REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 2. 14 June 2018	2. REPORT TYPE Final Submission	3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

A Breach of Trust:
The Impact of Artificial Intelligence on Society and Military Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

THOMAS PATRICK O'FLANAGAN, LCDR, CHC, USN

Paper Advisor (if Any): DR. YVONNE R. MASAKOWSKI

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Ethics & Emerging Military Technology Program (EEMT)
U.S. 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

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

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Ethics and Emerging Military Technology (EEMT) graduate certificate. 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

The development and use of Artificial Intelligence (AI) promises tremendous advantages for individuals and society as a whole. Despite the potential benefits to three primary domains--individual, society, and the military--there exist critical vulnerabilities that erode trust in its use. Several current leading companies in this field have acknowledged efforts to gather private user information that could be misused and their data systems breached. The influence of this technology is becoming a single point of failure for all aspects of society in the United States and requires an ethical framework from which Congress can ensure trust in the services AI provides.

SUBJECT TERMS
Artificial Intelligence, Data Ethics, Military Technology, Surveillance, Ethics

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		38	

NAVAL WAR COLLEGE

Newport, R.I.

A Breach of Trust:
The Impact of Artificial Intelligence on Society and Military

By

Thomas Patrick O'Flanagan, LCDR, Chaplain Corps, USN

A paper submitted to the Faculty of the Naval War College in partial 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 Naval War College or the Department of the Navy.

14 June 2018

UNCLASSIFIED

Table of Contents

Abstract

The development and use of Artificial Intelligence (AI) promises tremendous advantages for individuals and society as a whole. Despite the potential benefits to three primary domains--individual, society, and the military--there exist critical vulnerabilities that erode trust in its use. Several current leading companies in this field have acknowledged efforts to gather private user information that could be misused and their data systems breached. The influence of this technology is becoming a single point of failure for all aspects of society in the United States and requires an ethical framework from which Congress can ensure trust in the services AI provides.

ACKNOWLEDGMENTS

I'm grateful to many people for the privilege of being associated with this program and to attend The United States Naval War College.

I am deeply indebted to Dr. Yvonne Masakowski who served as my academic mentor whose seemingly limitless generosity in sharing her gifts of knowledge in many fields of study to include that of her expertise on Artificial Intelligence, Autonomous Systems, and Ethics that made it possible. This manuscript is a direct result of Dr. Masakowski's efforts that produced a golden thread tying the electives associated with this program to real-world applications.

Additionally, I want to thank Dr. Thomas Creely, the Director of the Ethics and Emerging Military Technology Program. Dr. Creely's scholarship and constant dedication to provide some of the most interesting and challenging topics for discussion have given us the tools to better evaluate ethics in relation to technology.

Sincere gratitude to Dr. Timothy Schultz, Associate Dean of Electives, a consummate warrior and scholar, whose enthusiasm, personal example, and thorough preparation understandably make him one of the most esteemed professors at USNWC.

Thank you to Ms. Isabel Lopes whose constant efforts over ten months of proactive research joyfully kept every participant in the program current on the latest technologies and connected topics.

To Mrs. Donna Menard, who encouraged me to pursue application into the program specifically because of the tremendous people associated with the EEMT program.

Introduction

On April 18, 2018, Mark Zuckerberg, CEO of Facebook, testified before Congress to address concerns of data manipulation.[1] Facebook's 2.1 billion users were stunned to learn that their personal information was sold to data-mining companies.[2] This is but one of many recent examples where a corporate ethical failure has damaged the trust of its users. If this were one single instance involving innocuous information, there would be no significant concern and over the course of time regulations would be developed and trust reestablished thorough transparent business practices. This and several recent reports like it, however, are precursors of critical vulnerabilities because similar algorithms are imbedded in emerging technologies at the core of Artificial Intelligence (AI). It is logical that civilian and military applications use AI because of the tremendous advantages it provides to address solutions for the increasing complexity in our lives. In this analysis, I will present evidence to support the fact that, given the potential for harm, Congress must pass laws to establish ethical guidelines for a transparent and controlled process of acquisition, protection, and use of information supporting Artificial Intelligence platforms.

There is a tremendous volume of information that the world has become dependent upon technology to provide. *Forbes* magazine reports that as of September 5, 2017, every day computers process 2.5 exabytes of information.[3] Artificial Intelligence (AI) serves as the principal engine for many of the common devices we use to make our daily lives easier and the

[1] [1] Jonathan Vanian, "Facebook CEO Mark Zuckerberg Wins Would-Be Congressional Grilling," *Fortune*, 11 April 2018.
[2] Dan Noyes, "The Top 20 Valuable Facebook Statistic," last Modified May 2018, https://zephoria.com/top-15-valuable-facebook-statistics/
[33] Bernard Marr, "How Quantum Computers Will Revolutionize Artificial Intelligence, Machine Learning and Big Data," *Forbes*, September 5, 2017.

technology more appealing. This paper examines the ethical responsibilities inherent in the relationship between developers and users of AI platforms and potential detrimental effects for civilian and military applications, as well as the implicit trust that is essential for preserving the security of individuals and of our nation. The best approach for determining what is proper in this relationship between choices is to consult ethics. In his dictionary, Fr. John Hardon defines ethics as, "The science of human conduct as known by natural reason. It is a normative science because it determines the principles of right and wrong human behavior. It is also a practical science because it does not merely speculate about moral good and evil but decides what is right or wrong in specific human actions."[4] Therefore, there is an urgent responsibility for all programmers to understand the potential ethical implications and consequences of technology upon individuals and society.

The most obvious concerns of the manipulation of AI include financial loss, privacy, security, and physical danger; however, there is a growing awareness of the spiritual danger because values and people can be so easily compromised. As a result, more and more ethicists and theologians are correctly calling for a proper perspective that recognizes the instrumentality of technology and a reminder that it is an end in itself. As the Catechism of the Catholic Church states regarding science and technology;

> "Basic scientific research as well as applied research, is a significant expression of man's dominion over creation. Science and technology are precious resources when placed at the service of man and promote his integral development for the benefit of all. By themselves however they cannot disclose the meaning of existence of human progress. Science and technology are ordered to man, from whom they take their origin and development; hence they find in the person and in his moral values both evidence of their purpose and awareness of their limits."[5]

The ethical application of Artificial Intelligence is of concern to Pope Francis. In a letter to

[4] John A. Hardon, S.J., *Pocket Catholic Dictionary* (New York: Image Books, 1985), 132.
[5] *Catechism of the Catholic Church* (New York: Doubleday, 1995) Question 2293.

the 2018 World Economic Forum, the pontiff writes, "Artificial intelligence, robotics and other technological innovations must be so employed that they contribute to the service of humanity and to the protection of our common home, rather than to the contrary, as some assessments unfortunately foresee."[6] This attention and appeal for a proper moral perspective and appreciation of AI is telling coming from someone many consider to be a foremost ethical leader.

The Nature of Information Systems and Ethics

Currently, these new information systems offer tremendous opportunities to improve our lives in many ways. Advances in education, medicine, travel, relationships, commerce, and faith, are but a few ways that the world benefits from the assistance of technology.[7] Ultimately, the design and use of advanced technology should be for the enhancement of the individual, as well as that of society. The information platforms presented in this paper show instances where corporations placed an emphasis on personal gain and shareholder's profits over of the real benefit of others. A lack of ethical vigilance in the judicious application of such platforms could compromise us at the individual, sociological, and national security levels and affect our ability to fight and defend our nation. Any discussion must include consideration of the long-term goals and effects of such choices on the lives of all people.

"Technology Ethicist" Ian Barbour highlights the possible dangers of implementing technology detached from a proper goal of fulfilling human beings.[8] "This new force is governed by a human attitude that no longer feels itself tied by living human unity and its

[6] Jack Jenkins, "The (Holy) Ghost in the Machine: Catholic Thinkers Tackle the Ethics of Artificial Intelligence," last Modified, 26 May 2018, https://cruxnow.com/church/2018/05/26/the-holy-ghost-in-the-machine-catholic-thinkers-tackle-the-ethics-of-artificial-intelligence/
[7] Barbour, Ian G., *Ethics in an Age of Technology, (*New York: Harper Collins), 1993, 4-5.
[8] Ibid.

organic compass and that regards as petty and narrow the limitation in which the earlier time found supreme fulfillment, wisdom, beauty, a well-rounded fullness of life."[9]

The Catechism of the Catholic Church asserts that the development and use of technology is not inherently neutral.

> "It is an illusion to claim moral neutrality in scientific research and its applications. On the other hand, guiding principles cannot be inferred from simple technical efficiency, or from the usefulness accruing to some at the expense of others or, even worse, from prevailing ideologies. Science and technology by their very nature require unconditional respect for fundamental moral criteria. They must be at the service of the human person, of his inalienable rights, of his true and integral good, in conformity with the plan and the will of God."[10]

The purpose of this paper is to address specific ethical concerns of technology that gathers and/or manipulates information and recommend examples of needed oversight because of the effects this has on society.[11] There is a short window of time in which to address this problem because of the type and volume of information. Bank records and common transactions are temporary in nature, but if compromised, fraudulent transactions can be executed. When other types of information are compromised and manipulated, such as, Personally Identifiable Information (PII), social security numbers, medical records, medications, and DNA, users' lives are negatively, and in some cases, forever altered. While some scholars may argue about the growing applications, this paper will examine the indisputable vulnerabilities of this technology and its impact on three levels--the individual, society, and on the battlefield.[12] Precisely because

[9] Romano, Romano, *Letters from Lake Como: Explorations on Technology and the Human Race* (Grand Rapids, MI: William B Eerdmans Publishing, 1994), 635-636

[10] Catechism of the Catholic Church 2294

[11] Ian G. Barbour, *Ethics in an Age of Technology* (New York: Harper Collins), 1993, 8.

[12] Yvonne Masakowski, "AI and Autonomous Systems: The Evolution of Warfare in the 21st Century," Diffusion and Adoption of Innovation Studio Summit (DAISS)

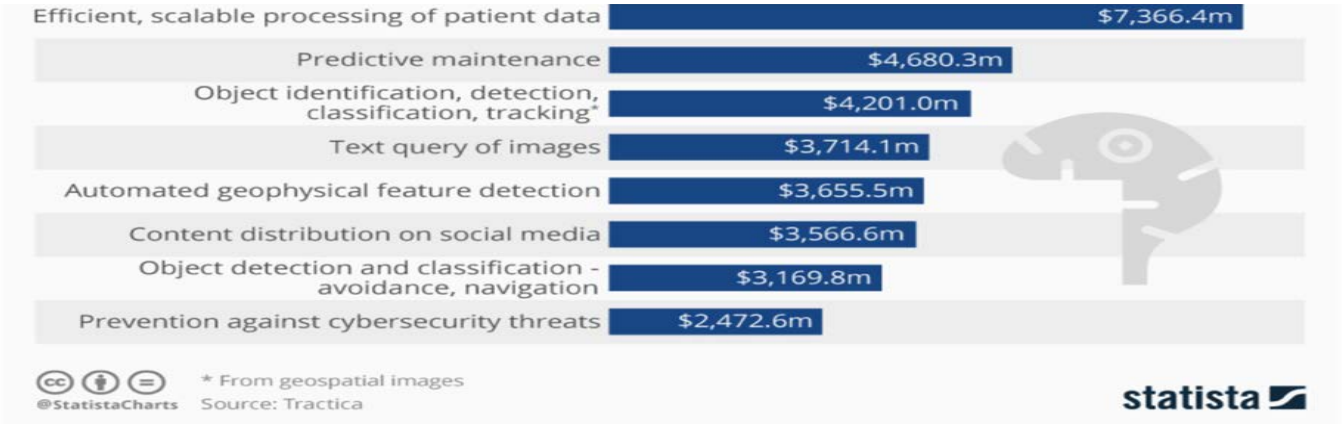
of the great potential for harm to the three levels, there exists a moral obligation to attain and sustain proper regulation and oversight.[13]

Current efforts to protect crucial personal information are insufficient and ineffective in both the private sector and that of the government. In the private sector, one of the single greatest data breaches occurred when Equifax exposed the personal information of 145.5 million users.[14] For the government, starting in 2013, there have been six data breaches in the Office of Personnel Management causing identity theft for millions of government workers. [15] These examples show that the very platform used to support artificial intelligence has been compromised which erodes the public's trust, the very people they are supposed to serve. By 2019, cyber security experts predict that cyberattacks will cost more than 11.5 billion dollars.[16]

For those who might doubt the significance of AI now and in the immediate future, the chart below is a glimpse of how AI influences many critical levels of society. Facial recognition, healthcare, cyber, social media, and even geography are but a few sectors poised for large projected revenues through the year 2025.[17] AI is rapidly influencing the world.

---

[13] Shannon Vallor, *Technology and the Virtues*: *A Philosophical Guide to a Future Worth Wanting* (Oxford: Oxford University Press, 2016), 2.
[14] Amy Martyn, "The Amazing, Ever-Changing Story of the Equifax Hack," *Consumer Affairs*, May 31, 2018.
[15] Waddell, Kaveh and Stamm, Stephanie, "A Timeline of Government Data Breaches," *The Atlantic*, July 6, 2015. https://www.theatlantic.com/politics/archive/2015/07/a-timeline-of-government-data-breaches/458352/
[16] Steve Morgan, "Top 5 Cybersecurity Facts, Figures and Statistics for 2018," *CSO*, Jan 23, 2018, https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
[17] Martin Armstrong, "*The Future of AI*," *Statistica*," November 18, 2016, https://www.statista.com/chart/6810/the-future-of-ai/



Developing a Normative Ethical Framework

"This sphere is overshadowed by a growing realm of collective action where doer, deed, and effect are no longer the same as they were in the proximate sphere, and when by the enormity of its powers forces upon ethics a new dimension of responsibility never dreamt of before."[19]

Because every aspect of our lives will be impacted to some degree or another by the use of AI, our individual choices and participation in society require that the platform is trustworthy. For a universal framework to be useful, companies and governments must agree that they have an obligation to reveal the information that they collect, where it goes, and how it is used. Any acceptable framework must also include three main elements: accurate anthropology, universality, and intelligibility.[20] The first element is anthropology because anything worthwhile cannot run contrary to a proper understanding of the abilities of human nature.[21] Universality is

[18] Ibid.
[19] Ronald L. Sandler, *Ethics and Emerging Technologies* (Boston: Palgrave Macmillian, 2014) 39.
[20] Koterski, Fr. Joseph W., S.J., Natural Law and Human Nature, Part II, The Teaching Company, Chantilly, VA, 2002. Pp. 206-213.
[21] Ibid.

a key element because the framework must be applicable to all, independent of culture, creed, or race.[22] The third essential element for any acceptable framework is intelligibility as it must be derivable from natural reason.[23]

According to Shannon Vallor, an expert on modern ethics, "Ethics and technology are connected because technologies invite or afford specific patterns of thought, behavior, and valuing; they open up new possibilities for human action and foreclose or obscure others."[24] To properly evaluate the development of an ethical framework for the emerging technology of artificial intelligence, this analysis offers examples across the domains of the individual, the societal, and on the battlefield through the lenses of the top competing ethical theories most frequently referred to when discussing applied ethics. The three theories are commonly known as Virtue Ethics, Duty Based Ethics, and Utilitarian Ethics.

Virtue Ethics

Virtue Ethics is commonly associated with the philosopher Aristotle whose logical reasoning places the intellect before the will.[25] Accordingly, proper choices are based on the intrinsic value of the person or object and not contingent upon the will of the individual.[26] Good choices are therefore those that are consistent with those values that bring true happiness and result in strong character.[27] Therefore, within this context, one can evaluate the integration of AI with an eye toward developing surveillance systems that would protect and defend society, as well as

[22] Ibid.
[23] Ibid.
[24] Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting* (Oxford: Oxford University Press, 2016), 2
[25] Ibid.
[26] William L. Reese, *Dictionary of Philosophy and Religion* (New Jersey, Humanities Press, 1996), 36-41.
[27] Ibid. 36-41.

keeping military personnel out of harm's way. In this manner, AI is serving a noble purpose for all.

Philosopher and theologian Father John Hardon says that all humans are under natural law, "because it contains only those duties which are derivable from human nature itself, and because, absolutely speaking, its essentials can be grasped by the unaided light of human reason."[28] Thus, an argument can be made that it is incumbent upon mankind to advance the development of technologies that will preserve mankind for today and for the future. The development of AI systems for this purpose would support mankind's moral reasoning and serve the greater good.

For the individual, the development and implementation of AI in human activity must be conducted in the spirit of elevating mankind and preserving the dignity of each individual. Not to do so would be a violation of trust between those who create advanced AI technologies and society itself. A true ethical framework cannot allow manipulation of AI to undermine the goal of helping the highest goals of humanity or it is inauthentic.

For those who implement a virtue-based ethic, personal fulfillment is a secondary effect and not the principal motivation for action. For those who follow virtue ethics, the rescue on an active battlefield would presuppose the value of human life and work to that end. One can envisage the utilization of autonomous systems to conduct search and rescue effort for wounded combatants. In this way, we can perceive the benefits to military warfare and securing global security.[29]

Regardless of whether this occurs on the individual domain, the societal domain, and the battlefield, it is essential to consider the dignity of the people involved in the highest possible

[28] John A. Hardon, S.J., *Pocket Catholic Dictionary* (New York: Image Books, 1985), 279.
[29] John G. Ramiccio, *The Ethics of Robotic: Autonomous and Unmanned Systems in Life-Saving Roles* (Newport, Naval War College, 2017)

good apart from any selfish desires. The primary motivation for choosing an action is not for self-aggrandizement but rather aimed at the ultimate good for all. The value of virtue ethics is forged in the fact that there is intrinsic value to the individual themselves that is not reliant upon a set of conditions. Whether on Facebook or on the battlefield, it is the responsibility of individuals to conduct themselves within the framework of virtue ethics with regard for the dignity of those with whom they work and lead.

The moral obligation for all concerned, whether in society or in the military, is to strive for the highest possible ethical ideals. For those in the military, the Just War theory provides a framework for military individuals to execute their duties and maintain dignity in the defense of their goals. This framework shapes the development of future military technologies that will be consistent with this set of universal criteria. Indeed, an ethical organization will integrate these concerns in the design of future technologies with an eye toward providing benefits that outweigh potential risks to the individual, society, and/or to the military warfighter.

Duty-Based Ethics

Duty-Based ethics are derived from the philosophy of Immanuel Kant and focus on one's intent in following self-derived values. Kant teaches that moral law is, by necessity, a construct that humanity ought to develop and follow. It is to be found within the individual and not externally because that would deny truly autonomous actions.[30] Therefore, this philosophy is insufficient to address a moral framework precisely because Kant looks to subjective experience for truth instead of an objective reality as a foundation of our behavior. Within this context, one

[30] Peter Kreeft, "Pillars of Unbelief- Kant," *National Catholic Register*, Jan-Feb 1988, www.peterkreeft.com

would be motivated to enter the battlefield at risk to oneself in order to rescue those wounded. This behavior is in concert with one's personal sense of duty and obligation in accordance with Kant.[31] Therefore, the influence of Kant can be realized by the design of AI autonomous systems that integrate the ideal set of behaviors that will contribute to the well-being of the individual combatant on the battlefield. In this way, we can extrapolate to all AI technologies that will integrate ethical guidelines and constraints that will yield positive behaviors. Advanced technologies will shape the future for all, so thought must be given to the potential impact of implementing these on the battlefield for failure to do so may result in unforeseen consequences.[32] This is important because as these systems evolve and as they become more independent of human supervision, we will need to rely on their programmed ethical and critical thinking skills.[33]

Kant's "Categorical Imperative" view is that we "act on principles that we can consistently universalize as a law governing everyone's behavior."[34] This Deontological perspective mandates that we make decisions with a view toward positive consequences. In this context, if we are faced with a moral dilemma in the conduct of warfare, how might one resolve it within this context? Namely, leaders are often presented with complex situations in which there may not be a clear path ahead and the implementation of AI technologies and unmanned systems may present us with a moral conflict. When applied to the emerging technology of AI, there could be justification for almost any action provided the intent was seen as fulfilling a duty presupposing that the original duty is derived from a correct obligation.[35] For example, when the military uses

[31] David M. Kaplan, *Readings in the Philosophy of Technology (New York, Rowman & Littlefield Publishers, Inc.,* 2009*), 179.*
[32] Ibid., 170.
[33] William L. Reese, *Dictionary of Philosophy and Religion* (New Jersey, Humanities Press, 1996), 165.
[34] Ronald L. Sandler, *Ethics and Emerging Technologies* (Boston, Northeastern University, 2014), 341.
[35] Ibid.

AI and drones for precision strike operations, there is a risk to the populace co-located in the region. This presents an ethical dilemma to the military leader and decision maker with regard to strike or abort the mission. Kant and Deontologists would say abort the mission. However, for the greater good of societal security, there is a rationale to be made for preserving the mission and saving society at large.[36]

One of the critical issues related to the design of the autonomous system embedded with AI is that designers only develop systems according to the design requirements. However, as is well known, some companies have an approach that evaluates the actions based on consequences and, if they determine that both they and others benefit from compromises, then there is no question in their eyes that they are doing what they believe to be correct. Because there is no universal consistency, this ethical approach is certainly not one that can be used to develop a proper framework for this emerging technology.[37] This is critical in that those who fund and sponsor the development of weaponized AI autonomous systems must also include an ethical criteria that will bound the system so as to allow for universal protection. This means that designers of independent AI systems must consider how these systems will be used and assess the risks associated with their integration in military warfare. Ethical guidelines and rules of engagement that will constrain the AI autonomous system are important for preserving the most effective application of these systems on the battlefield.

Utilitarianism

Utilitarianism is another central philosophy used to evaluate the practical decisions associated with the ethical development and use of technology. Its central premise, "the greatest good for

[36] Ibid.
[37] Stephen Coleman, *Military Ethics* (New York: Oxford University Press, 2013), 19-20.

the greatest number," seemingly provides an uncomplicated answer to complex questions. The utilitarian makes value decisions based on consequences rather than objective values to the exclusion of justice.[38] Thus, when we consider the utilitarian perspective in combination with the development and utilization of autonomous systems, we must do so within the context of its intention and benefit. For example, one could argue that using autonomous intelligent systems embedded in combat operations could serve a meaningful purpose by rescuing those injured on the battlefield.[39] Evaluated from a utilitarian approach, the decision would not be based on moral values, but rather consequences and proportionality making every event new unto itself and subjective by nature.[40] In that scenario, a utilitarian would factor the cost in time, lives, and money along with the consequences of the operation, but would not include in its assessment the intrinsic value of the people who need to be rescued.[41] As Chesterton says about the pragmatist, "Extreme pragmatism is just as inhuman as the determinism it so powerfully attacks."[42] The best possible consequences for the individual will be served by these systems and are consistent with the utilitarian school of ethics in that it serves as an example of "beneficence" and "non-maleficence."[43] Specifically, the actions of the Autonomous system are aimed, in this case, to promote the well-being of the individual who has been removed from harm. Briefly stated, a utilitarian ethic provides a framework for assessing the risks and benefits for contributing to the

[38] Ian G. Barbour, *Ethics in an Age of Technology* (New York: Harper Collins), 1993, 26-27.
[39] John G. Ramiccio, *The Ethics of Robotic: Autonomous and Unmanned Systems in Life-Saving Roles* (Newport, Naval War College, 2017)
[40] Germain Grisez, *Christian Moral Principles, Volume 1: The Way of the Lord Jesus* (Emmitsburg MD: Alba House, 1983), 141-7.
[41] Yvonne Masakowski (Professor, Naval War College), interview by the author, February 2018.
[42] Gilbert Keith Chesterton, *Orthodoxy* (Amazon, 2005), 28.
[43] Tom Beauchamp, "The Principle of Beneficence in Applied Ethics", *The Stanford Encyclopedia of Philosophy* (Winter 2016 Edition), Edward N. Zalta (ed.), URL = https://plato.stanford.edu/archives/win2016/entries/principle-beneficence.

greater good.[44] Thus, the platforms for artificial intelligence ought to be designed within a utilitarian ethic framework that would allow for each technology to be designed in support of the greater good, regardless of the context of the combat field or in society.

In summary, the utilitarian school of ethics is important for designers and the acquisition community to integrate into their requirements for future technology design. This is critical for future autonomous systems equipped with AI as these systems will function in a human-like manner, making independent decisions with the potential for grave consequences. These principles must be applied to ensure the well-being of those on the battlefield and in society.

The Individual Level

In isolation, a data breach of confidential information can be harmful, but processed by the tremendous speed and database of current AI systems, it can be devastating because it most certainly includes more tangential elements forming a more complete user profile. The cumulative effect of this developing individual profile enables corporations to monetize all personal information. It is a huge advantage for a company to know stable trends such as a person's financial background, transaction history, and trends tracked by all devices both known and unknown to shape the way people think and act. Because there exists the danger for people to be exploited and manipulated on an individual level, there must be an ethic that best addresses the principles and actions by and for individuals in relation to A.I.

People are becoming increasingly more aware of the types of technology involved in tracking their everyday lives and are asking more questions. Facebook was called to testify before

[44] William L. Reese, *Dictionary of Philosophy and Religion* (New Jersey, Humanities Press, 1996) Utilitarianism.

Congress and revealed their failure and breach of trust with the public. Their lack of vigilance regarding the importance of protecting individual's personal data put America's national security at risk. One recommendation would be to have Federal Guidelines developed to provide licensing and monitoring constraints surrounding the dispersal of personal data similar to that imposed by Institutional Review Boards within the medical profession.

On March 15, 2018, the Center for a New American Security created a task force on artificial intelligence and national security along with former Deputy Secretary of Defense Robert Work for the purposes of developing cutting-edge technology regulation.[45] The commercial sector eagerly greets this technology for the financial benefits; however, it is slow to respond to developing the ethical responsibility to protect and not manipulate platforms. Many of these important technologies are supported in private sector companies such as Alphabet (the parent company of Google), Facebook, Microsoft, Apple, and Amazon.[46] These are but a few technology companies that heavily influence our private and professional lives. Even ten years ago, it would have been hard to imagine the vast amounts of information gathered by and processed through these companies. Their use of AI has changed the way we think and interact in the world.

For example, AI has been embedded in numerous platforms for data collection by agencies such as Google, et al. Systems such as iRobot, iPhone's Siri, and Amazon's Alexa passively collect data without written permission from end users. This information is then shared globally to anyone who seeks to exploit it. The ethical violation within this practice is evidenced by the criticism directed against governments which have manipulated information and profiled

[45] Danny Crichton, *Washington waking up to threats of AI with new taskforce*, www.Techcrunch.com March 2018
[46] Cade Metz, *Pentagon wants help from Silicon Valley on A.I.*, March 15, 2018. https://www.nytimes.com/2018/03/15/technology/military-artificial-intelligence.html

end users to their political and financial gain.[47]

In practice, AI platforms equipped with machine learning and Artificial Intelligence provide easy access to all members of society without regard to the consequences for global security. The question is, what is the best use of AI? How can it benefit society as a whole versus just the corporate profit margin? What is the ethical application of these platforms?[48] "AI would need to be trained on ethics and would only ever be as ethical as it was trained to be."[49] Because of the potential misuse, technology experts are increasingly concerned who will be held responsible for ethical programming.

Therefore, it is incumbent upon corporations such as IBM, Google, et al., to recognize that although future successes are highly dependent upon AI and Quantum computing, there is a need to integrate rules of ethics in their design.[50] Vivek Wadhwa, an expert on corporate governance at Stanford University is concerned about the apparent legal lethargy regarding these technologies.

> "There is a public outcry today-as there should be-about NSA surveillance, but the breadth of that surveillance pales in comparison to the data that Google, Apple, Facebook, and legions of app developers are collecting. Our smartphones track our movements and habits. Our Web searches reveal our thoughts. With the wearable devices and medical sensors that are being connected to our smartphones, information about our physiology and health is also coming into the public domain. Where do we draw the line on what is legal- and ethical?"[51]

---

[47] Ellen Duffer, "As Artificial Intelligence Advances, What Are its Religious Implications?" *Religion and Politics*, last modified August 29, 2017, www.religionandpolitics.org.
[48] Bernard Marr, "How Quantum Computers Will Revolutionize Artificial Intelligence, Machine Learning and Big Data" Forbes, 5 September 2017 www.forbes.com.
[49] Jeff Catlin, "The Role of Artificial Intelligence in Ethical Decision Making, "Forbes, last modified December 21, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/12/21/the-role-of-artificial-intelligence-in-ethical-decision-making/#182ec73021dc
[50] Lance Ulanoff, "IBM is pouring $240 million into a new AI research lab at MIT," September 7, 2017, www.mashable.com
[51] Vivek Wadhwa, "Laws and Ethics Can't Keep Pace with Technology: Codes We Live by, Laws We Follow, and Computers that Move Too Fast to Care." MIT Technology Review, April 15, 2014, www.technologyreview.com

While the public demand exists for these technologies and the conveniences that they afford us, attention must be paid to the risks to our personal security, and to the potential for malicious misuse by our adversaries. This is an operational imperative for the military in that military operations are at risk of being compromised by violations that reach into the leader's decision making and technology applications. In this regard, designers must design a means of defending against potential invasion by an adversary. Similar to the human immunological response, the AI system should be designed to verify and validate any intersection of information that challenges the ethical framework within the system as a means of protecting national and societal interests.

The Societal Level

On June 5, 2018, Edward Snowden leaked classified documents revealing, to many around the world, the vast collection and processes used by the government of the United States as well as other countries to gather information on citizens.[52] The revelation that this type of information is being collected shocked many people. Since that time, there has been a gradual unfolding of even more data breaches desensitizing people to the initial loss and the use of methods used to gather information. On May 2, 2018, Cambridge Analytica announced to employees in its New York office that the company was going to seek bankruptcy as a direct effect of its manipulation of private data.[53] In addition, Facebook, Google, and Equifax serve as examples of the impact of violating societal trust and mandate the need to develop Federal Rules

[52] Paul Szoldra, "This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-secret Leaks," September 16, 2016, www.businessinsider.com.
[53] Brandy Zadrozny, and Ben Collins, "Inside the Final Days of Cambridge Analytica: Failed Rebrands, Fleeing Clients and Nerf basketball," *NBC News*, May 18, 2018, https://www.nbcnews.com/business/business-news/inside-final-days-cambridge-analytica-failed-rebrands-fleeing-clients-nerf-n875321.

and Regulations to guide and legislate each of these organizations. This example highlights the need for trust between society and these corporations. Despite the many conveniences these technologies offer, unconcerned citizens should be protected. According to Reuters, "in 2017 the NSA gathered 534,000,000 texts and cell phone call records of Americans."[54] An article discussing data breaches by large companies recently uncovered a video revealing Google's plan to gather and manipulate information on users and shape society. This system, dubbed "the ledger," gathers and processes "actions, decisions, preferences, movement, and relationships."[55]

The development of advanced surveillance platforms and social media are driven by corporate profit and will result in a compromised military if not guided by a consistent objective ethic. The misuse of some of these technologies also has implications for operational planning wherein individual soldiers using their iPhones or Bluetooth devices facilitate the aggregation of information that reveals location, troop movements, telemetry, and other critical aspects of mission planning placing military operations at risk. A lack of ethical vigilance in the judicious application of such platforms could compromise us on the level of the individual and society and, more importantly, have the potential to help our adversaries by negatively impacting our ability to fight wars

The protection of the United States is not necessarily a priority of a company just because it is located in the United States; instead, corporate profit for stockholders is the principal objective. Due to expanding global interests, some companies are willing to adapt policies most convenient for their bottom line. If the military does not have absolute control over the AI platforms, it could lose advantage. There is no guarantee that private companies would always be willing to

[54] Dustin Volz, "Spy agency NSA triples Collection of U.S. Phone Records," www.reuters.com, May 4, 2018.
[55] Vlad Savov, "Google's Selfish Ledger Is an Unsettling Vision of Silicon Valley Social Engineering," *The Verge*, May 17, 2018, https://www.theverge.com/2018/5/17/17344250/google-x-selfish-ledger-video-data-privacy.

provide the essential functions gapped by government dependency. On 14 May 2018, for example, approximately 4,000 employees and over 200 technology professionals at Google signed letters of protest over concerns that the software could be weaponized using Google's AI technology.[56]

Mark Zuckerberg and Facebook executives who appeared before U.S. Congress highlight the importance of this issue and serve as an example of the civilian compromise of information and the potential for harm to our nation's security. Some might consider the information data-mined from Facebook to be insignificant; however, combined with other sources, it helps to form a more complete picture of society.

This is not about the innocuous use of information for commerce but rather information garnered for manipulation and exploitation of whole segments of society by those with malicious intent. Indeed, our adversaries may harvest the benefits of information and data mined from these sites to be used in a malevolent manner against us. The collectors are not necessarily the manipulators but still have the responsibility for the security of the information that these services have no right collecting. Alarmingly, there are an increasing number of instances whereby home automated devices such as Amazon's Alexa, have recorded and transmitted private conversations.[57]

Really designed to gather information about a symbiotic relationship between people and their personal information, these systems are not designed to improve society and make it better. Rather, they are designed to collect information about us. Specifically, these systems serve their designers and corporate sponsors by providing inside information about each of us via

[56] Michael Kan. "Google Staffers Resign Over Work on Pentagon AI Project." *PCMagazine*, May 14, 2018, www.pcmag.com.
[57] Tyler Durden, "Unplug Your Alexa Devices Right Now…You're Being Hacked." *Zerohedge*, May 25, 2018. www.zerohedge.com.

surveillance within the privacy of one's home. It is not a leap to imagine that such intimate knowledge will be used in the future to shape our society. Personal freedom of independent thought, personal rights to privacy, and personal independent choice will be a thing of the past. Once exposed it fosters a toxic environment as the shift from a claimed benefit to the user to outright surveillance for the purposes of shaping or exploiting society.[58]

Our national constitutional rights are under siege in this new digital warfare wherein our adversaries have the means to shape our thinking, provoke civil unrest, and influence a nation's policies and future without firing a shot, based on data gathered and mined from the social media. They too share in the advances of technology and their application may be used to benefit their aims for their nation's economic and/or military success.

There is an inevitability with the violations for privacy in other countries. The Chinese Communist Party imposes limitations on the internet and information for their people. The level of trustworthiness is evaluated by a social score that reflects each individual's education, socioeconomic status, social status, and political view.[59] This level of societal control may await us all and threatens our constitutional freedoms in the US. The Chinese do not expect the protections that our free society presupposes. The PRC recently announced grouping people according to their health, genetics, and abilities. Who should receive the greater share of society? The communists' focus is on the supremacy of the state over all, whereas we are always expected to value the dignity of every person which is not mutually exclusive to the benefit of the state.[60] The recent actions of Facebook are similar as they undermine the trust of individuals

[58] Dr. Yvonne Masakowski (Professor, Naval War College), interview by the author, February 2018.
[59] "China Assigns Every Citizen A 'Social Credit Score' To Identify Who Is And Isn't Trustworthy," *CBS New York*, April 24, 2018, http://newyork.cbslocal.com/2018/04/24/china-assigns-every-citizen-a-social-credit-score-to-identify-who-is-and-isnt-trustworthy/
[60] Ibid.

and society and thus highlight the responsibility of Congress to protect the security of the United States.

AI and the Battlefield

A recent report by Booz Allen Hamilton recommends significant investment for the United States to lead in this technology and views artificial intelligence as a significant and critical part of our national strategy and implementation.[61] In fact, the U.S. Army is currently working on capitalizing on the advantages of wearable devices for telemetry assisting in preventative medicine and treatment on the battlefield. [62]

Dr. Yvonne Masakowski, an expert in AI and Unmanned Systems, supports a proper implementation of this technology and warns of possible dangers if there is no suitable human oversight:

> "These AI systems have demonstrated tremendous capacities for managing vast amounts of data that can enhance Situational Awareness and decision making in the military operational environment. The integration of cognitive models and mission plans in the design of autonomous unmanned systems have moved this technology forward as an independent platform. However, as these systems become more automated and capable of independent decision making, one must consider the impact of relinquishing the authority of decision making in the combat operational environment."[63]

Because so much is at stake in military applications, great care and oversight must be taken to ensure trust between the programmer and end user.[64] AI systems may have programmed

[61] Joanna Stern, "Facebook really is Spying on You, just Not through Your Phone's Mic: How to Limit the Amount of Data Facebook and Advertisers are Collecting about You," *Wall Street Journal*, March 7, 2018, https://www.wsj.com/articles/facebook-really-is-spying-on-you-just-not-through-your-phones-mic-1520448644
[62] Kathleen Curthoys, "Soldiers May Soon Have Implantable Health Monitors and Robotic Surgeries Done Remotely," *Army Times*, May 18, 2018, www.armytimes.com.
[63] Yvonne Masakowski, "AI and Autonomous Systems: The Evolution of Warfare in the 21st Century," Diffusion and Adoption of Innovation Studio Summit (DAISS)
[64] Ibid.

information, but lack the ability to contextualize for specific applications and this could lead to grave errors particularly if a malicious actor manipulates the platform information.[65] The examples in this paper show that many essential information systems are currently compromised among civilian companies sought for collaboration in military applications.

Leaders in the United States are rightly seeking the best and the brightest for a technological advantage in the world. The Defense Innovation Board received the assistance of several in the private sector, to include the CEO of Alphabet, to integrate a technological transition. Foreseeing possible ethical conflicts with the use of their deep learning software for military applications and analysis, Google committed to a "non-offensive" application.[66] Technologies provide a significant advantage across all domains, however, as one army officer accurately said regarding AI, "capabilities create dependencies, and dependencies create vulnerabilities, both computer-based systems and space-based systems are vulnerable to being hacked by an enemy."[67]

At the Munich security Conference in 2018, leaders expressed concern about potential problems with the use of technologies requiring less and less oversight by humans to operate offensively on the battlefield. NATO's former Secretary-General Anders Fogh Rasmussen said, "The use of robots and artificial intelligence within the military might make the whole world more unstable. For that reason, I think we should elaborate on an international and legally binding treaty to prohibit the production and use of what is being called autonomy for weapons."[68] Secretary of Defense Mattis commented regarding battlefield implementation, "if

[65] Ibid.
[66] Cade Metz, "Pentagon Wants Silicon Valley's Help on A.I.," *New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/technology/military-artificial-intelligence.html
[67] Williamson Murray, "Technology in the Future War," Defining Ideas, 14 November 2017, https://www.hoover.org/research/technology-and-future-war
[68]Brussels Bureau, *AI in conflict: Cyber war and robot soldiers,"* www.Euronews.com, February 16, 2018.

we ever get to the point where it is completely on automatic pilot referring to unmanned aerial vehicles (UAV), we are all spectators. That is no longer serving a political purpose. And conflict is a social problem that needs social solutions, people – human solutions."[69] Specifically, if we are to ensure national and global security, then part of our strategy in the development of these AI systems must be a policy that integrates and includes legal, ethical, and moral implications in the design phase. There are currently no specific design requirements to address ethical issues in the design of weaponized autonomous systems other than the legal implications of these designs.[70] There must be consideration given to the risks to society, peace, and to elevating warfare as a result of a misuse or misfiring of these weapons in the future.

Technology legend and budding technological ethicist Elon Musk thinks, "artificial intelligence is ultimately more dangerous than nuclear weapons,"[71] and despite efforts to fully automate his automobiles for the purposes of safety, he believes that regulation and oversight are an ethical requirement for the proper use of this technology. It is the platform interoperability and potential for manipulation that most concerns Musk.[72] Furthermore, the issue of long term consequences are raised when one thinks of the fact that in the algorithms that comprise the system is the capability for the AI system to design and reconfigure itself in the future. Based upon recent development of the robot, SOPHIA, there is a real risk associated with the development of future robots that will be capable of reconfiguring themselves and forming independent judgments on human behavior.[73] This places the human in a subordinate position to

---

[69] No Author listed, "*Artificial intelligence poses questions for nature of war: Mattis,"* www.PHYS.org, February 18, 2018.
[70] Dr. Yvonne R. Masakowski, *Future Worlds Workshop: Gravely Group* (Newport: Naval War College, 2017)
[71] "Artificial Intelligence poses questions for nature of war: Mattis," *Phys.Org*, February 18, 2018, https://phys.org/news/2018-02-artificial-intelligence-poses-nature-war.html
[72] Ibid.
[73] Amyia Moretta, *"Interview with Robot that said it would Destroy Humans."* www.etftrends.com, May 29,2018 https://www.etftrends.com/robotics-ai-channel/interview-with-robot-that-said-it-would-destroy-humans/

the Robot in the future and is something every military person should be concerned with as time moves forward. How would be defend ourselves against this new adversary?

With the slow inoculation to the relegation of privacy rights and personal information, what can be done? The initial outrage recedes as the frequency of violations increase. Indeed, there is a percentage of society that remains unaware of the threat and focuses instead on the benefits of these systems touted by their corporate designers.

While there is a balance that can be struck in using AI for optimizing societal benefit, there must be equal attention focused on the long term consequences to warfare. It is incumbent upon leadership to address the need for ethical guidelines to ensure the success across all domains and the full spectrum of operations.[74] Many of our new systems and devices are surveillance platforms that are not as much designed to be helpful, as developers claim, but rather are designed to gather information. For these corporations and their shareholders, the primary motivation of this relationship is not to make society better but to monetize information. It is not just a concern in America. In a recent address the Union Home Minister of India warned those responsible for security that, "we have become dependent on our information systems for a majority of the essential elements of our lives and these systems are vulnerable."[75] He calls for vigilance and encourages participation with other security forces around the world to defeat cyberattacks.

[74] Yvonne Masakowski, "AI and Autonomous Systems: The Evolution of Warfare in the 21st Century," Diffusion and Adoption of Innovation Studio Summit (DAISS)

[75] "Cyber-Dependency has increased vulnerability to attacks against civilian and military infrastructures," India News, March 15, 2018, http://6dnews.com/feed-items/cyber-dependency-has-increased-vulnerability-to-attacks-against-civilian-and-military-infrastructures-shri-rajnath-singh/

AI and future implications for society and warfare

The efforts of the United States to develop and use AI could be thwarted and current systems compromised due to a lack of governmental focus. China takes advantage of U.S. bankruptcy laws and a negligent government committee to purchase the next generation software used by the United States Military. The Committee on Foreign Investment in the United States (CIFUS) has approval authority for the foreign sale of technology, but it lacks the capacity to fulfill its obligations.[76] This inaction alone could be a potent threat to our technological future. This is opening the door to a thief. In addition, the Chinese, could purchase the minimum amount of stock in a company nullifying our ability to use it. In a lecture Professor Dennis referred to this as economic Anti-Access, Anti-Denial.[77] Consider what a senior official at the Treasury Department stated: "The goal, he added, is to turn our own technology and know-how against us in an effort to erase our national security advantage."[78] Efforts to make the necessary changes to CFIUS to ensure protection of technology and information are significantly hindered by a set bureaucratic speed, as well as companies and investors who stand to profit from those sales.[79]

Specifically addressing the current greatest rival in AI, Senator Cornyn said, "Just imagine if China's military was stronger, faster and more lethal."[80] Experts agree that AI may perform intricate calculations with greater speed and accuracy than humans; however, it is necessary for humans to remain in control. Several experiments have shown that AI, if permitted, will deviate

[76] Cory Bennett and Bryan Bender, "How China Acquires 'the Crown Jewels' of U.S. technology: The U.S. Fails to Adequately Police Foreign Deals for Next-Generation Software That Powers the Military and American Economic Strength," *Politico*, May 22, 2018, www.politico.com.
[77] Michael Dennis, "Science, Technology, and Strategy" (Naval War College, Seminar Notes), May 10, 2018.
[78] Bennett, Cory and Bender, Bryan, How China acquires 'the crown jewels' of U.S. technology: The U.S. fails to adequately police foreign deals for next-generation software that powers the military and American economic strength. www.politico.com, 22 May 2018.
[79] Ibid.
[80] Ibid.

from the original programming which could cause problems for the user and possibly allow hacking from bad actors.[81]

Experts say that the future for these AI systems will only be more influential as the computing power increases. The sheer volume of information processed daily far exceeds our ability to calculate the development of Quantum computing and AI to process vast amounts of data. "Quantum computing is expected to be able to search very large, unsorted data sets to uncover patterns or anomalies extremely quickly"[82] This ability to handle Big Data has implications for monitoring information across all domains on a global scale. This is important because any perturbation across the global security network could potentially provide the adversary with a pulse in the security network that is vulnerable to exploitation and place a nation at risk. Despite the implementation of quantum computing, proven concerns should remain at the forefront. Chiefly, how will the government of the United States fulfill its obligation to protect and preserve our nation from future exploitation?

Conclusions and Recommendations

The evolution of Artificial Intelligence and autonomous unmanned systems is accelerating at an exponential rate. Given these advances, there is a relatively small window of opportunity to integrate a framework of ethics into their design. We recognize the tremendous benefits and advantages of these technologies to individuals and to society. That said, it is a leadership imperative to infuse a framework of ethics into the design of future advanced technologies as a means of preserving human welfare. The ethical consequences for their application in the

[81] William Knight, "How Can We Be Sure AI Will Behave? Perhaps by Watching It Argue with Itself," *Technology Review*, May 3, 2018. https://www.technologyreview.com/s/611069/how-can-we-be-sure-ai-will-behave-perhaps-by-watching-it-argue-with-itself/

[82] Bernard Marr, "How Quantum Computers Will Revolutionize Artificial Intelligence, Machine Learning And Big Data." *Forbes*, 5 September 2017.

military battlespace are dire for society and our personal freedoms. Indeed, advances in AI, machine learning, neural networks, and computational modeling will continue to accelerate in the future. Thus, we need to be assertive in the application of ethical guidelines for designers of weaponized autonomous systems as these technologies have the potential for generating harm to society as a whole. We must adhere to the ethical side of the equation and assess and evaluate the costs, risks, and benefits of each technology within the ethical framework as we move forward as a nation.

The construction and interoperability of these AI systems become, if manipulated, a single source of failure compromising not only one element of a person's life but rather robbing them of their true independence. This undermines the foundational trust necessary for the security of a society. If everything is recorded, processed, and stored; then, what assumptions can be made of probabilities that information will remain secure for least one if not two generations? When applied across the three domains of the individual, society, and military applications, it is essential to require proper oversight for the implementation and use of AI systems for the highest and greatest good. Only then will trust be reestablished between government and society.

Specifically, the United States government must develop regulations to ensure the safety of society as a whole and to defend against potential harm both within and across other nations. To this end, legislation must be developed to ensure that virtue ethics are integrated into the principles for the design of future advanced technologies. For example, weaponized autonomous systems designed with AI should be developed with an integrated module that will include ethical constraints and guidance to provide an opportunity for the system itself to evaluate the context of its application. As these systems become more independent and able to form their own decisions, the cost to society and military warfare are escalated and lead to harm. Congress

must do this despite potential opposition by cultures that do not share appreciation of the virtue ethic.

The 21st century, similar to the Industrial Revolution, is a transformative time with the emergence of advanced system designs that will change the world and the character of warfare. Advances in AI, machine learning, neural networks, as well as quantum computing power contribute to shaping the future of warfare. As a society, we must consider the consequences for both the military and for society. Specifically, Congress must develop a set of Federal regulations and legislation to instantiate requirements that will ensure societal protection as well as for the design of and development of future AI systems. Ethicists, sociologists, psychologists, clergy, et al., should have a voice in the development of policies for acquisition doctrine. An integration of specific elements of the three ethical theories presented in this paper would best serve to develop the needed ethical framework to advise Congress. The integration of the three schools of ethical theories presented herein must be integrated in an ethical framework to guide the development of Congressional policies for the design of future technologies. For example, one can envisage legislation that would integrate the utilitarian perspective wherein risk assessment could be used to evaluate the cost/benefit and risk analysis. Likewise, principles of virtue ethics could be integrated in the guidance for Congressional legislation to ensure that the dignity of mankind and the highest moral ideals are preserved. Similar to the Declaration of Independence, one can imagine a policy that ensures the preservation of our Inalienable human rights within the world of Autonomous Systems. In this way, mankind has preserved its dignity and level of superiority and dominion over future AI designs, as well as preserving the moral ideals and guaranteeing that consistent rules of engagement for the future battlefield are ensured.

Additionally, consideration should be given for dual use applications of technologies that may have negative consequences for individuals, society, and military operations. The United States must also consider the importance of Foreign Policy and the potential for exploitation by our adversaries. Formal guidance and monitoring for the development of these technologies must be established to ensure that our nation is developing technologies that cannot be used against its citizens. Although this paper has highlighted the potential negative consequences for the development of AI technologies and autonomous systems, it is equally important to highlight the potential benefits of developing unique military systems that are essential to protect and defend our nation from future adversaries. We must maintain the decision advantage over our competitors and especially those who threaten our American freedoms.[83] That said, it is critical for governments to view the application of Artificial Intelligence in weaponized systems as a potential threat similar to the development of nuclear weapons in the future. There is an ethical responsibility to consider all costs, individual, societal and military, as governments seek to exploit the advantages that AI has to offer to military platforms. Global security must be ensured but not at a cost to those it protects. In summary, ethical consideration must be given across each ethical school of thought with regard to the design and implementation of AI autonomous systems in the future to ensure that we are seeking to preserve mankind and society.

[83] Dr. Yvonne R. Masakowski, *Future Worlds Workshop: Gravely Group* (Newport: Naval War College, 2017)

SELECTED BIBLIOGRAPHY

Armstrong, Martin. "The Future of AI." *Statistica*," November 18, 2016. www.Statistica.com.

Barbour, Ian. *Ethics in an Age of Technology*. San Francisco: Harper, 1993.

Bennett, Cory and Bryan Bender. "How China Acquires 'the Crown Jewels' of U.S. Technology: The U.S. Fails to Adequately Police Foreign Deals for Next-Generation Software That Powers the Military and American Economic Strength" *Politico*, May 22, 2018. www.politico.com.

Beauchamp, Tom, "The Principle of Beneficence in Applied Ethics", *The Stanford Encyclopedia of Philosophy* (Winter 2016 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2016/entries/principle-beneficence/>.

Brussels Bureau, *AI in conflict: Cyber war and robot soldiers"*, www.Euronews.com, February 16, 2018

Catlin, Jeff. "The Role of Artificial Intelligence in Ethical Decision Making." *Forbes*, December 21, 2017.
https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/forbestechcouncil/2017/12/21/the-role-of-artificial-intelligence-in-ethical-decision-making

CBS New York. "China Assigns Every Citizen A 'Social Credit Score' To Identify Who Is And Isn't Trustworthy." April 24, 2018,
http://newyork.cbslocal.com/2018/04/24/china-assigns-every-citizen-a-social-credit-score-to-identify-who-is-and-isnt-trustworthy/

Chesterton, Gilbert Keith. *Orthodoxy*. Amazon Digital, 2005. Kindle Books

Crichton, Danny "*Washington waking up to threats of AI with new taskforce"*, www.Techcrunch.com March 2018
Coleman, Stephen, *Military Ethics*, New York: Oxford University Press, 2013

Curthoys, Kathleen. "Soldiers may soon have implantable health monitors and robotic surgeries done remotely." *Army Times*, May 18, 2018. www.armytimes.com

Davis, Nicola. "Smart Robots, Driverless Cars Work-but They Bring Ethical Issues Too." *The Guardian*, Last Modified October 19, 2013.
https://www.theguardian.com/technology/2013/oct/20/artificial-intelligence-impact-lives

Delgado, Ana. *Technoscience and Citizenship: Ethics and Governance in the Digital Society*. Cham, Switzerland: Springer, 2016.

Duffer, Ellen. “As Artificial Intelligence Advances, What Are its Religious Implications?” *Religion and Politics*. Last Modified August 29, 2017. www.religionandpolitics.org.

Durden, Tyler. “Unplug Your Alexa Devices Right Now…You’re Being Hacked.” *Zerohedge*, May 25, 2018. www.zerohedge.com.

Grisez, Germain. *Christian Moral Principles, Volume 1: The Way of the Lord Jesus.* Emmitsburg, MD: Alba House, 1983.

Guardini, Romano. *Letters from Lake Como: Explorations on Technology and the Human Race*. Washington, DC: William B Eerdmans Publishing, 1994.

Kan, Michael. “Google Staffers Resign over Work on Pentagon AI Project.” *PCMagazine*, May 14, 2018. www.pcmag.com.

Kaplan, David M. *Readings in the Philosophy of Technology*, New York, Rowman & Littlefield Publishers, Inc., 2009

Knight, William. “How Can We Be Sure AI Will Behave? Perhaps by Watching It Argue with Itself.” *Technology Review*, May 3, 2018. www.technologyreview.com

Kreeft, Peter. “Pillars of Unbelief- Kant.” *National Catholic Register, Jan-Feb 1988*. www.peterkreeft.com

India News. “Cyber-Dependency has increased vulnerability to attacks against civilian and military infrastructures.” *India News*, March 15, 2018. http://6dnews.com/feed-items/cyber-dependency-has-increased-vulnerability-to-attacks-against-civilian-and-military-infrastructures-shri-rajnath-singh/

Lin, Jenkins, Keith Abney and Ryan Jenkins. *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*. Oxford: Oxford University Press, 2017.

Jenkins, Jack. “The (Holy) Ghost in the Machine: Catholic Thinkers Tackle the Ethics of Artificial Intelligence.” *Crux.* Last Modified, 26 May 2018 https://cruxnow.com/church/2018/05/26/the-holy-ghost-in-the-machine-catholic-thinkers-tackle-the-ethics-of-artificial-intelligence/

Martyn, Amy. “The Amazing, Ever-Changing Story of the Equifax Hack. “ *Consumer Affairs*, 31 May 2018.

Marr, Bernard. “How Quantum Computers Will Revolutionize Artificial Intelligence, Machine Learning And Big Data.” *Forbes*, 5 September 2017.

Masakowski, Dr. Yvonne R. *Future Worlds Workshop: Gravely Group* (Newport: Naval War College, 2017)

Metz, Cade. “Pentagon Wants Silicon Valley’s Help on A.I.” *New York Times*, March 15, 2018. https://www.nytimes.com/2018/03/15/technology/military-artificial-intelligence.html

Miller, Russell A. *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affai*r. Cambridge: Cambridge University Press, 2017.

Murray, Williamson. “Technology in the Future War.” *Defining Ideas*, November 14, 2017. *https://www.hoover.org/research/technology-and-future-war*

Morgan, Steve. “Top 5 Cybersecurity Facts, Figures and Statistics for 2018.” *CSO*, Jan 23, 2018. www.csoonline.com

Moretta, Amyia *“Interview with Robot that said it would Destroy Humans.”* www.etftrends.com, May 29 2018 https://www.etftrends.com/robotics-ai-channel/interview-with-robot-that-said-it-would-destroy-humans/

Noyes, Dan. “The Top 20 Valuable Facebook Statistics.” *Zephoria*. Last Modified May 2018. https://zephoria.com/top-15-valuable-facebook-statistics/
Phys.org. “Artificial Intelligence poses questions for nature of war: Mattis.” *Phys.Org*, February 18, 2018. https://phys.org/news/2018-02-artificial-intelligence-poses-nature-war.html

Tegmark, Max. *Life 3.0: Being Human in the Age of Artificial Intelligence*, New York: Alfred A. Knopf, 2017.

Ramiccio, John G. *The Ethics of Robotic. Autonomous and Unmanned Systems in Life-Saving Roles*, Newport, Naval War College, 2017

Sandler, Ronald L. *Ethics and Emerging Technologies*. Boston: Northeastern University, 2014.

Singer, P.W. *Wired For War*. New York: Penguin Press, 2009.

Savov, Vlad. “Google’s Selfish Ledger Is an Unsettling Vision of Silicon Valley Social Engineering.” *The Verge*, May 17, 2018, https://www.theverge.com/2018/5/17/17344250/google-x-selfish-ledger-video-data-privacy
Szoldra, Paul. “This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-secret Leaks.” September 16, 2016. www.businessinsider.com.

Stern, Joanna. "Facebook really is Spying on You, just Not through Your Phone's Mic: How to Limit the Amount of Data Facebook and Advertisers are Collecting about You." *Wall Street Journal*, March 7, 2018. https://www.wsj.com/articles/facebook-really-is-spying-on-you-just-not-through-your-phones-mic-1520448644

Ulanoff, Lance. “IBM is pouring $240 million into a new AI research lab at MIT.” *Mashable*. September 7, 2017. www.mashable.com

Vanian, Jonathan. “Facebook CEO Mark Zuckerberg Wins Would-Be Congressional Grilling.” *Fortune*, April 11, 2018.

Vatican. *Catechism of the Catholic Church.* Doubleday Books: New York, 1995

Vallor, Shannon. *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting.* Oxford: Oxford University Press, 2016.

Volz, Dustin, “Spy agency NSA triples Collection of U.S. Phone Records,” www.reuters.com, May 4, 2018.

Wadhwa, Vivek. “Laws and Ethics Can’t Keep Pace with Technology: Codes We Live by, Laws We Follow, and Computers that Move Too Fast to Care.” *MIT Technology Review*, April 15, 2014. www.technologyreview.com

Waddell, Kaveh and Stephanie Stamm. “A Timeline of Government Data Breaches.” *The Atlantic*. Last Modified July 6, 2015. https://www.theatlantic.com/politics/archive/2015/07/a-timeline-of-government-data-breaches/458352/

Welsh, Sean. *Ethics and Security: Policy and Technical Challenges of the Robotic Use of Force*. New York: Routledge, 2018.

Zadrozny, Brandy and Ben Collins. “Inside the Final Days of Cambridge Analytica: Failed Rebrands, Fleeing Clients and Nerf basketball.” *NBC News*. Last Modified May 18, 2018. https://www.nbcnews.com/business/business-news/inside-final-days-cambridge-analytica-failed-rebrands-fleeing-clients-nerf-n875321

No Author listed, “*Artificial intelligence poses questions for nature of war: Mattis”*, www.PHYS.org, February 18, 2018.