REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
(08-06-2018)	FINAL	

4. TITLE AND SUBTITLE

Ethical Dilemmas of Weaponizing Commercial Cyber Technologies

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Stephen Fulkerson

Paper Advisor (if Any): **Dr. Chris Demchak, Dr. Hank Brightman, Dr. Thomas Creely, and Dr. Timothy Schultz.**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Ethics and Emerging Military Technology
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

For Example: Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the U.S. Naval War College faculty in satisfaction of the requirements of the Ethics and Emerging Military Technology graduate certificate program. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Cyber commercial-off-the-shelf (COTS) technologies are affordable and have the potential to be used as an offensive weapon. It is only a matter of time before belligerent governments begin to weaponize these COTS technologies to meet political objectives. When a cyber-attack using COTS happens and there are collateral damages that negatively impact the innocent cyber technology company, who should be held accountable? There are laws, social norms, ethics, and expert recommendations that help guide a government's responsibility should there be collateral damage. While many ethical foundations should drive the government's response to collateral damage, deontology, or ethics of duty, should play the strongest role within western democratic nations in establishing the belligerent's responsibility to pay reparations for any collateral damages to the cyber company.

15. SUBJECT TERMS

Cyber, cyberwarfare, cyber-attacks, Deontology, Ethical Dilemmas, Commercial Technologies, Commercial-off-the-shelf, COTS, Ethics of Duty, Duty, Ethics of Virtue, Utilitarianism, Ethics of Greater Good,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Director, EEMT Dept.
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		**36**	401-841-7542

Standard Form 298 (Rev. 8-98)

This page is intentionally left blank.

CONTENTS

ACKNOWLEDGEMENTS

I would like to extend my sincere gratitude to Dr. Chris Demchak, Ph.D., Director of the Center for Cyber Conflict Studies Strategic and Operations Research Department in the United States (U.S.) Naval War College for her guidance and assistance during the research and development of this cyber paper. Likewise, I would like to thank Dr. Hank Brightman, Ed.D., EMC Informationist Chair, and Professor in the College of Maritime Operational Warfare at the United States Naval War College, for his outstanding recommendations and review of the material of this paper. Furthermore, I would like to thank Dr. Thomas Creely, Ph.D., Director, Ethics and Emerging Military Technology Program at the United States Naval War College for his encouragement, guidance and direction in this project. He opened my eyes to critical thinking on many ethical issues that I had previously not considered. I am very grateful to Dr. Yvonne R. Masakowski, Ph.D., Associate Professor of Strategic Leadership and Leader Development for her sponsorship in my selection for this program and Dr. Tim Schultz, Dean of Electives, for his continued encouragement and support. I am thankful for the research team of Isabel Lopes, Research and Instruction, and Stephen Poirier, Intern, at the U.S. Naval War College for their assistance in research of the case studies. Also, I extend my gratitude to Dr. Kevin P. Eubanks, Ph.D., Associate Professor of Writing at the U.S. Naval War College, for his thorough review and feedback on this research paper. I am very grateful to God for allowing me to attend the U.S. Naval War College and to be selected for the Ethics and Emerging Military Technology program. Lastly, I would like to extend my profound gratitude to my wife, Katy, and two daughters, Lauren and Lily, for supporting me during this period of research and writing.

NAVAL WAR COLLEGE

Newport, RI

Deontology: Ethical Dilemmas of Weaponizing Commercial Cyber Technologies

By

Stephen Fulkerson

LCDR / USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Graduate Certificate in Ethics and Emerging Military Technology based on the following topic:

QUESTION: "When a government exploits civilian cyber companies' technologies for national security issues and the company loses business as a result, what are the ethical responsibilities of the belligerent?"

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ***Stephen Fulkerson***

June 8, 2018

PAPER ABSTRACT

Cyber commercial-off-the-shelf (COTS) technologies are affordable and have the potential to be used as an offensive weapon. It is only a matter of time before belligerent governments begin to weaponize these COTS technologies to meet political objectives. When a cyber-attack using COTS happens and there are collateral damages that negatively impacts the innocent cyber technology company, who should be held accountable? There are laws, social norms, ethics, and expert recommendations that help guide a government's responsibility to mitigate the collateral damage. While many ethical foundations should drive the government's response to collateral damage, deontology, or ethics of duty, should play the strongest ethical value within western democratic nations in establishing the belligerent's responsibility to pay reparations for any collateral damages to the cyber company.

INTRODUCTION

When a civilian company is damaged by a government's covert cyber operation using that company's commercial-off-the-shelf (COTS) capability for national security issues, the ethics of deontology (duty) is the best principle to guide the actions of the belligerent government to compensate the business for damages incurred. There are those who would argue that governments cannot be held responsible for using a cyber COTS product differently than how it was designed, nor be held responsible for collateral damages when it was not the government's intention to hurt the cyber company. The actions of the government were not malicious towards the cyber business. However, if the company was damaged by the government's use of their technology for covert cyber-attacks, the business should receive compensation. There are established global norms, ethics, and laws surrounding intent, collateral damage, and reparations that clearly outline how the government should respond to the cyber company. There are also ethics that outline the government's responsibility to pay reparations even if they were never caught in the act of misusing cyber technology for covert operations.

When the law fails to properly guide societies through these conflicts, it is important for ethics to help sort out the issue.[1] Cyber technologies and cyber capabilities are moving faster than the speed of law. There are numerous cyber ethical issues today that have no laws to help societies or governments mitigate a successful outcome. Cyber technologies are inexpensive and have a global reach. Cyber enables individuals, businesses, militaries, and governments to reach out and

[1] George Lucas. *Ethics and Cyber Warfare. The Quest for Responsible Security in the Age of Digital Warfare.* (New York: Oxford University Press, 2017), 40.

affect situations and outcomes like never before in human history. If one were to compare the costs associated with using a cyber-attack versus the costs associated with using traditional armies and navies to engage in an attack, cyber will surface as more cost-effective. In cyber-attacks, there are limited or no requirements needed to pay for the logistics of troop movements. Cyberwarfare can give weaponized strength to a nation that previously did not hold a global position of power. As a result, a nation previously not considered powerful can possibly impact the national theater by using cyber in a positive or negative way.

Cyber COTS technologies are inexpensive which makes them attractive to governments who can identify ways to use them for military purposes. It is possible for governments and non-state actors to use cyber COTS in ways never before intended by the original creators. New commercial cyber technologies are available at a fraction of the cost to the public compared to what governments pay for custom cyber technologies created for national defense purposes. When the military identifies a global cyber COTS application that could be leveraged for national security purposes, it opens the door for vulnerabilities to be exploited. This is especially true when a government uses a foreign nation's COTS product with the intention to use the technology beyond the intended design. The risk the government takes in using a COTS application beyond the scope of design can also include the business receiving negative press or financial losses. In essence, this situation could result in a backlash from the company's loyal customer base disapproving of a perceived cooperation with foreign or domestic governments.

A company has no way to determine or regulate how the public may use its product. When the public determines a new way to use a commercial product, the future use of the invention can change without notice. An example of a well-known current technology is the remote-controlled quadcopter drone that has many purposes. Quadcopters are versatile and have multiple

capabilities, not only in how the military uses them, but also in commercial, and personal applications.[2] The scope of military requirements for the use of quadcopters and drones are typically allocated for intelligence, surveillance and reconnaissance missions (ISR).[3] The drones have additional multifunctional capabilities as law enforcement agencies also equip quadcopters with cameras, radio equipment, and sensors to conduct surveillance and investigations.[4] Law enforcement agencies also use quadcopters for lifesaving activities including disaster response and relief operations.[5] Likewise, aerial photography and videography can be leveraged by law enforcement, military, and commercial companies, such as real estate to take advantage of aerial viewpoints.[6] The largest of these drones are the military drones which today can carry a payload of weapons designed to neutralize their target.[7] Leveraging cyber technologies, a remote pilot can fly these unmanned aerial vehicles from potentially any place on earth with proper equipment and a strong satellite signal. As one can see, these technologies can be used in a simplistic manner or they can be weaponized and used for lethal purposes.

The increased advancements in cyber capabilities challenge the boundaries of what is right and wrong, what is moral, and what is ethical. The United States government and watchdog groups keep a pulse on how products are being used and what safety issues these products may pose to society. However, there are times when the imaginations of the public create new ways to use a product that has lethal outcomes. Does the cyber commercial company, cyber inventor, or cyber creator get a voice in how their invention will be utilized? Most often, businesses cannot control

---

[2] Greg Strimel, Scott Bartholomew, and Eunhye Kim, "Engaging Children in Engineering Design through the World of Quadcopters," *Children's Technology and Engineering* 21, no 4 (May 2017): 9.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Henry Perritt and Eliot Sprague, "Drones," *Vanderbilt Journal of Entertainment and Technology Law* 17, no. 17 (2015): 701.

how their products are used. Mankind's use of technology for purposes other than the intended design is not new. Examples of using technologies in a way not imagined are seen in most wars. For instance, in World War I and II, most nations involved in the wars used weaponized airplanes. However, airplanes that were originally designed for transportation were adapted for the delivery of bombs and mass destruction. However, the Japanese, took weaponized airplanes to another level when they devised the kamikaze pilot. No one ever imagined that an air force would be created with suicide dive-bombers to deliver an arsenal of bombs to destroy their target. Just as aircraft designers did not get a voice in how their aircraft would be used, it is highly unlikely cyber companies will have a voice in how their products will be used.

If people communicated back to the cyber technology company on how they were using their product, it would still be very difficult for the cyber company to police the ethics of customer usage. Furthermore, there are not well-established ethics, laws, or norms surrounding how a person decides to use a technology. It may be unrealistic to believe that people will have the interest to communicate back to the business on how they are choosing to use their cyber products. It would seem logical to assume that users of cyber products most likely will not take the extra step to alert cyber technology companies on how they intend to use their products. Given that it is difficult for a business to police its customers use of its cyber technologies, it is important to examine a hypothetical scenario that could easily happen, if it hasn't already happened.

CYBER ETHICAL SCENARIO

The following hypothetical cyber scenario will be presented to set the stage for possible covert cyber operations that were deployed using COTS technologies and the subsequent ethical issues that resulted. There was a national security threat against a government from a state cyber

actor. A decision was made to neutralize the state actor's computer equipment to remove the threat. If it had been needed, a secondary action would have been to neutralize the state actor if the equipment could not be contained or neutralized. Intelligence reporting suggested that the state cyber actor routinely used a smartphone. Further intelligence reporting indicated that prior to going to bed, the cyber actor placed the smartphone on top of his laptop keyboard to recharge through the computer's universal serial bus (USB) port during the night. The defending government investigated the smartphone used by the state cyber actor and discovered a software code vulnerability in the COTS application. The defending government used the vulnerability of that software code to build an offensive plan that gave them the ability to deploy a precise covert cyber-attack. The government's intelligence that was collected painted a picture of the evening routine which would allow a plan to reprogram the smartphone software during the night when the cyber actor was sleeping. The reprogrammed smartphone software would overheat the lithium battery. The expected outcome would result in the smartphone catching fire, at an established preset time during the middle of the night, while the smartphone owner target sleeps. The expected outcome of this covert action was to force the smartphone to catch fire quickly and destroy the laptop hard drive. The action was expected to stop the cyber actor's ability to continue to use his computer which was believed to have threatening cyber programs.

However, like many military operations, the plan did not execute as designed. Instead of following the normal evening routine, the state cyber actor placed the smartphone on the nightstand by the actor's personal bed. That night, the belligerent government remotely deployed their malicious code into the cyber actor's smartphone at the prescribed time. The cyber actor was asleep and unaware of any activity. By changing the normal routine and placing the smartphone on the bedroom nightstand instead of the office laptop, the smartphone was exposed to the bedroom

curtains. The curtains were neatly draped behind the bedside nightstand and exposed to the overheating smartphone. As a result, the entire bedroom and home were engulfed in a fire. Smoke inhalation eventually killed the cyber actor, and subsequently, the entire family in the process. The military mission would be considered a success for the sponsoring government even though it was a plan B course of action (COA) instead of plan A. The loss of life for the actor and the cyber actor's family members would be considered collateral damage for the needs for national security.

The fire department investigated the cause of the fire. It was determined that the fire started in the vicinity of the smartphone and could have been the cause of the fire. As a result, the remains of the smartphone and computer equipment were sent off to be examined as potential causes for the fire. As investigators examined the smartphone remains, they were unaware of any covert military activities that introduced post-release software code design into the smartphone. Information about the smartphone potentially being the cause of the fire was learned by the news media. The media did not wait to see if there were similar stories about smartphones causing fires. Instead, the press picked up the story immediately and broadcasted that the smartphone could be the reason for the deaths of the entire family. The negative global press was published by newspapers and social media websites. As a result of the media coverage, there were societal demands for recalls on this brand of smartphone. Additional negative press flooded the news, sparking fears and concerns about cell phone battery safety. Meanwhile, the smartphone company stocks plummeted, and their credibility and reputation were put into question on national news. The cyber COTS business was in crisis mode which prompted their public relations teams to be mobilized in order to counter the negative publicity. Company technology teams were deployed to review their software code in order to understand the possible causes for the battery overheating. The smartphone manufacturer allocated all technical teams to examine their software code in order

to find any reason that could have caused their smartphone to overheat. Their findings decisively indicated that the software code that regulates the battery was faulty and the cause for the battery to overheat.

The smartphone battery overheating was not the fault of the business. It was the fault of the belligerent government's cyber covert operations teams that used a vulnerability to change the software code. When this operation was launched, there were no contingency plans developed for what actions would be taken if the smartphone company would be damaged financially. As a result, it is important to evaluate what are the ethical responsibilities and courses of actions the belligerent government should take as a result of this unforeseeable situation. Furthermore, it will be important to evaluate the ethics of the government's responsibility to the business. Should the government allow the cyber business to take the financial hit and potential loses? Or should the government reveal their covert actions and offer reparations? The following research will explore these questions and provide best-practice recommendations.

ASSUMPTIONS AND CAVEATS

There are several assumptions and caveats that must be presented for this ethical dilemma. This scenario is notional and in no way reflects a known real-life classified or unclassified covert military cyber activity. As stated, it is only a hypothetical situation that appears likely to happen as a result of the inexpensive costs of cyber COTS and the possibilities available to state and non-state actors. Historically, the news media would normally hold off delivering a story so quickly without many similar scenarios or situations being replicated multiple times. Times have changed and today, some believe that the media leads with many stories without always checking for facts and truth which allowed this story to quickly go to market. It may not always be likely that a

smartphone could survive a fire as described, but for purposes of this cyber-attack, there were remnants that gave investigators clues as to what happened and identify potential governments that had the software skills and capability to have delivered the cyber-attack.

The scenario and the arguments will be centered predominantly on western democratic governments. There is not enough empirical data from non-democratic nations that have admitted guilt, or documentation proving reparation payments have occurred. However, since there was no data from non-democratic nations, the intent of the information presented will suggest the best course of actions to be taken by any government that would use cyber COTS technologies for offense, defense, and lethal covert operations. The actions taken by the belligerent government were intended to target that actor's equipment, removing hardware and software files that gave the actor dangerous cyber capabilities. The outcome of this scenario was that the covert actions of tampering with the cyber technology's software coding were discovered during the independent investigation when reviewing the phone. Lastly, the assumption of this scenario was that the covert cyber warfare attacks were actions taken without a formal declaration of war to eliminate a target that was considered a threat to national security.

LIMITATIONS

The cyber scenario presents multiple ethical dilemmas. Despite the fact there are many ethical issues and dilemmas to consider in the cyber scenario, the scope will not focus on undeclared war nor will it focus on military lethal actions against non-combatants like the state cyber actor's family. Instead, the focus will be centered on the ethical obligations of the government that used cyber COTS resulting in lethal outcomes and collateral damages. Additionally, the focus will examine the obligations and subsequent responsibilities of the

government to mitigate damages to the cyber company's reputation, and damages to their commercial business. The intent will be to suggest that the actions taken by a government to mitigate damages made to the cyber COTS company should be the same if the company resides in another country. The location of a business should not be a factor that changes the recommendation for the outcome. For purposes of scope, this paper will only examine case studies of Western governments that damaged businesses or people. As discussed, there were limited or no sources about non-democratic nations admitting to damaging businesses or people and their subsequent courses of actions taken.

COMPETING ETHICAL VALUES

The cyber scenario is rich with multiple ethical dilemmas captured in deontology, utilitarianism, divine command, and virtue. These ethics all play a part in defining how the government should respond to the ethical dilemma presented. Deontology, commonly referred to as ethics of duty (or duty ethics), is most notably seen in the military as the ethics that are derived from a duty to follow rules, regulations, orders, and governmental laws.[8] The ethics of duty is best positioned to follow the orders of the government regardless of the outcome. Ethics of the greatest good, commonly referred to as utilitarianism, is the belief that the morally correct action achieves the greatest good.[9] The ethics of divine command is concerned about the loss of life and how that challenges or collides with religious ideologies.[10] Lastly, the ethics of virtue, (or virtue), would

[8] Gabriela Pohoata, "Confucius and Kant or the Ethics of Duty," *Cogito Bucharest* 2, no. 1 (2010) 55.
[9] Jay Avella, "The Dilemma of Ethical Leadership," *Journal of Leadership Studies* 11, no. 2 (2017): 42.
[10] Lawrence Hinman, *Ethics: A Pluralistic Approach to Moral Theory* (San Diego: Harcourt Brace College Publishers, 1998), 76-8.

focus less on your actions and more on what the motive was for taking those actions.[11] For the purposes of further discussion, these four ethics will be called duty, utilitarianism, divine command, and virtue.

From the beginning of the cyber scenario, the government took decisive action against the cyber actor and it was acting ethically from their perspective by following the ethics of duty. The belligerent government believed it had a duty to protect its security and national interest by whatever forces it deemed necessary. The sovereignty and national security of its people were being threatened, and the government believed its duty was to stop the cyber actor before something tragic happened. However, conflicts in perceptions about the ethics of this action are possible. The fact remains that the government modified the cyber COTS technologies to stop the cyber actor. One might argue that the government initially started the activity with a violation of virtue by the fact that they modified a commercial COTS application and should have recognized that they could put that company at risk.

Once the government established that there was collateral damage, the ethics of duty would be strong because there are many rules, norms and proposed laws surrounding a government's responsibility to limit collateral damages during conflicts. Furthermore, duty is strong in its guidance suggesting that it should follow the same established rules of laws, norms, and guidelines to pay reparations for the collateral damages incurred. Competing values could suggest that if the government was based on goodness and virtue, then the government should not have modified the software code of the cyber company. Instead, it should have created its own cyber applications for a cyber-attack that could not potentially damage the business and reputation of a cyber

[11] Michael Lawler and Todd A. Salzman, "Virtue Ethics: Natural and Christian," *Theological Studies* 74, no. 2 (2013), 442-45.

company. If the government was a representation of its people, and its people are positioning themselves as virtuous or good, then the government should have taken steps to ensure the business was not damaged as a result of manipulating their product to target another individual. However, because duty is strong in believing in public accountability, duty is most likely to hold itself accountable and follow through on self-identification. Lastly, the ethics of duty would also believe that its duty requires it to limit the overall costs to the government and people it supports. Despite the competing values against the other three ethics, the ethics of duty would be the strongest value to guide the government on how to limit collateral damage, respond with paying reparations, hold itself accountable to the public, and ensure that the operation has limited overall costs.

Utilitarianism would evaluate the cyber scenario and recognize that the greatest good may require the death and collateral damages to the business in order to achieve the best outcome for the many. Utilitarianism would be moderate in its approach to supporting the collateral reparations by again factoring that the actions taken supported a greater good. Utilitarianism would not likely sympathize with the ethics of divine command regarding the death of the military target and the family members. If more lives were saved by the deaths of those individuals, that would serve the greater good to ensure safety for the masses. Also, in the cyber COTS scenario, both duty and utilitarianism would have their own ethical battles in that, "the ethics of greater good states that consequences matter whereas ethics of duty says that the consequences do not matter but the morality (legality) of the action does."[12] Simply put from a utilitarian perspective, the government's actions which took the cyber actor's life outweigh the bad because other lives were saved as a result of the action. The utilitarian approach would not be as concerned about the public

[12] Michael Lawler and Todd A. Salzman, "Virtue Ethics: Natural and Christian," *Theological Studies* 74, no. 2 (2013), 442-45.

accountability if the purpose did not serve the greater good for the general public. This notion is also true for limiting the overall costs of the cyber operation and subsequent collateral damage. If the greater good would benefit, it would not consider the costs as important as neutralizing the threat.

The divine command ethical practitioners could disagree with virtue in that, regardless of the motive of the government, there are obvious ethical dilemmas which led to the death of the cyber actor and his family members. Divine command followers would prefer to see an adherence to non-violent or non-lethal outcomes that did not put human life in danger. Given this scenario did not land on a traditional battlefield, the loss of innocent lives could have been avoided by following the ethics of divine command. However, it would be apparent that the government used intelligence which suggested that the routine of the cyber actor would allow for the equipment to be neutralized and no lives would be lost. Additionally, based on the information provided that the cyber scenario takes place in a Western democratic nation, there are probably multiple religious beliefs that would be in conflict with the violent outcome. It is in scenarios and situations like this where the ethics of divine command and duty can have a competing interest. Divine command's belief system has been traditionally based on the foundations and principles of religion. Comparing divine command against duty, the foundations of duty are structured around the compliance in following rules, regulations, society norms, laws, and governmental constitutions.[13] However, not every society has laws and norms that will formulate the same sense of ethics of duty and where those boundaries can be challenged by other ethical dilemmas.[14]

[13] Gabriela Pohoata, "Confucius and Kant or the Ethics of Duty." *Cogito Bucharest* 2, no. 1 (2010): 55.
[14] Lawrence Hinman, *Ethics: A Pluralistic Approach to Moral Theory* (San Diego: Harcourt Brace College Publishers, 1998), 77.

Taking a life also introduced ethical issues emanating from the ethics of divine command which would compete with the ethics of duty. The divine command would be the ethical conviction in which religion guides our actions.[15] There are no well-established religious faiths where murder alone is acceptable outside of a perceived God-inspired directive.[16] Especially in some Western democratic nations where Christianity is the dominant faith, the Ten Commandments outline the framework for laws to live by and one of those laws is very clear in stating that murder is against the law.[17] Given that the scenario presented was a military action taken not during a wartime effort, ethics of divine command would also compete with values of the ethics of duty. The divine command would be less concerned about limiting the overall costs of the operation, collateral damages but more concerned about public accountability and taking responsibility for the actions of one's government.

The values that motivate an ethics of virtue compete with the foundational values of the other three. As a result, it would be weaker in usefulness in evaluating the actions to limit the overall costs incurred. Virtue typically aligns with the strong belief in justice. Therefore, limiting collateral damages to the innocent would be an issue with virtue and it, like duty, would expect justice to be served and an injustice to be corrected. Virtue would be moderate in terms of how it would respond to reparations because it would depend on the culture and the situation. Where a situation allowed an apology or financial compensation, the ethics of virtue could potentially

---

[15] Lawrence Hinman, *Ethics: A Pluralistic Approach to Moral Theory* (San Diego: Harcourt Brace College Publishers, 1998), 77.
[16] David Perry, "The Problem of Holy War" (Presentation Adapted from an Ethics at Noon presentation given at Santa Clara University, September 25, 2001).
[17] Lawrence Hinman, *Ethics: A Pluralistic Approach to Moral Theory* (San Diego: Harcourt Brace College Publishers, 1998), 245.

support either situation. It would also not be vested in issues of limiting the overall costs of the cyber operation and subsequent collateral damages.

There have been four ethical dilemmas presented. Each class of ethics categorically presents a unique perspective to guide a government's belief system. There are other factors that should be considered besides ethical foundations. It is important to understand what laws are in place to also guide a government through the process of evaluating their response.

CYBER LAWS

The belligerent government that initiated the covert cyber-attack must be responsible for the damages to the cyber technology COTS smartphone company according to *The Tallinn Manual*, U.N. Article 2(4), democratic social norms, and the ethics of duty. As previously stated, the use of cyber technology is challenging existing laws. Cyber violations that could be perceived as illegal have occurred faster than cyber laws can be created. As a result, it is difficult to ascertain what the laws mandate about cyber-attacks. However, there is an international group of cyber experts that have united to document and capture what they believe to be best practices for cyber laws and a code of cyber ethics that should be followed. These well-known recommendations for international cyber laws are found in *The Tallinn Manual,* and also in *The Tallinn Manual 2.0*. The recommendations found in *The Tallinn Manual* are guidelines focused on the scope of how cyber is being used. Both *The Tallinn Manual* and *Tallinn Manual 2.0* establish the ethical framework for right and wrong in the world of cyber and the recommendations to follow multiple ethical frameworks. The ethics of duty places the greatest focus on following and being in compliance with the guidelines and recommendations. *The Tallinn Manual* does not hold the power of international law but reflects social values and norms of what is right and what is wrong

in cyber-space. *The Tallinn Manuals* both give credence to what a large group of international experts considers right and wrong. Based on ethics that follow rules, the ethics of duty would be the strongest ethic that aligns with *The Tallinn Manual* and helps guide a government to follow those recommendations.

The Tallinn Manual legal cyber framework was developed as a result of the Russian cyber-attacks on Estonia in 2007.[18] The city of Tallinn, Estonia, wanted to move a Russian statue from its current location to another location in hopes that it would reduce the perception of Russian presence in its country.[19] The Russian government was not pleased by this action and launched a direct cyber-attack which negatively impacted normal city and country economical operations.[20] Estonia was attempting to transform its economy and infrastructure to be similar to most other Western states.[21] As a result, Estonia relied heavily on the Internet for its electronic commerce, critical infrastructure, and government operations.[22] Additionally, Estonia's electric banking services, water supply, and electric power grids were all integrated into electronic controls based on the Internet.[23] In Estonia, daily use of the Internet and almost all bank transactions that occurred were enjoyed by approximately half of all Estonians.[24] The cyber-attack against Estonia exposed its vulnerability and reliance on electronic commerce.[25] To protect itself from additional attacks, the Estonian government locked down its network systems removing the ability to access internet

---

[18] David Perry, *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation* (New York: Rowman and Littlefield, 2016), 177.
[19] Ibid.
[20] Ibid.
[21] Herzog, Stephen, "Revisiting the Estonian Cyber-attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 51.
[22] Herzog, Stephen, "Revisiting the Estonian Cyber-attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 51.
[23] Ibid.
[24] Ibid.
[25] David Perry, *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation* (New York: Rowman and Littlefield, 2016), 177

commerce systems.[26] Estonians had to experience very difficult challenges all because they wanted to remove a historic Russian statue.[27] Their city and economy were greatly damaged and significantly inconvenienced. The total costs of damages may still be unknown, but to give a perspective regarding the scope and size of the attack, damages released from one bank which estimated that during the cyber-attack, its business suffered approximately $1 million USD in damages.[28] This figure – if multiplied across many other businesses – paints a picture of very sizeable damages. When the dust settled, an investigation by Estonia was conducted, much like in the cyber scenario presented, and Russia was alleged to be the culprit.[29] All data discovered and presented suggested to a high degree that Russian state-sponsored institutions were involved.[30]

If the Russian government was the belligerent, or if the actions were from a non-state actor, the course of action should be the same. The cyber and legal experts all agreed and clearly stated in Section 2, Rule 6 that it was the State's responsibility for cyber actions taken by the state, by state-contracted efforts, or by independent actors.[31] Regardless if the cyber-attack was state-sponsored or not, the state should be responsible and accountable for actions taken within its territorial borders.[32] From *The Tallinn Manual* community of global experts, their guidelines would indicate that, in this scenario, the Russian government should be held responsible for the cyber actions used in the covert cyber operations. The recommendations from *The Tallinn Manual*

---

[26] David Perry, *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation* (New York: Rowman and Littlefield, 2016), 177.
[27] Ibid.
[28] Herzog, Stephen. "Revisiting the Estonian Cyber-attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 51-52.
[29] Anonymous, "Take That! Putin Underlines Regional Gas Hegemony," *Russian Life* 50, no. 4 (2007): 8.
[30] Ibid.
[31] Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2013), 29-35.
[32] Ibid., 29-35.

experts were notable, but it is important to understand the legal framework as defined by the United Nations (U.N.).

The U.N., which represents over 190 states, has legal frameworks which are agreed upon by all active members, in particular, the definitions and restrictions of the use of force. Like many nations and entities, the U.N. is working to identify vulnerabilities in its legal frameworks that do not clearly capture cyber activities and their relationship to the use of force. However, until such time as those updates are available, all nations are looking at Article 2(4) of the U.N. Charter that says, "all Members of the United Nations shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[33] In legal situations, there are differences of opinions regarding the definitions surrounding the word, *force*. Specifically, there are concerns regarding what force means and how to best interpret the U.N. Article as it relates to actions taken by a state using cyber capabilities. There are some nations who interpret the U.N's Charter to mean that the use of force is specific to physical kinetic force. However, there are many other nations that believe that using cyber is a force and those who use cyber as a force are ethically and legally accountable to U.N. Article 2(4) for their actions.

The United Kingdom was quick to take a position regarding its interpretation of the definition of cyber being considered a force. Subsequently, the United Kingdom's "National Security Strategy emphasizes that 'activity in cyberspace' is 'a military weapon for use by states and possible others' and the U.K. Under-Secretary for Security and Counter-terrorism declared

[33]Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 44.

that a cyber-attack that takes out a power station would be an act of war."[34] This means that if actions in cyberspace were taken against the U.K., those actions would be viewed by the U.K. as a military weapon. As a result, the nation who would launch the attack would be subject to international cyber laws for all cyber actions taken.

Analysis from examining both *The Tallinn Manual* and U.N. article suggest with a high degree that both legal suggestions and legal frameworks follow the ethics of duty as the primary foundation. It is the ethics of duty that causes governments to follow the rules and laws. During the time period of the cyber-attacks on the city of Tallinn, there were no declarations of war by Russia. Therefore, there are no competing ethical values. Competing ethical values from utilitarianism are limited because the cyber-attack action possibly taken by Russia did not serve a greater good. Quite the opposite, the cyber-attacks on the city of Tallinn appeared to be serving a self-serving objective related to the statue removal, and not serving a greater good. Also, given that the cyber-attack on the city of Tallinn was not a virtuous action, there would be no conflict of the ethics of virtue. Again, the ethics of duty appears to be the strongest force suggesting that ownership of the action and any such reparations would fall onto the government who initiated the attack.

REPARATION LAWS

A review of global reparation laws also indicates that the belligerent government should pay the cyber COTS for damages to their business, including reparations for stock losses, and a loss of consumer confidence. Several legal frameworks outline what reparations should be

[34] Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford: Oxford University Press, 2014), 51.

required for injuries, moral damages, and restitution. First, *The Tallinn Manual 2.0* discusses what reparations should be taken by the belligerent government as a result of injuries sustained from covert cyber actions. The intent of reparations and compensations are congenial in that they both intend to offer up a restitution that will work to outweigh the object of the consequences removing all signs and indications that the situation ever existed.[35] To achieve this objective, the reparations offered should include the best restitution possible to meet expectations.[36] The guidance from Tallinn suggests that the belligerent should financially restore the cyber COTS company to its previous baseline prior to the cyber-attack. It may be difficult to have empirical data present to evaluate the baseline between the public perception of the COTS company prior to the cyber-attack and post-attack.

The ethical recommendations that should be followed as referenced by *The Tallinn Manual* suggest that "Injury refers to any material or moral damage caused by an internationally wrong cyber operation. Material damage includes property damage and harm affecting other interests of the injured State when said harm can be assessed in financial terms."[37] The belligerent government that caused injury to the cyber company should be responsible for repaying and repairing the damages of the cyber business. The damages to the cyber company's reputation would be highly difficult to gauge and validate. For example, if a company already had a bad reputation and it was claiming it needed financial compensation for damages to its reputation, it will be difficult to prove the claim. Since Tallinn suggests that reparations should be made for the financial damages for property, placing a price tag on reputation would be very difficult to prove

[35] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 51.
[36] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press), 144.
[37] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* (Cambridge: Cambridge University Press), 144.

with empirical data. Net Promoter Scores (NPS) or Customer Satisfaction Scores (CSAT) would be possible indicators but they are fluid and change daily.[38] As previously stated, the government is a reflection of the people. The people of the government would need to make a great effort to restore the cyber company financially but there would be significant challenges for the government to ensure the cyber business's reputation was restored. There are two possible courses of action a government could take to mitigate the damages to a company's reputation. First, the government could assist financially by providing the company with marketing and advertisement budgets. Second, the government could absorb the costs associated with a company name change should that be needed. A company name change is very costly but could potentially give the cyber company a fresh start if it is unable to recover from the press and media coverage of its perceived failed products.

In the final legal recommendations by *The Tallinn Manual*, there were broad sweeping recommendations of reparations that included, "in the cyber context, injury resulting from an internationally wrongful act may befall individuals or entities other than the State, such as its nationals or companies."[39] This would indicate that the cyber business should be covered by international agreement and laws because, although it was not directly attacked, it was the victim of the government's cyber-attacks and subsequent damages to its business. As a result, the cyber company would be subject to receiving reparations as a result of the damages it received. Although there may be situations where there were competing values between the four ethical values discussed, the ethics of duty best aligned to *The Tallinn Manual* because it was believed to be a universal law that all nations were following. In the example provided on the cyber-attacks on

[38] Darren Mackintosh, "Net Promoter Scores: Monitoring Practice Performance," *In Practices* 37, no. 7 (2015): 371.
[39] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press), 145.

Estonia, no country came forward and identified itself as the aggressor. The culprit of the cyber-attack was believed to be Russia as alleged by Estonia during the investigation.[40] Russia did not admit to the cyber-attacks and even in recent events, the Kremlin has demonstrated a consistent response of confusing statements and denial of involvement in order to mislead Western media.[41] In viewing how Russia responded to allegations of cyber-attacks and subsequent collateral damages, it is fair to examine Western democratic nations that have accidentally injured businesses or persons and to understand what course of action was taken or should have been taken.

REPARATION CASE STUDIES

In the last decade, the only well-known cyber-attack case studies have been Estonia, Georgia, and Stuxnet. In all three of these case studies, no country openly admitted its involvement. As a result, it becomes important to examine recent real-world conflicts including the Iraq and Afghanistan wars where there were admissions of collateral damages. These wars were not known for their use of cyber. Instead, the damages occurred through conventional means. However, the cases should help guide us to craft ethics and regulation that are related to cyber-attacks. Therefore, it is imperative to evaluate how Western democratic coalition forces responded to unintentional damages to people, properties, and businesses.

There are still no current established norms within the "international human rights or international humanitarian law requiring a government to compensate foreign nationals innocently harmed. However, an emerging norm requiring compensation or reparation exists if the harm

[40] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security 4*, no. 2 (2011): 51.
[41] Michael Weiss. "Maybe Putin's Telling the Truth about Winning Syria." *The Daily Beast*, Mar 15, 2016. https://search.proquest.com/docview/1782980043?accountid=322

results from a war crime or crime against humanity."[42] There have been lawful military actions taken across the globe sanctioned by the U.N. However, the global community has not developed and built the foundation of international laws that would require militaries to compensate civilians or businesses that were damaged during lawful military actions.[43]

Although there have been no substantial bodies of law that require compensation to injured civilians, there are countries that believe that this is the ethical and moral step needed to win the hearts and minds of fellow countrymen to ensure proper relationships moving forward. Any country that would take such action to properly compensate civilians demonstrates a higher ethical commitment to raise the bar to meet or exceed societal expectations. There are many competing values between the four ethical foundations. One might evaluate the four ethical foundations presented and believe that it is the ethics of duty, utilitarianism, and virtue combined that would drive a country to provide reparations to people or business when international laws do not require it. It is difficult to assess each scenario of competing ethical values that could have multiple ethical values as the driving force. The fact remains that ethics of duty is inherently aligned with following laws and regulations. The ethics of duty would be the strongest ethical value that to guide a government surpassing both utilitarianism and virtue.

According to Jonathan Tracy, "When a nation chooses to enter war, whether justifying it under the doctrine of Responsibility to Protect or some other authority, it takes on the responsibility to fight a 'just war.' While many just war discussions focus on *jus ad bellum* — the justness of entering a war — and *jus in bello* — fighting a war in a just manner, few emphasize *jus post*

[42] Jonathan Tracy, "Responsibility to Pay: Compensating Civilian Casualties of War," *Human Rights Brief* 15, no. 1, (2007): 1.
[43] Ibid., 2.

bellum, justice after war."[44] There are governments that choose to limit innocent civilian casualties in order to adhere to a moral and ethical code of conduct. Subsequently, those government's belief system will place a higher value on life, morals, principles, and international relations. Governments also look for ways to make a wrong, right. There can be strategic social and political goodwill from taking responsibility for unintentional actions that harmed the well-being of others and their business when accidentally or unintentionally damaged during wars. The United States is one such government in which the Congress and military have allocated funding to provide financial assistance to citizens who have been killed, injured, or suffered property damages resulting from military forces.[45] Jonathan Tracy noted that, "The only form of combat claims that U.S. military regulations allow are termed *solatia* payments. These are nominal amounts payable from a commander's operation and maintenance funds as an expression of sympathy."[46] The United States Department of Defense noted that, from fiscal years 2003 to 2006, approximately $2 million USD in solatia payments and nearly $30 million USD in condolence payments to Afghanistan and Iraqi citizens that were injured, killed or received property damages resulting from U.S. or coalition forces' actions resulting from combat.[47] The reparations provided to the Afghani and Iraqi citizens are expressions of profound remorse and sympathy.[48]

Despite this act of mercy, there are sometimes no common admissions of legal liability or fault committed by the United States government which can be considered by some to be contrary

---

[44] Jonathan Tracy, "Responsibility to Pay: Compensating Civilian Casualties of War," *Human Rights Brief*. 15, no. 1, (2007): 1.
[45] United States Government Accountability Office*, Military Operations, The Department of Defense's Use of Solatia and Condolence Payments in Iraq and Afghanistan*, (May 2007): 3.
[46] Jonathan Tracy, "Responsibility to Pay: Compensating Civilian Casualties of War," *Human Rights Brief* 15, no. 1, (2007): 2.
[47] United States Government Accountability Office, *Military Operations, The Department of Defense's Use of Solatia and Condolence Payments in Iraq and Afghanistan*. (Washington, DC: GPO, May 2007), 4.
[48] Ibid.

to the act of virtue and justice.[49] U.S. Geographic Combatant Commanders have the authority to make condolence payments to their geographic citizens who may be victims, by "using funds provided by Congress for the Commander's Emergency Response Program (CERP)."[50] Should the situation warrant the necessity, commanders in the field are authorized to make solatia compensations which are "funded from unit operations and maintenance accounts. Pub. L. No. 108-106 (2003)."[51] However, as a part of the United States government's checks and balances, doing so requires the Department of Defense to provide quarterly reporting to the American public on the sources, allocations, and funding status of CERP.[52]

In evaluating the Iraq war, there were cases that have rhymed with marginal similarities to the cyber scenario, and give ethical guidance as to how a government should respond to collateral damages much like in the cyber scenario. In looking at the Iraq war, there was a military situation on June 18, 2003, in which a former Iraqi Army soldier, Mr. Mohammed, was participating in a protest of the dissolution of the Iraqi Army in Baghdad.[53] During the demonstration, Mr. Mohammed was fatally shot by a Military Police convoy when military forces fired two shots into the crowd and one of those bullets fatally struck Mr. Mohammad who died as a result of his injuries.[54] His case was presented to the U.S. military and subsequently, his widow was paid $2,500 for her loss.[55] Compared to the 2017 average U.S. funeral costs of $8,755, that number would appear to be low but there was no data to substantiate how much the funeral costs the $2,500

[49] United States Government Accountability Office, *Military Operations, The Department of Defense's Use of Solatia and Condolence Payments in Iraq and Afghanistan*. (Washington, DC: GPO, May 2007), 4.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Jonathan Tracy, "Responsibility to Pay: Compensating Civilian Casualties of War," *Human Rights Brief* 15, no. 1, (2007): 1.
[54] Jonathan Tracy, "Responsibility to Pay: Compensating Civilian Casualties of War," *Human Rights Brief* 15, no. 1, (2007): 1.
[55] Ibid.

payment will cover in Afghanistan.[56] However, the actions of doing nothing by the United States government would have been far worse in the court of public opinion.

In another Iraqi war example, in June of 2003, Mr. Abbas was in transit in his personal van in Baghdad.[57] On this particular day, he was passing through the traffic circle of Hamm ad Shihab when nearby United States soldiers came under fire from a rocket-propelled grenade fired from a green BMW.[58] Fortunately for those soldiers, none of them were injured and as a result, they quickly returned fire.[59] The green BMW who provoked the combative situation with U.S. forces quickly sped away from the scene of the crime, but unfortunately, two bullets aimed for the green BMW struck through his white van and hit Mr. Abbas.[60] Despite fighting for his life for several days at a nearby hospital he passed away, and once again the U.S. paid his grieving widow $2,500 for the loss of her husband.[61] The amount seemed hardly worthy of praise in these scenarios but as previously stated, doing nothing would have only further angered and enraged a generation to categorically loathe the United States.

There was no data available to suggest that hatred towards the United States has not already happened after receiving solatia payments. The act of providing solatia payment demonstrates the ethics of duty as expressed through the compensation for their losses. Process and procedures dictate the amounts per country and region; however, general and flag level officers with the rank of one-star (O-7) or higher have the authorization on behalf of the U.S. government to authorize the payment up to $10,000 should the situation warrant.[62] The U.S. Tort law mandates the

[56] "Statistics," National Funeral Directors Association, accessed June 5, 2018. http://www.nfda.org/news/statistics
[57] Ibid.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Jonathan Tracy, "Responsibility to Pay: Compensating Civilian Casualties of War," *Human Rights Brief* 15, no. 1, (2007): 3.

compensation limitations. The reparations and procedures demonstrated how the U.S. government has taken action to compensate a civilian for unintentional damages incurred. The United States is not the only democratic government that evaluates the moral and ethical responsibilities of compensation to others resulting from military actions. Next, it is important to evaluate the actions of other Western democratic countries and the competing ethics those governments may use to guide how to compensate innocent civilians injured in the war in Afghanistan.

During Operation Enduring Freedom (OEF), the war in Afghanistan presented challenges and opportunities for the United States government. The war was not with the people of Afghanistan. The war objectives were directed at locating Osama Bin Laden and destroying his network while also removing the Taliban from governmental power because it was sheltering him from the United States. The war was initially directed at a few insurgents, but many would suffer losses. Civilians and businesses also experienced loss of life and property as a result of military actions taken by NATO forces during the war. In Afghanistan, neither members of the North Atlantic Treaty Organization (NATO) nor the International Security Assistance Force (ISAF) has proactively provided solatia compensations to innocent victims of combat.[63] However, despite this long-standing history, a few ISAF Troop Contributing Nations (TCNs) subsequently offered Afghanistan compensation for damages to civilian property, civilian injury, and civilian deaths in relation to their respective country's combat operations.[64] Even though TCNs had no legal obligation to provide solatia payments to Afghanis for damages resulting from the legal and lawful conduct, the payments were subsequently awarded *ex gratia* as a gesture of goodwill to the people that were impacted.[65] The ISAF countries proactively participating in armed conflict settling

[63] Amsterdam International Law Clinic and Center for Civilians in Conflict*, Monetary Payments for Civilian Harm in International and National Practice* (Washington: DC: Center for Civilians Conflict, 2014), 11.
[64] Ibid.
[65] Ibid.

included Canada, Australia, United Kingdom, The Netherlands, and Poland.[66] There were a plethora of solatia payments made to civilians who were victims of accidents and military actions.

It can be impactful to understand how many western democratic nations had demonstrated ethics of duty in how they responded to Afghanistan. By more than one nation acting in the same capacity doing the right thing, that action has the potential to spread to other non-democratic nations. If more nations have the same action, it could become closer to being the norm of what a government should do in this situation. However, did the United States demonstrate the same type of ethics in how they responded to those accidentally injured during the war? The next summary will investigate two case studies in which accidental damages in which the United States Army compensated Afghanistan families for their losses.

In the first Afghanistan case study, an Afghani man indicated his brother, and his brother's friend was in transit on a motorcycle which was traversing in parallel to a U.S. convoy on August 26, 2005, in the Logar province.[67] During transportation, a convoy vehicle took evasive action to avoid colliding with another car in its lane and accidentally crashed into their motorcycle.[68] The impact caused the motorcycle to crash which resulted in the riders receiving major injuries to his brother and the eventual death of the brother's friend.[69] The Afghanistan man's brother was taken to a nearby hospital and remained in a perpetual coma. The man's brother who was in the coma ran a local shop that was the primary source of income for his large family of nine members.[70] For the injuries he received, the Afghanistan survivor requested a compensation of $100,000 USD to

---

[66] Amsterdam International Law Clinic and Center for Civilians in Conflict*, Monetary Payments for Civilian Harm in International and National Practice* (Washington: DC: Center for Civilians Conflict, 2014), 11.
[67] U.S Army, "Documents received from the Department of the Army in response to ACLU Freedom of Information Act Request," Army Bates 32131-32147. *ACLU.org*, last modified March 2010, https://www.aclu.org/sites/default/files/webroot/natsec/foia/log2.html
[68] Ibid.
[69] Ibid.
[70] Ibid.

help cover the damages and expenses of the hospital bills. The U.S. Army investigated the accident and agreed that its driver was negligent.[71] Even though the U.S. Army agreed that their driver was at fault, they chose not to pay the $100,000 USD and instead paid the claim for only $3,000 USD, for the following reason: "According to the valuation chart for death claims in Afghanistan $6,000.00 USD is fair and reasonable for the death of a local national; therefore, $3,000.00 is fair and reasonable for the injuries sustained by the claimant's brother." The file also notes that a solatia payment was made to the wife of the man who died and that the woman was planning on filing a claim under the Foreign Claim Act."[72]

There was not enough information provided by the U.S. Army to justify why it chose not to pay the Afghanistan man the full amount requested for damages. However, this example makes an important point related to the original cyber scenario in that the victim of the cyber scenario was a smartphone business that had nothing to do with the government, but its world was turned upside down. The compensation the U.S. Government paid the Afghanistan victim was marginal compared to the loss of his life and probably the significant hospital bills incurred for the Afghanistan man who was put into a coma. However, where does the line start and where does the line stop on what is fair and reasonable? Offering an apology in many similar cases has appeased the offended party.[73] However, "offering apologies has become so commonplace in world politics that some have referred to this as the 'Age of Apology.'"[74] As a result, governments run the risk of their apologies being received as insincere. It would appear that it is still better to

---

[71] U.S Army, "Documents received from the Department of the Army in response to ACLU Freedom of Information Act Request," Army Bates 32131-32147. *ACLU.org*, last modified March 2010, https://www.aclu.org/sites/default/files/webroot/natsec/foia/log2.html.

[72] Ibid.

[73] Rachel R. Steele and Craig W. Blat, "Faith in the Just Behavior of the Government: Intergroup Apologies and Apology Elaboration," *Journal of Social and Political Psychology* 2, no. 1 (2014): 271.

[74] Jeff Corntassel and Cindy Holder, "Who's Sorry Now? Government Apologies, Truth Commissions, and Indigenous Self-Determination in Australia, Canada, Guatemala, and Peru," Human *Rights Review* 9, no. 4 (2008): 467.

side with caution by providing something that demonstrates a need for forgiveness or regret for injuries received rather than doing nothing at all.

The second case study occurred in Koshtowz, Afghanistan. In this situation, a young Afghanistan female was accidentally killed, and subsequently, her father was severely injured by the indirect fire from military forces.[75] What prompted this accidental death was that the father of the young girl was informed that his cattle were killed by the indirect military fire which prompted him to immediately investigate.[76] While on location with his cows, he and his daughter decided to salvage the meat from the cows to bring back to their family, but a cross-fire between opposing military forces broke out.[77] Military investigators reviewed the situation and their investigation indicated that lawful mortar fires were used to combat enemy forces.[78] Investigators believed that enemy forces were using local nationals to lure them into battle zones by putting them in harm's way to reduce fire from the allied forces.[79] The family of the victim was granted a solatia payment even though the military actions were lawful and they were cleared of any evidence of wrongdoing.

In the first Afghanistan case study, the U.S. military was negligent and paid a solatia payment. In the second case study, the U.S. military was conducting lawful military actions and, despite any evidence of wrongdoing, paid a solatia payment to the family for the loss of their daughter and the injuries sustained by the father. No one can say for sure except that Afghanistan family, but the gesture of the compensation from the U.S. for their losses may have served the U.S. government's interests in appeasing Afghanistan families and communities. Taking such action

---

[75] U.S. Army, "Documents received from the Department of the Army in response to ACLU Freedom of Information Act Request," Army Bates 30587-30630. *ACLU.org*, last modified March 2010, https://www.aclu.org/sites/default/files/webroot/natsec/foia/log2.html

[76] Ibid.

[77] Ibid.

[78] Ibid.

[79] U.S. Army, "Documents received from the Department of the Army in response to ACLU Freedom of Information Act Request," Army Bates 30587-30630. *ACLU.org*, last modified March 2010, https://www.aclu.org/sites/default/files/webroot/natsec/foia/log2.html.

was better than taking no actions at all. In looking at which competing ethic would best drive a government to comply with the collateral damage processes and procedures established, the ethics of duty would be the strongest ethical value to make a government want to pay collateral reparations.

In comparing the cyber COTS scenario against the real war case studies where people or businesses were damaged, the results are very similar. In the case studies and the cyber scenario, the government was brought into a situation where security was paramount and actions needed to be taken. The outcomes of the government's action did not match its plan and as a result, lives were lost and damages to a cyber COTS business were incurred. In the Afghanistan case studies presented, the gesture and action of doing something kind would show a greater ethical duty and virtue rather than doing nothing. One may notice that there are competing values between utilitarianism and duty in both the cyber scenario and real war case studies. Specifically, utilitarianism could be viewed as the driving force that caused the government to recognize that the actions that were taken served the greater good. Also, it may appear that the consequences mattered which is why utilitarianism is the competitive principle driving the actions of the western democratic governments. However, the motive of the government also plays a significant role which introduces another competing value, ethics of virtue, which would claim that these were proactive steps taken by governments to pay solatia. Even though there could be competing values, the ethics of duty is still the dominating force that should drive the actions of governments because they are trying to follow a moral universal code of conduct, while also adhering to the laws of the land.

ETHICAL RESPONSIBILITY, COLLATERAL DAMAGE, AND NON-COMBATANTS

The previous examples of war reparations made as a result of damages incurred suggest a solid argument for how a government should respond in the cyber scenario. In matters of national security does the cybersecurity company that was breached, and its code modified, have any negligence or responsibility? In this scenario, the cyber company does not have negligence. They were not consulted by the belligerent government, nor were they aware that their software code was being manipulated on their customer's smartphone for military purposes. However, the actions taken by the belligerent government, in theory, are representative of the will of their people. If the governmental body is representative of its people, then the government's actions reflect the will of the people.[80] This suggests that the actions were a public act and the damages incurred belong to not only the government but also the people of the government.[81] Whether the government was democratic, authoritarian or a dictatorship, the argument would be that "persons are morally responsible for what they bring about, what they intend to bring about, what they help to bring about; they are also responsible for what they endorse and for what which they chose to identify themselves."[82] If the government does not take proper steps to do what is right, then the people must demand such actions from their government.

[80] Neta Crawford, *Accountability for Killing – Moral Responsibility for Collateral Damage in America's Post – 9/11 War* (New York: Oxford University Press, 2013), 433.
[81] Ibid.
[82] Ibid.

COUNTER-ARGUMENT

Critics of the argument presented could four points: first, it is the company's responsibility to tighten their code to thwart hacking; second, there are acceptable forms of collateral damages in matters of national security; third, COTS applications are cheaper; and fourth, cyber warfare saves lives compared to traditional warfare.

The government should be able to exploit cyber-COTS technologies recognizing that it is the business's responsibility to tighten their code to thwart hacking. Any global hacker could have discovered the same vulnerability and conducted a similar type of activity and, if undiscovered, the cyber COTS business would not have received any compensation from a global hacker because of their own defective software vulnerabilities. Furthermore, in many conflicts, bombings produce an impersonal form of collateral damage. Bombings cause collateral damage and unfortunately, it is treated as something that just happens, and there is little to no fault attributed to the forces which caused the death or damages. Also, leveraging the use of cyber COTS for warfare activity is far more cost-effective than traditional conventional warfare because it does not have the logistical requirements of traditional warfare, and it has a precision capability built in which allows some cyber-attacks to be very precise with smaller risks to collateral damages. As a result, cyber warfare potentially has the ability to save lives from collateral damage, compared to traditional conventional warfare. If there are indeed accidental damages incurred by a corporation, an apology by the belligerent government may be sufficient, and no further solatia compensation would be required.

It is natural in most societies to acknowledge that there are acceptable forms of collateral damage in not only cyber warfare but also conventional and unconventional warfare. To

elaborate, any human-made technology is imperfect and comes with inherent risks. In many cases, those risks come with a potential loss of life. Until such time that businesses have created sound training and doctrine surrounding the use of the new technology, the unplanned or unimagined uses could have deadly consequences. As it relates to cyber warfare, there are many unexplored avenues that could have lethal consequences. Especially, as it relates to any type of warfare, there are potential accidents and it is unattainable for there to not be casualties as a result of the war, including cyber warfare.

Creating military specific cyber technologies are very costly in terms of time and money to citizens. Military planners could take full advantage of leveraging cyber COTS at a fraction of the costs and still allocate monies for collateral damages or incidents. This would save the taxpayers money by not having to pay for research and development costs, training, overhead deployment, marketing, and testing. Even if there is collateral damage - from the costs saved, it makes economic sense to continue with cyber COTS and allocate budgets for the unfortunate reparations should they be warranted.

Cyberwarfare has the potential, depending on how it is used, and provided that it is not being used to launch nuclear weapons, to saves lives compared to conventional warfare. In cyber warfare, the technologist can be on location or remote from the site of an attack in order to access networks, manipulate networks, and deploy their strategy with only the risk of their digital signature being captured in the network or Internet. Unlike conventional warfare, this same type of covert action would require putting trained military forces on the ground to penetrate enemy forces and be exposed to hostile enemy ambush and attacks.

The number of military lives that can be saved from not having to put people in harm's way would easily justify any potential reparations costs. As a result, it makes more economic

sense to try to use cyber COTS for cyber warfare and take the chance paying for an unexpected reparation as a result of collateral damage incurred. If the belligerent government was blamed for the collateral damages resulting from the cyber-attack, they would have to pay reparations as a result of their operational tactics. The same type of proactive actions should be taken even if the belligerent government was not identified as the culprit. The government should follow the ethics of duty to identify itself and establish the baseline of fear with the global community regarding its global capability and then use the funds set aside for any potential damages that need to be paid.

REBUTTAL

While the preceding section includes legitimate arguments, it would then suggest that every business would be responsible for the actions of its customers. For example, if a car manufacturer built a vehicle for transportation purposes only as its intent, and another belligerent government purchased the car in order to run over and kill an operative, would that place the burden of blame on the car manufacturer because they did not make their product in a way that could prevent accidental or intentional homicide? The same argument would be true for firearms manufacturers. If the firearm manufacturer made its product for hunting and self-protection purposes only and their product was used to kill innocent people, could there be a legitimate claim that the firearm manufacturer should have corrected made a smart gun that would not kill an innocent person? There is a line that must be drawn on the responsibility of inventors and the public using their product in ways not always intended. In the cyber scenario, the government changed the code of the cyber COTS application, and the cyber business should not be responsible for someone changing their software code.

The cyber scenario had an element where there was unexpected collateral damage. There may be places in the world where collateral damage is expected when conducting warfare. But that should not mean that it is ever acceptable to discount the loss of innocent life. Globally, all are members of the same human race, members of the same Earth, and all should agree that all innocent lives should be protected from intentional or unintentional harm.[83] It should not be acceptable to think that the unintentional harm inflicted on a business that costs people their jobs, income, credibility, and ability to find new work would be acceptable in the name of national security.

Cyber COTS may have a cheaper acquisition cost as compared to the research and development of creating new cyber technologies. However, there are inherent risks when using cyber COTS as demonstrated in the cyber scenario. The cyber technologies are untested or unknown to government planners. Information operation planners are counting on a cyber-effect from a cyber COTS application when they begin planning. The challenge becomes that there may not be empirical data to support the stability of the product or the expected outcome. In an environment where the government built its own cyber weapons, it has the ability to war game and test scenarios to see how applications will perform. The testing and wargaming phase is not always available when using a cyber COTS. Cyber COTS may be a more cost-effective form of leveraging cyber warfare but they come with a greater risk to the mission. The cyber scenario presented did not war-game a smartphone overheating with a curtain nearby. That could be poor planning or a limitation of not knowing the thresholds of the cyber COTS technology and when it would become a fire risk outside of normal and expected projections. Taking those extra steps

[83] Neta Crawford, *Accountability for Killing – Moral Responsibility for Collateral Damage in America's Post – 9/11 Wars*(New York: Oxford University Press, 2013), 473.

could ensure greater success in cyber COTS operations and reduce the chances of collateral damage.

There was not enough data to suggest that cyber warfare saves lives compared to traditional warfare. There have not been enough wars that leveraged cyber to compare it against traditional wars. Those that will leverage cyber effects in a cyber-attack will remain quiet about their cyber-attack, and the victim will most likely not advertise that they are the recipient of a cyber-attack so as to confuse and deceive the aggressor. The Stuxnet cyber-attack against the Iran nuclear power plant centrifuges is a clear example that if an attack was lethal enough, catastrophic damages could happen off the battlefield and by using cyber to attack nuclear power plants causing them to have nuclear core meltdowns. A cyber-attack that focused on causing a nuclear bomb to explode in its launch bay silo clearly would show how cyber has the potential to cause mass destruction as well as mass disruption.

CONCLUSION

In conclusion, cyber-attacks will inevitably become more utilized by governments in their offensive attacks. The use of cyber technologies extends the reach of a government to exact a cyber-effect on another government to demonstrate political will. The cyber-attacks of Estonia, Georgia, and Stuxnet have all demonstrated that a new type of cyber warfare exists. It is only a matter of time before something like the cyber COTS scenario presented will happen. If a type of cyber-scenario as described in this research occurs, it would be paramount that governments that participate in these type of cyber-attacks plan for the unexpected. In their planning, they should have an ethical disposition and solution developed in order to respond to damages or injuries inflicted on others. The unexpected results of covert cyber-attacks will inevitably result in

outcomes including the loss of life, damages to businesses, and financial losses coupled with the potential damages to business reputations. As a result, it is imperative for all governments that sponsor covert cyber-attacks to recognize they have ethical responsibilities to do the right thing even when nobody is looking.

Historically, the cyber-attacks seen in Estonia, Georgia, and Stuxnet have all revealed that governments will not openly admit their involvement in a cyber-attack. If governments will not admit their involvement in a cyber-attack, it is logical to assume governments will not take responsibility for any collateral damages. It is doubtful that Russia, China, or any non-democratic nation would openly admit any wrongful action or assume responsibility for collateral damages. It is hopeful that Western democratic nations would take ownership of collateral damages inflicted on innocent people or businesses. In the cyber scenario, the government should not have waited for an independent research investigation to discover the manipulated code. The government should have followed the ethical values as seen in and recommendations from cyber experts of *The Tallinn Manual* to guide them on how to respond to the collateral damages incurred.

There are a host of ethics foundations, societal norms, rules, and laws that clearly outline a course of action to remediate the situation. The responsibility belongs to the belligerent government delivering the cyber-attack, and as a result, all reparations and damages should be taken by that government. While there are four ethics that could contribute to how the government should respond, the ethics of duty should be the primary ethical value to help guide a government to respond in kind to make reparations for damages incurred. Looking at Table 1, the outline demonstrates the strengths or weaknesses of each competing ethical value. Specifically, the legend examines the ethical dilemmas such as it would respond to taking accountability for the cyber-

attack, or how it should respond to following international laws. From comparing these situations, it is evident that the ethics of duty is the strongest ethic in each situation.

As shown in Table 1, this analysis suggests the ethics of duty is the most powerful influence on four key effects of a government's decision to use cyber means and incur the risk of harm to non-involved parties including families and corporations. Given the notional scenario guiding this work, a government's decision makers would be wise to focus on the ethics of duty in designing the most ethical operations in the future.

Table 1: Effects of Competing Ethics on Government Actions

EFFECTS / ***ETHIC***	***Limited Collateral DAMAGE***	***Collateral REPARATIONS***	***Public ACCOUNTABILITY***	***Limited Overall COSTS***
DUTY	**S**	**S**	**S**	**S**
UTILITARIANISM	**M**	**M**	**W**	**W**
DIVINE COMMAND	**S**	**M**	**M**	**W**
VIRTUE	**S**	**M**	**S**	**W**

Legend: S = Strong effect, M = Moderate effect, W = Weak effect

Duty should be the primary ethic that drives the government's behavior in how it would respond to reparations for collateral damages. It was the responsibility of the government to provide reparations to the cyber COTS company to ensure its business and financial losses were repaired as a result of its code being hacked by the government to attack a military target. If what one tolerates becomes the standard, then it is hopeful that if western democratic nations continue to follow this ethical framework, the possibility exists that the standard government response would be to accept responsibility and mitigate the collateral damage by paying reparations as quickly as possible.

BIBLIOGRAPHY

Anonymous. “Take That! Putin underlines regional gas hegemony” *Russian Life* 50, no. 4 (2007):8.

Avella, Jay. “The Dilemma of Ethical Leadership.” *Journal of Leadership Studies* 11, no. 2 (2017): 42-3.

Bhatia, Mandeep Singh. "World War III: The Cyber War." *International Journal of Cyberwarfare and Terrorism* 1, no 3 (2011): 59-69.

Corntassel, Jeff and Cindy Holder. “Who’s Sorry Now? Government Apologies, Truth Commissions, and Indigenous Self-Determination in Australia, Canada, Guatemala, and Peru.” *Human Rights Review* 9, no. 4 (2008): 465-89.

Crawford, Neta. *Accountability for Killing – Moral Responsibility for Collateral Damage in America’s Post – 9/11 Wars.* New York: Oxford University Press, 2013.

Dombrowski, Peter, and Chris Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67, no 2 (2014): 71-96.

Elbner, Thomas, and Reinhold Janke, Ed. *Didactics of Military Ethics, From Theory to Practice*. Boston: Brill Nijhoff, 2016.

Farwell, James P, and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival Global Politics and Strategy* 53, no. 1 (2011): 23-40.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.

Himan, Lawrence. *Ethics: A Pluralistic Approach to Moral Theory.* San Diego: Harcourt Brace College Publishers, 1998.

Lawler, Michael G and Todd A. Salzman. “Virtue Ethics: Natural And Christian.” *Theological Studies* 74, no. 2 (2013): 442-73.

Libicki, Martin. *Cyberspace in Peace and War*. Annapolis: Naval Institute Press, 2016

Lindsay, Jon. 2013. "Stuxnet and the Limits of Cyberwarfare." *Security Studies* 22, no. 3 (2013): 365-76.

Loo, Bernard Fook Weng. "Decisive Battle, Victory and the Revolution in Military Affairs." *Journal of Strategic Studies* 32, no. 2 (2009): 189-211.

Lucas, George. *Ethics and Cyber Warfare. The quest for Responsible Security in the Age of Digital Warfare.* New York: Oxford University Press, 2017.

Mackintosh, Darren.“Net Promoter Scores: Monitoring Practice Performance” *In Practice* 37, no. 7 (2015): 371.

McGuffin, Chris, and Paul Mitchell. "Oh Domains: Cyber and the Practice of Warfare." *International Journal* 69, no 3 (2014): 394-412.

Perritt, Henry and Eliot Sprague.” Drone.” *Vanderbilt Journal of Entertainment and Technology Law* 17, no. 3 (2015): 673-749.

Perry, David L. *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation.* New York: Rowman and Littlefield, 2016.

Perry, David L. “The Problem of Holy War: Adapted from an Ethics at Noon presentation given at Santa Clara University, September 25, 2001.

Pociumban, Andrei. "The Evolution of Cyber Operations." International Scientific Conference "Strategies XXI" (2017): 405.

Pohoata, Gabriela. “Confucius and Kant or the Ethics of Duty.” *Cogito* 2, no. 1 (2010): 50-56.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford, UK. Oxford University Press, 2014.

Schmitt, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Schmitt, Michael. “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.” Cambridge: Cambridge University Press, 2017.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* 91, no. 6 (2011): 63-68.

“Statistics.” National Funeral Directors Association, Accessed June 5, 2018. http://www.nfda.org/news/statistics

Steele, Rachel R. and Craig W. Blatz. “Faith in the Just Behavior of the Government: Intergroup Apologies and Apology Elaboration.” *Journal of Social and Political Psychology* 2, no. 1 (2014): 268-288.

Stiennon, Richard. *Surviving Cyber War*. Lanham: Lynne Rienner Publishers, 2010.

Strimel, Greg J., Scott R. Bartholomew, and Eunhye Kim. "Engaging Children in Engineering Design through the World of Quadcopters." *Children's Technology and Engineering* 21, no. 4 (2017): 7.

Tracy, Jonathan. “Responsibility to Pay: Compensating Civilian Casualties of War,” *Human Rights Brief* 15, no. 1, (2007):1.

U.S. Department of the Army. “Documents received from the Department of the Army in response to ACLU Freedom of Information Act Request,” Army Bates 30587-30630. ACLU.org. Last modified March 2010, https://www.aclu.org/sites/default/files/webroot/natsec/foia/log2.html

U.S. Department of the Army. “Documents received from the Department of the Army in response to ACLU Freedom of Information Act Request,” Army Bates 32131-32147. ACLU.org. Last modified March 2010, https://www.aclu.org/sites/default/files/webroot/natsec/foia/log2.html

United States Government Accountability Office. Military Operations, The Department of Defense's Use of Solatia and Condolence Payments in Iraq and Afghanistan. Washington: DC: U.S. Government Accountability Office, May 2007.

Valeriano, Brandon, and Ryan Maness. *Cyber War Versus Cyber Realities*. New York: Oxford University Press, 2015.

Weiss, Michael. "Maybe Putin's Telling the Truth about Winning Syria." The Daily Beast, Mar 15, 2016. https://search.proquest.com/docview/1782980043?accountid=322

Zetter, Kim. *Countdown to Zero Day Stuxnet and the Launch of the World's First Digital Weapon.* New York: Crown Publishers, 2014.

Zhang, Mo. "Tort Liabilities and Torts Law: The New Frontier of Chinese Legal Horizon." *Richmond Journal of Global Law and Business* 10, no. 4 (2011): 415.