around 72 million liters of herbicides was sprayed over 12% of South Vietnam soil to destroy crops (Ichikawa, 2009). This has left lasting damage to the local population, as the deformed birth rate in 2002 was over ten times higher than other European countries, in addition to other health risks. Lasting effects were also seen from

the atomic bombs dropped on Hiroshima and Nagasaki by the United States in World War II (Douple et al., 2013).

The laws of armed conflict set a defined standard of operations within conflict. The rules of engagement and laws of armed conflict are implemented for militaries to reduce unethical long-term effects of traditional warfare. Despite them, traditional warfare attacks continue to cause significant and lasting effects. For example, the 2022 Russian invasion of Ukraine caused a significant loss in Ukrainian infrastructure which cannot be easily repaired (Blinov & Djankov, 2022). Another example was the Iran-Iraq War from 1980 to 1988 which caused lasting effects on the Iranian population and infrastructure (Fox & Haines, 2014). Many breaches of rules of engagement and laws of armed conflict result in lasting damages, but these are not the only cases. The laws of armed conflict require minimal use of force to achieve necessary ends, but even minimal means can be extensive. Not all severe attacks violate the laws of armed conflict or the rules of engagement but a violation bears consequence. International law supports the claims that countries who operate outside the rules of engagement and cause significant damage to other countries must help rebuild and repair the damage (Litan, 2022). Such consequences are one reason why countries are shifting towards cyber warfare in the hope that cyber warfare can cause less damage and permit less attribution than traditional warfare in achieving the same objectives.

B. PREVIOUS WORK ON CYBER WARFARE

Traditional warfare tries to damage land, people, and infrastructure to reduce the ability of an adversary to fight. Cyber warfare is similar as it tries to damage cyber physical and logical critical infrastructure. Though the goal of cyber warfare is to incapacitate a certain party, it often can be done without physically harming them (Robinson et al., 2015). Another advantage to cyber warfare is easier anonymity of the attacker. For example, in the 2021 Colonial Pipeline cyberattack on the United States, the Russian government claimed that they had nothing to do with the attack, although evidence showed that the attacker was likely operating inside Russia (Jasper, 2021). Since this was a cyberattack, it was difficult to prove the Russian government was involved, this is not the case if the attack

was done with traditional warfare methods. As technology has progressed, more ways can find the source of an attack, but also more ways to hide the source are possible.

Some cyberattacks are denial-of-service (DoS) attacks, eavesdropping, phishing, cross-site scripting, direct-success attacks, bot networks, clickjacking, backdoors, spoofing, man-in-the-middle (MitM) attacks, and tampering (Sumi et al., 2019). Their goals are to gain administrator privileges, prevent access to information, destroy information, and eavesdrop on information being transmitted. Some do not cause much damage, like eavesdropping, and some can cause significant damage, like man-in-the-middle attacks. An example of a man-in-the-middle attack is the 2010 Stuxnet cyberattack, which was effective because the controllers of the Iranian centrifuges did not know that their information was no longer coming from a trusted source (Karnouskos, 2011). This caused significant destruction and hindered Iran's nuclear power program. This incident showed the world the potential for cyberattacks to be as threatening as traditional warfare attacks.

C. PREVIOUS WORK ON RANSOMWARE METHODS

Ransomware disables programs or data of a victim until the victim pays a ransom to the perpetrator (Kok et al., 2019). These attacks are popular with criminals for extortion. Ransomware attacks have been growing and their methods have been getting more sophisticated. Large organizations are more vulnerable to ransomware attacks as they have more access to large sums of money, though they often have better security to compensate because of such threats. Ransomware attacks increased 105 percent from 2020 to 2021, and ransomware attacks on hospitals more than doubled from 2016 to 2021 (Lightfoot, 2022; Fox, 2023). The increased sophistication of ransomware methods and the continued growth in cyberspace means ransomware can be dangerous.

Most ransomware uses strong encryption algorithms and high-grade encryption keys to take control of a system (Genç et al., 2018). Once ransomware is installed on a system, it will modify target files, often by encrypting them (Gangwar et al., 2018). Strong encryption methods and good encryption keys allow ransomware to operate quickly and maneuver past antivirus and antimalware. The two major types of ransomware are locky

and crypto. Locky ransomware blocks a system or resource from its user and does not usually alter it. Crypto ransomware uses encryption with a key not known to the victim to modify software or data to make it unusable by the victim. This type can be harder to undo because only the attacker can decrypt (Kok et al., 2019).

The growth in ransomware is aided by the many ways discovered to put malware into a system. These include spam or phishing emails, visiting an infected website, downloading malicious software, exploiting open remote access (RDP), and many other unsafe cyber practices (Datto, 2020). Ransomware typically hides on a user's system by renaming files and changing file extensions. Some attacks implement passwords on files and require a ransom to receive the password. Others contain an executable file that, when started, will infect the whole system with malicious software (MacRae & Franqueira, 2018). Ransomware can hide within other files, as for instance an executable file hidden a .pdf file. Typically, ransomware stores itself in memory, creates a key, and encrypts data so restoration of the system is possible (Gonzalez & Hayajneh, 2017).

Despite all the ways malicious software can be installed, many detection techniques to help identify and remove the malicious code before it becomes installed exist. Aside from keeping a system safe with good cybersecurity practices, black-lists (listing as dangerous) and white-lists (listing as safe) of files or their hashes are good ways to prevent non-native software from accessing specified parts of a system (Moussaileb et al., 2018). Machine learning can learn new clues to detect a ransomware attack (Kok et al., 2019; Ganfure et al., 2022); although these detection mechanisms work well on previously used ransomware techniques, they may fail on new ransomware. It is best to prevent a ransomware attack by removing it early before it has been installed on a system, and detection is the main line of defense (Kok et al., 2019). Ransomware attacks often find vulnerable parts of a systems to install the ransomware, so some directories are more likely targets than others (MacRae & Franqueira, 2018; Gonzalez & Hayajneh, 2017).

D. RESTORATION FROM BACKUP

A ransomware attack is an example of a reversible cyberattack and restoring data from backup is another way to reverse a ransomware attack and restore the original system

software. Unfortunately, restoring large amounts of data from backup can take significant time and leave systems nonfunctional for long periods. The restoration process is often very slow due to the large amount of information being restored and the fragmentation often associated with this information (Li et al., 2020). Finding the information that must be restored may not be easy if it is stored in many places, and restoration may require trail-and-error methods which take much time. Backing up data frequently and keeping stored data at a remote location can also be burdensome but is necessary if a victim wants to be able to restore their data from backup.

Many levels, methods, and products for backing up the information on a system are possible. Organizations need a backup retention strategy to determines the quality of the restoration. (De Guise, 2009, Chapter 3). A good method for backup retention is the dependency-based retention which means that the recovery of the filesystem is reliant on the last full backup and the intermittent backups are only saved if they replace all previous data. Three types of system recovery exist within a backup retention strategy to achieve an effective recovery. Last filesystem view recovery is necessary because it can recover the filesystem the way it was saved in the last backup. Point-in-time recovery is necessary because it allows the administrators of a system to choose what saved version of the filesystem is restored and when. Lastly, non-index recovery is necessary because it allow recoveries when an index for a backup is unavailable.

Storing the backed-up data remotely from the system is essential to prevent the backup site from being attacked as well (Min et al., 2020). This can require significant overhead storage to keep the important information of a busy organization. Backup restoration takes time, so more damage can occur during an ongoing attack even while backup restoration is happening. In serious attacks, restoration may be started without the organization knowing the full extent of the attack, and wasting time on unnecessary restoration in the meantime while missing important restorations that they need to do. A defender attempting to restore data from backup could increase collateral damage unlike if the attacker restored only the parts that were attacked.

E. PREVIOUS WORK ON REVERSIBLE CYBERATTACKS

Reversible cyberattacks can use four major methods (Rowe, 2010). Cryptographic attacks involve the attacker concealing the victim's information, and can be easily reversed because the attacker can restore the victim's information by decryption once the attack is over (Kolodenker et al., 2017). Encryption can act upon information local to a system, information in transit, or transiting information going to or from the victim. It is easily detectable because encryption changes normal programs and software on a system. Encryption attacks can be thwarted by a victim restoring their information from backup but only if the victim is consistently backing up their data. The process of encryption and decryption are also only possible if the defending system has enough free space and time for processing.

Obfuscating attacks make information difficult to understand by rearranging software within a system or changing data values without encrypting it; they can be reversed by undoing their damage in the reverse order if the changes were known or could be inferred. When applied to malware, it can get past antivirus scanners (You, 2010). The advantage of an obfuscation attack is that different methods could be required to reverse the attack, unlike encryption where one general method will reverse it. Obfuscation attacks can also be used in conjunction with cryptographic methods to make the attack more difficult to break.

Attacks can also withhold information, as by intercepting information being sent before it is received. A variant is a man-in-the-middle attack where the attacker modifies information before it is received; if the changes are reversible, the attack can be reversed. Information-withholding attacks prevent the user from seeing key information they need by allowing the attacker to control what the victim has access to. Attack reversal would be to allow the victim to restore their normal traffic

Finally, resource-deception attacks can modify metadata (data about data) to mislead victims; they can be reversed by providing the true information. Resource-deception attacks confuse a user the state of the resource on their system. The system could show false error messages or false warnings which would prompt the victim to take

unnecessary actions. The victim can foil this kind of attack by reinstalling the system software.

Not all reversals of reversible cyberattacks are equally easy, as they depend on the details of the attack (Rowe, 2010). A responsible reversible cyberattack must still be focused to avoid collateral damage, just as with any cyberattack. It must avoid physically harming civilian populations or impeding companies that operate within the borders of the attack. To be effective, it must also be disguised so it cannot be detected until its intended effects are accomplished. Then, the victim of a ransomware attack should be told who the attacker is, so that the victim understands what is required of them; this is unlike most cyberattacks in which the attacker wants to be anonymous, like attacks of terrorist or hacktivist groups. The goals of reversible cyberattacks are to operate more ethically than other types of cyberattacks while still achieving the same outcome and to strategically advance military objectives more effectively than available alternatives.

F. STRATEGIC USE OF REVERSIBLE CYBERATTACKS

Reversible cyberattacks have both strategic advantages and disadvantages. A traditional cyberattack can be more strategically beneficial than a reversible cyberattack when permanent damage to a country's infrastructure will have more effect than attempting cyber coercion through a reversible cyberattack. On the other hand, reversing a cyberattack can result in less final damage as a traditional cyberattack while achieving the same effect temporarily. This means that a reversible cyber counterattack to prevent a malicious attack could be more moral that using a traditional cyberattack which could offer strategic advantages by encouraging the victim and future victims to comply to demands. A reversible cyberattack could prevent a foreign organization from committing an unjust attack, while allowing a return to normal when the victim demonstrates clear abandonment of their attack. Though reversible cyberattack methods can allow a return to normal, some effects can make this impossible, like in the Stuxnet cyberattack where irreversible damage prevented return to normal. Reversible cyberattacks may improve the effectiveness of offensive cyber operations because of the improved coercive effect (Lewis, 2015).

Reversible cyberattacks can be considered either offensive or defensive due to the circumstances. Cyber coercion could use offensive actions with a defensive purpose as a counterattack. Unlike other forms of cyber coercion, a reversible cyberattack is more controllable by length and severity of the attack, and permits more strategic actions to be taken. Traditional forms of cyber coercion are offensive and could require careful management to avoid escalation and long-term damage but reversible cyberattacks offer a major strategic advantage by being less-escalatory (Lewis, 2021).

III. DETAILS OF REVERSIBLE CYBERATTACKS

Although cyberattacks can be effective in cyberwarfare, they are not always usable or desirable. Reversible cyberattacks require attention to detail, complexity, and sophistication to succeed in practice. This chapter evaluates and analyzes the features of traditional cyberattacks which must be considered in the operation, goals, and strategy of a reversible cyberattack. We also address locations where a reversible cyberattack could attack and when each could be beneficial.

A. POSSIBLE REVERSIBLE CYBERATTACKS

Any individual or organization that uses technology is vulnerable to a cyberattack (Kamiya et al., 2018). Large organizations that rely on technology are often a preferred target for cyber attackers, especially if that organization can offer some strategic advantage. Organizations in the United States or holding United States citizens' information can be a desirable target for an adversary. United States government organizations are also a desirable target to many nation-state adversaries who have advanced intelligence-gathering cyber capabilities.

The most common cyberattacks are distributed denial-of-service (DDoS), man-in-the-middle packet interception, eavesdropping, phishing, drive-by downloads, cross-site scripting, password cracking, database injection, and malware attacks (Biju et al., 2019). Attacks can be used to infiltrate and modify systems to cause different effects. The cyberattacks most suitable for a reversible cyberattack will now be explained.

1. Denial-of-Service Attacks

Denial-of-service attacks are common with ransomware (McIntosh et al., 2021). Denial-of-service attacks can exhaust resources from the victim, like network bandwidth, computing power, or storage (Hussain, et at., 2003). They can flood the victim with requests over the Internet to impede necessary traffic. They can exploit software bugs in the victim to disable their system or software. Denial of service is reversible because the attacker can stop sending packets to the victim systems to stop the resource exhaustion.

The attacker can also save packets blocked during the attack and restore them later for better reversibility.

2. Man-in-the-Middle Attacks

Man-in-the-middle attacks intercept traffic between two trusted sources (Pingle et al., 2018). These attacks are common in ransomware attacks due to their easy reversibility but not all man-in-the-middle attacks are reversible. The Stuxnet cyberattack, for example, used a man-in-the-middle attack method and caused irreversible damage to physical objects and long-term damage to cyber capabilities that is not reversible. Man-in-the-middle attacks can exploit character injection, packet filtering, automatic password collection, secure-shell support, Web services, point-to-point tunneling, and connection termination to affect what is being seen by the victim system. Man-in-the-middle attacks can also intercept, send, or receive data sent to the victim without the victim's knowledge. They can be damaging because they can go long periods unnoticed with a large effect on the victim.

3. Drive-by-Download Attacks

Drive-by download attacks are attacks where malicious content is delivered by Web browser, either in Web pages or in additional downloaded files (Le et al., 2013). The pages or downloads can be deleted in some cases for reversibility, but if they involve persistence malware, they could have additional effects that could be hard to trace and undo. In a military setting, this attack can render ineffective as few Internet searches are done on non-secure web pages and the systems are generally well protected (Oz et al., 2022).

4. Malware Attacks

Malware attacks can involve viruses, works, Trojans, rootkits, ransomware, spyware, and other methods (Rudd et al., 2017; Biju et al., 2019). They install malicious software on a victim's computer without their consent, and can be hidden by being attached to legitimate software. If they can obtain administrator privileges, their code can access parts of a system that are otherwise secure, like private networks, sensitive information, user data, and various other kinds of private sections. They can also use capabilities like rootkits to allow malicious code to bypass protection systems. Malware attacks can use

ransomware methods: Use an encryption key to encrypt files on a disk, send that to a server, and then remove the copy from the victim's system. This type of attack is reversible by providing the encryption key to restore files from the victim. Damage to code and data in the cyber domain is reversible, but not the effects of that damage such as the ability to do espionage.

B. HOW REVERSIBLE CYBERATTACKS COULD WORK

The steps in a reversible cyberattack can be very similar to those of a sophisticated ransomware attack. The steps in most ransomware attacks are infection, communication with command and control, damage, extortion, and remediation (Oz et al., 2022). In the infection phase, the ransomware is delivered into a victim's system. In the communication with command-and-control phase, malicious software will connect to the command-and-control server to report essential security information. In the damage phase, the ransomware will do encryption or other methods to disable a system. The extortion phase alerts the victim to the requested ransom and may share the attack details. If a ransom is received, a remediation phase will connect to the system and undo the effects of the attack.

The phases in common ransomware attacks are similar to those of an advanced persistent threat (APT). Steps in advanced persistent threats vary, but eleven steps occurred in the Colonial Pipeline cyberattack (Alvee et al., 2021):

1. Initial access
2. Execution
3. Persistence
4. Privilege escalation
5. Evasion
6. Discovery
7. Lateral movement
8. Collection

9. Command and control

10. Inhibit response function

11. Impair process control

Some of these steps are harder to achieve than others. For example, privilege escalation tries to gain higher access levels, like administrator privileges which is far more difficult because they are protected by harder-to-guess passwords and multiple-factor authentication. In may seem easier to find a vulnerability in a system and exploit that without using privilege escalation, but the number of such vulnerabilities on systems is generally small and they can get fixed unexpectedly.

A reversible cyberattack can follow the steps and phases of APT attack structure. For a sophisticated attack against a nation-state, the attacker must gain administrator access to disable defense and detection mechanisms which will allow it to remain persistent (CyberArk, 2016; Oz et al. 2022). Gaining administrator access can be done by a drive-by download attack or a phishing attack in which malicious code is downloaded to the victim system. A man-in-the-middle attack, an eavesdropping attack, or a vulnerable Web server can try to intercept credentials to also help the attacker escalate privileges. Once the attacker has administrator privileges, they can install malicious software onto the system, hide or disguise it, and install their tools to improve their effectiveness. Then the attacker controls the system. Once the malicious software is installed on the system and the attacker has administrator access, the target information can be hidden or encrypted. This can be done by downloading an executable file onto the victim system and running it. It could do several things, such as encrypting files, obfuscating files, allowing the attacker access to the system, or adding features to the file like a different file extension which would make them unusable (Unitrends, 2020). A reversible cyberattack must also be sufficiently sophisticated as to make it difficult or impossible for the victim to reverse it on their own other than restoring from backups. Four good techniques are cryptography, obfuscation, information withholding, and resource deception as discussed in section II.E.

C. POSSIBLE TARGETS FOR REVERSIBLE CYBERATTACKS

Reversible cyberattacks can attack different parts of a system, either the operating system (OS), the applications software, or the critical data the system contains or produces. Different attack locations offer advantages and disadvantages for the attacker so the effectiveness and importance of these targets varies depending on the system's features and attacker's goals. Different types of attacks may also be more suitable for different targets.

Attacking the operating system is common in ransomware but could be less effective in nation-state attacks since the victims could redownload their operating systems to recover. This is necessary occasionally so there are effective ways to do it from backup. There are, however, advantages as many vulnerabilities in operating systems could make gaining access to the system easier for the attacker. This could be useful if the attack is time-sensitive or a vulnerability is already found in the operating system that can be exploited. Due to the likelihood of backup restoration in this target, victims with vulnerable backup data may be a better target to decrease the likelihood for a failed attack.

Attacking the applications software, like weapons systems, can be an advantage to the attacker because backups may be missing if software came from different vendors at different times. This increases the difficulty for the attacker to find and attack the different versions. This target can be advantageous if the strategic goal of the attacker is to immediately disable an application software for attack prevention. This can also be used in timely matters since disabling applications software can quickly hinder a victim and prevent them from using their attacking mechanisms.

Attacking the critical data that the system contains or produces, like an employee database, could require searching an entire system to find the files. They can be located anywhere in the system and could be archived which could make it difficult for the attacker to find and attack. Gaining access to the critical data on a system could be advantageous if the attackers' goals were to find that critical data and use it against the victim. This target could also be advantageous if the attacker keeps the data for further cyber coercion if the attacker reverts to their original plan after reversal.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SECURITY AND ETHICAL ISSUES IN ATTACK REVERSAL

Reversing a cyberattack requires restoring all the important parts of a system and limiting long-term effects. Although it is generally easier than doing a cyberattack since the specific attacked locations are known, other important factors should be considered like security systems of the target system and doing reversal in a way that permits future cyberattacks. Ethical implications to a reversible cyberattack must also be addressed.

A. ASPECTS OF CYBERATTACK REVERSAL

Only certain attacks allow efficient or possible reversal. Generally, there must be an initial step of reversal that stops the attack. For example, if a system was subject to a denial-of-service attack, the attacker must restore service; if the attack used false error messages, the attacker must stop them. If malware was used in the attack, it should be removed from the system. If malware encrypted files, they should be decrypted and files that were deleted from the system or modified should be restored. Information recovery may not completely restore the damage that was done. Take the Stuxnet cyberattack for example. In this attack, the aspects of the worm could have been reversible, but the physical damage to the Iranian centrifuges that it caused were not reversible. Depending on circumstances, reversible cyberattacks may contain irreversible aspects if they affect timely operations or objects outside the cyber domain.

1. Reversal of Specific Attack Types

In an obfuscation attack, data is not hidden but just difficult to understand. Given the many ways information can be obfuscated, it can be difficult for the victim to reverse-engineer the obfuscation (Dalai et al., 2017). An example is obfuscation by an exclusive-or with a key that is very difficult to guess, like a one-time pad (Kissel, 2005). But there are many possible reversible mappings of bytes and it is difficult to recognize the one that has been used on some data. While obfuscation attacks make reversal difficult, improving the sophistication of the obfuscation can reach the same effect as an encryption (Rowe, 2010).

A cryptographic attack conceals information in a way that is not easily reversible without a key. To reverse an encryption, the attacker could either restore the original from their own backup or decrypt the victim system using the decryption key; the latter could be faster since it could minimize network data transfer, but would likely reveal something of the attack methods and targets if the victim monitors the repair. An important aspect of public-key cryptology keys is not reusing the encryption or decryption key. Reusing the same keys can allow defenders to share this information and potentially stop this attack in the future. An encryption strengthened by later applying an exclusive-or algorithm can make reversal impossible for a defender because the algorithm obfuscates the encryption and both must be solved to reverse the attack.

Information-withholding attacks conceal information from the victim and intercept information before they get to the victim system to prevent their access to it. Reversal removes the blocking and returns the blocked data. This could be done in hardware, software, or in a network.

A resource-deception attack provides false information about the state of a resource. Revealing the deception reverses it. These attacks can be effective against many cyber defenses since many false positives generated by cyber defenses can occur and they can look normal (Clark & Mitchell, 2019, Chapter 1).

B. IRREVERSIBLE EFFECTS OF ATTACKS

Some situations may not require full restoration of a system to its initial state. Some routine activity may not be important to restore, only the important data and software on a system, and some files may be too costly to restore such as routine log data. Partial reversal could also be useful in preventing future counterattacks by the defender. Nonetheless, any partial reversal could still seem to leave unjust damage to the defender and raise questions of fairness.

Data recovery may not completely restore the collateral damage done by an attack, however. In the Stuxnet cyberattack, for example, some aspects of the worm could have been reversible, but the physical damage to the Iranian centrifuges was irreversible.

Nonetheless, the amount of collateral damage may be acceptable according to the law of armed conflict in view of the objectives achieved (International Committee of the Red Cross [ICRC], 2002).

Aside from physical damage, irreversible effects can include loss of strategic or tactical opportunity with military actions. This includes loss of an ongoing sensor data streams such as intrusion detection alerts. Such temporary harms are generally acceptable by the law of armed conflict.

C. SECURITY SYSTEMS INVOLVED IN REVERSAL OF A CYBERATTACK

Many security systems like firewalls and intrusion-detection systems (IDS) can catch dangerous code and block it from entering a system. These systems are well understood in the aspect of committing a cyberattack, but they may also pose obstacles to reversing an attack. Keeping secret the details of both the attack and the repair makes it more difficult for the victim to reverse a similar attack on their own in the future.

Getting into a system to reverse the attack could be harder than the initial attack if the first attack alerted the victim and the victim removed vulnerabilities and added more security measures. For example, once an initial phishing attack is committed, the victim will be alert for more phishing attacks, and it is unlikely that another attempt will succeed. This means it will be unlikely that the attacker can maintain access to the system, as with an open port connection or a new user account, since those can be easy for the victim to detect. That means that reversal generally requires cooperation of the victim, and secrets of the attack may be revealed in the reversal process.

It is undesirable that a reversible attack disable security subsystems, as this will make it easy for the victim to recognize they have been attacked since most systems constantly monitor their security subsystems. New access for reversing may be easier to gain if security systems are still enabled. However, a new kind of attack will generally be necessary to gain the access needed to reverse the previous attack, since the victim has likely hardened their system against the original attack in the meantime. They may also

have been induced to make a major security upgrade, in which case the attacker may need to try many attacks until they can find one that lets them to get access to reverse the original attack. Reversing an attack is not always straightforward.

D. ETHICAL STANDARDS

Cyber warfare can harm people, so we need a moral standard for how to use it (Kerstein, 2019). Depending on circumstances, an ethical obligation to use a reversible cyberattack instead of traditional cyberattack, could occur. For example, when a cyberattack is necessary, using a reversible cyberattack can limit or eliminate long-term effects. If the target is critical infrastructure or civilians, reducing or eliminating long-term effects once an adversary has surrendered could be a moral obligation, similarly to how a less-harmful cyberattack could be ethically preferable to a traditional physical attack (Denning, 2008). Consider a cyberattack which accidentally damaged the critical infrastructure of a large city. If the cyberattack were reversible, the attacker could restore critical infrastructure after a surrender and the civilians of the attacked nation would not suffer longer than necessary. The incentive of restoring critical infrastructure quickly could encourage the attacked country to submit to demands. On the other hand, a traditional cyberattack could be more ethical if there is reason to think that the target will continue its previous course anyway after reversal.

One consideration in choosing a traditional cyberattack versus a reversible cyberattack is the difficulty of the victim restoring their information from backup, given that backups require time and efforts to restore. Backup restoration takes considerable time but reversible attacks can reverse their damage quickly when well designed. Additional collateral damage may also occur during backup restoration because of the victim's inability to completely understand the severity of the attack. The time and resource expenditures of backup restoration may hinder the victim more than the initial attack. This is particularly an issue for countries with limited cyber infrastructure and few trained personnel.

V. CONCLUSIONS AND FUTURE WORK

The cyber domain differs from other military domains in important ways and reversible cyberattacks permit the unusual opportunity to undo an attack and the damage it has caused. Thus, a reversible cyberattack in warfare can be an advantage strategically and ethically. With the many differing effects that a cyberattack can have on an organization, reversing these short-term and long-term effects has many benefits strategically and ethically.

Strategically, using a reversible cyberattacks provide additional options for counterattacks. Counterattacks are necessary in warfare, and a reversible cyber-counterattack can prevent a malicious action from occurring in a different way than cyber defense. In addition, a surprise cyber-counterattack can catch a potential attacker off guard. A reversible cyberattack also has a unique advantage by introducing an ultimatum, proving it is a true threat, and then offering reversal of the attack once specified conditions are agreed to.

The various types of reversible cyberattacks and their ability for reversal can be chosen consistent with strategic goals. Cyberattacks that use reversible techniques are generally not much more difficult to reverse than non-reversible techniques; often they use some activity that can be reversed by stopping it. Reversible attack implementations can also include methods that prevent the victim from easily reversing the attack on their own as from backup copies.

In some situations, reversible cyberattacks may be a moral obligation if there is a danger that cyberattacks would also harm civilians in violation of the rules of armed conflict. This could occur when a cyberattack could cause lasting harm to civilians for an extended period of time, either directly or through logical critical infrastructure. The information discussed in this thesis suggests further work focusing on the implementation of reversible cyberattacks. Many details need to be worked out for the types of reversible attacks and their applicable situations. After experimentation, reversible cyberattacks can be implemented in the United States military.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Sci Eng Ethics*, *25*, 993–1006. https://doi.org/10.1007/s11948-016-9864-0

Alvee S. R. B., Ahn, B., Kim, T., Su, Y., Youn, Y., & Ryu, M. (2021). Ransomware attack modeling and artificial intelligence-based ransomware detection for digital substations. *2021 6th IEEE Workshop on the Electronic Grid (eGRID),* 1–5. https://doi.org/10.1109/eGRID52793.2021.9662158

Biju, J. M., Gopal N., & Prakash A. J. (2019). Cyber attacks and its different types. *International Research Journal of Engineering and Technology, 6*(3), 4849–4852. https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf

Blinov, O. & Djankov, S. (2022). Ukraine's recovery challenge. In L. Garicano, D. Rohner, & B. Weder di Mauro (Eds.), *Global Economic Consequences of the War in Ukraine: Sanctions, Supply Chains and Sustainability* (pp. 164–168). CEPR Press.

Boddens Hosang, J. F. R. (2020). *Rules of engagement and the international law of military operations*. https://doi.org/10.1093/oso/9780198853886.003.0001

Clark, R. M. & Mitchell, W. L. (2019). *Deception: counterdeception and counterintelligence*. SAGE Publications, Inc.

CyberArk. (2016, August 2). CyberArk labs: new research analyzes ransomware behavior and evolving enterprise risk. *CyberArk: The Identity Security Company*. https://www.cyberark.com/press/cyberark-labs-ransomware-research/

Dalai, A. K., Das, S. S. & Jena, S. K. (2017). A code obfuscation technique to prevent reverse engineering. *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 828–832. https://doi.org/10.1109/WiSPNET.2017.8299877

Datto (2020, August). Datto's global state of the channel ransomware report. Datto. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf

De Guise, P. (2009). *Enterprise systems backup and recovery: a corporate insurance policy*. [E-reader version]. https://doi.org/10.1201/9781420076400

Denning, D. E. (2008). The ethics of cyber conflict. *The handbook of information and computer ethics*, 407–428. https://doi.org/10.1002/9780470281819.ch17

Douple, E. B., Mabuchi, K., Cullings, H. M., Preston, D. L., Kodama, K., Shimizu, Y., Fujiwara, S., & Shore, R. E. (2013). Long-term radiation-related health effects in a unique human population: lessons learned from the atomic bomb survivors of Hiroshima and Nagasaki. *Disaster Medicine and Public Health Preparedness*, *5*(1), 122–133. https://doi.org/10.1001/dmp.2011.21

Faix, M. (2014). Rules of engagement – some basic questions and current issues. *Czech Yearbook of Int. Law*, *1*, 133–145. https://ssrn.com/abstract=2458884

Fox S. C. & Haines, D. D. (2014). Acute and long-term impact of chemical weapons: lessons from the Iran-Iraq War. *Forensic Science Review*, *26*(2), 97–114. https://pubmed.ncbi.nlm.nih.gov/26227026/

Fox, A. (2023, January 10). Half of ransomware attacks have disrupter healthcare delivery. JAMA report finds. *Healthcare IT News*. https://www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds

Ganfure, G. O., Wu, C., Chang, Y., & Shih, W. (2022). DeepWare: Imaging Performance Counters with Deep Learning to Detect Ransomware. *IEEE Transactions on Computers*, *72*(3), 600–613. https://doi.org/10.1109/TC.2022.3173149

Gangwar, K., Mohanty, S., & Mohapatra, A. K.(2018). Analysis and detection of ransomware through its delivery methods. *Data Science and Analytics*, *799*, 353–362. https://doi.org/10.1007/978-981-10-8527-7_29

Geiss R., & Lahmann H. (2013). Cyber warfare: applying the principle of distinction in an interconnected space. *Israel Law Review*, *45*(3), 381–399. https://doi.org/10.1017/S0021223712000179

Genç, Z. A., Lenzini, G., & Ryan, P. Y. A. (2018). Security analysis of key acquiring strategies used by cryptologic ransomware. *Central European Cybersecurity Conference 2018 (CECC 2018)*, 1–6. https://doi.org/10.1145/3277570.3277577

Gonzalez, D. & Hayajneh, T. (2017). Detection and prevention of crypto-ransomware. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 472–478. https://doi.org/10.1109/UEMCON.2017.8249052

Hirschfelder, J. O. (2015). The effects of atomic weapons. *Bulletin of the Atomic Scientists*, *6*(8-9), 236–286. https://doi.org/10.1080/00963402.1950.11461276

Hussain, A., Heidemann, J., & Papadopoulous, C. (2003). A framework for classifying denial of service attacks. *SIGCOMM '03: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 99–110. https://doi.org/10.1145/863955.863968

Ichikawa, H. (2009). Children after the war: long lasting sufferings and invisible threats. *IPSHU 研究報告シリーズ, 42,* 255–271. https://heiwa.hiroshima-u.ac.jp/Pub/42/14Ichikawa.pdf

International Committee of the Red Cross. (2002, June). *The law of armed conflict: basic knowledge*. https://www.icrc.org/en/doc/assets/files/other/law1_final.pdf

Jasper, S. (2021, June 1). Assessing Russia's role and responsibility in the Colonial Pipeline attack. *New Atlanticist*. https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/

Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms [Working Paper]. National Bureau of Economic Research. https://www.nber.org/papers/w24409

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 4490–4494. https://doi.org/10.1109/IECON.2011.6120048

Kehler C. R., Lin, H., & Sulmeyer, M. (2017). Rules of engagement for cyberspace operations: a view from the USA. *Journal of Cybersecurity*, *3*(1), 69–80. https://doi.org/10.1093/cybsec/tyx003

Kerstein, S. (2019). Treating persons as means. In E. N. Zalta (Ed.), *Stanford Encyclopedia of Philosophy* [E-reader version] (Summer 2019 ed.). Metaphysics Research Lab, Sandford University. https://plato.stanford.edu/archives/sum2019/entries/persons-means/

Kissel, Z. A. (2005). Obfuscation of the standard XOR encryption algorithm. *XRDS: Crossroads, The ACM Magazine for Students*, 11(3), 6. https://doi-org.libproxy.nps.edu/10.1145/1144396.1144402

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019) Ransomware, threat and detection techniques: a review. *IJCSNS*, *19*(2), 136–146. https://seap.taylors.edu.my/file/rems/publication/105055_5256_1.pdf

Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017). PayBreak: defense against cryptographic ransomware. *ASIA CCS '17: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 599–611. https://doi.org/10.1145/3052973.3053035

Le, V. L., Welch, I., Gao, X., Komisarczuk, P. (2013). Anatomy of a drive-by download attack. *AISC '13: Proceedings of the Eleventh Australian Information Security Conference*, *138*, 49–58. https://dl.acm.org/doi/10.5555/2525483.2525489

Lewis, J. A. (2015). The role of offensive cyber operations in NATO's collective defense. *The Tallinn Papers*, (8), 1–12. https://www.ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf

Lewis, J. A. (2021). Toward a more coercive cyber strategy: remarks to U.S. cyber command legal conference. *Center for Strategic & International Studies*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210310_Lewis_Cyber_Strategy.pdf?VersionId=vWWwFUld1a_iv.OI9edoEALt0KeBxNpI

Li, P., Hua, Y., Cao, Q., & Xhang, M. (2020). Improving the restore performance via physical-locality middleware for backup systems. *Middleware '20: Proceedings of the 21st International Middleware Conference*, 341–355. https://doi.org/10.1145/342321103425691

Lightfoot, L. (2022, November 24). The top 10 biggest cyber attacks of 2021. Expert Insights. https://expertinsights.com/insights/10-high-profile-attacks-2021/

Litan, R. (2022, March 16). Russia can be made to pay for Ukraine damage now. *Bloomberg*. https://www.bloomberg.com/opinion/articles/2022-03-16/russia-can-be-made-to-pay-for-ukraine-damage-now?leadSource=uverify%20wall

MacRae, J. & Franqueira, V. N. L. (2018). On locky ransomware, Al Capone and Brexit. *Lecture Notes of the Institute of Computer Sciences*. https://doi.org/10.1007/978-3-319-73697-6_3

McIntosh, T., Kayes A. S. M., Chen Y. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: a comprehensive review, research challenges, and future directions. *ACM Computing Surveys*, *54*(9). https://doi.org/10.1145/3479393

Min, D., Ko, Y., Walker, R., Lee, J., & Kim, Y. (2022). A content-based ransomware detection and backup solid-state drive for ransomware defense. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 41(7), 2038–2051. https://doi.org/10.1109/TCAD.2021.3099084

Moussaileb, R., Bouget., B., Palisse, A., & Bouder, H. (2018). Ransomware's early mitigation mechanisms. *Proceedings of the 13th international Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3230833.3234691

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: evolution, taxonomy, and defense solutions. *ACM Computing Surverys, 54*(11). https://doi.org/10.1145/3514229

Pingle, B., Mairaj, A., & Javaid, A. Y. (2018). Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use. *2018 IEEE International Conference on Electro/Information Technology*, 192–197. https://doi.org/10.1109/EIT.2018.8500082

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: issues and challenges. *Computers & Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Rowe, N. (2010). Toward Reversible Cyberattacks. *9th European Conference on Information Warfare*, 261–267. https://faculty.nps.edu/ncrowe/rowe_eciw10.htm

Rudd, E. M., Rozsa, A., Gunther, M., & Boult, T. E. (2017). A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions. *IEEE Communications Surveys & Tutorials*, *19*(2), 1145–1172. https://doi.org/10.1109/COMST.2016.2636078

Sumi, F. H., Dutta, L., & Sarker, F. (2019). A review on cyberattacks and their preventative measures. *Int'l Journal of Cyber Research and Education*, *1*(2), 12–29. https://doi.org/10.4018/IJCRE.2019070102

Tabansky L. (2011). Basic concepts in cyber warfare. *Military and Strategic Affairs*, *3*(1), 75–92. https://www.inss.org.il/wp-content/uploads/2017/02/FILE1308129610-1.pdf

Unitrends. (2020). How ransomware works. *Unitrends: A Kaseya Company*. https://www.unitrends.com/solutions/ransomware-education

You, I. & Yim, K. (2010). Malware obfuscation techniques: a brief survey. *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, 297–300. https://doi.org/10.1109/BWCCA.2010.85

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California