DEVELOPMENT OF TARGET LOCATING SOFTWARE ON EMBEDDED SYSTEMS

THE ETHICAL AND STRATEGIC DEVELOPMENTS IN WARFARE THROUGH AUTONOMOUS COMBAT TECHNOLOGY

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science University of Virginia
In Partial Fulfillment of the Requirements for the Degree Bachelor of Science in Electrical and Computer Engineering

By Lilian Price

October 27, 2022

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

ADVISORS

Catherine D. Baritaud, Department of Engineering and Society

Harry Powell, Department of Electrical and Computer Engineering

One of the main objectives of the United States revolves around national security, whether that be within the United States or globally. With the rise in concerns for national security, the government has increased military funding in order to improve technology that can assist with internal and external threats, and create an advantage to other world powers such as Russia, China, and North Korea (Fiott, 2018, p. 41). This rise in funding has generated a new generation of technology, specifically focused on autonomous weapons, meaning devices that use "theoretical methods and techniques for simulating and expanding human intelligence", and are essentially self-taught (Cao, 2017, p. 701). These devices have been implemented as missiles, aircrafts, drones, and other pre-existing weapons involved in armed combat. Due to the rise in these autonomous weapons, a new wave of military tactics and ethical concerns have risen.

The motivation behind looking further into the development of these autonomous weapons stems from the ethical and societal implications that arise from these systems. Given that autonomous weapons are primarily used in combat where human lives are the primary data pool, the risks of these devices pose potentially harmful consequences on a massive scale. My technical research and tightly coupled STS research both look into the development of these systems both on a hardware and software level in order to gain perspective into the implications of autonomous weapon technology in the future. On the technical side, my team and I will develop a target locating sensor that will consist of both an infrared laser component in addition to a visual camera-based component for two systems of target detection. By creating a target locating device, my team will be able to assess design decisions that result in device failure and user misuse alongside the limitations of target locating software. This technical project will be conducted next semester under the advice of Harry Powell, who is an Associate Professor of Electrical and Computer Engineering in the School of Engineering and Applied Science. Tightly

coupled, my STS project focuses on the ethical implications of autonomous weapons that use target locating software, and the risks associated with device failure and user misuse. These implications are analyzed through the use of a sociotechnical model, and the broader social scope is explored using Actor-Network Theory (ANT).

DESIGN OF TARGET LOCATING SOFTWARE ON AN AERIAL DRONE

Under the advice of Electrical and Computer Engineering Professor Harry Powell, myself alongside a team of other computer and electrical engineers, which will be chosen next semester, will seek to develop a target locating system through a dual authentication network. Prior to the development of this system, this state of the art technical report covers the research behind the development of this potential design project.

This project seeks to create a target locating system in order to generate a higher range of accuracy on an autonomous drone. This project creates a system through the implementation of Infrared (IR) sensors and a camera which provide data back into an autonomous flight device. This will allow for a higher resolution of imagery and a dual authentication system, providing more accurate data from which the autonomous device can learn from in order to more accurately locate a given target. Designing this system using IR sensors will support a "high precision that goes beyond the accuracy of [a] standard [commercial] GPS," providing the device with more accurate information (Badakis, Koutsoubelias, Lalis, 2021, p. 4). Previous designs typically include an array of high-definition cameras in order to generate active feedback to a control center for target identification (Hartmann et al., 2022, p. 3). Additionally, other designs include a GPS system while relying heavily on computer software for "geometric matching of 2D materials" in order to properly identify a target (Jaeger, Bers, 2001, SPIE Proceedings). However in real applications, the use of high definition cameras can grow ineffective due to the

changing weather and visibility conditions within a field of interest, and GPS sensors pose a risk of lacking the high resolution data that an unmanned aircraft needs to accurately distinguish between targets. Therefore, in order to implement a camera which has a greater ability to detect various terrain, another form of target confirmation is needed.

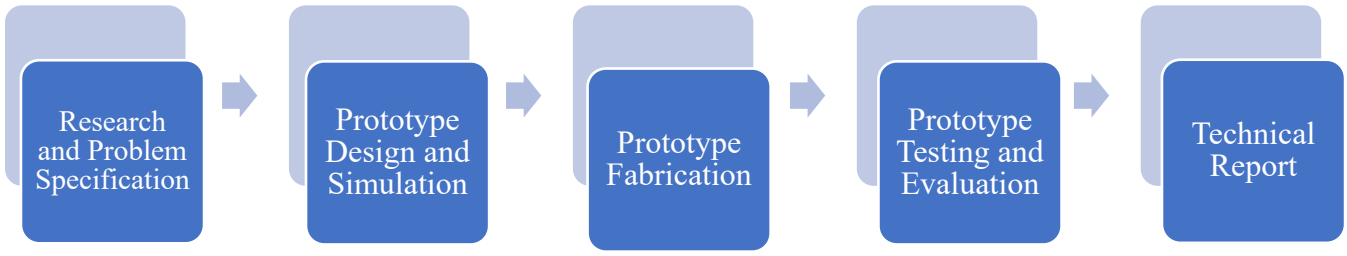

Figure 1: Target Tracking Dual-Authentication System Design Plan Outline. The design project takes place in five major steps from research and design to the technical report (Price, 2022).

The design and implementation of this embedded system will take place during a semester-long capstone course, which will be led by Professor Harry Powell in the Electrical and Computer Engineering Department of the School of Engineering and Applied Science at the University of Virginia. The design process will consist of five major steps occurring over 14 weeks, which can be visualized in Figure 1.

EXPANSION OF GOVERNMENT FUNDING FOR LETHAL AUTONOMOUS WEAPON SYSTEMS

The United States government, over a five-year period, allocated $2 billion to the development of technology such as lethal autonomous weapons systems (LAWS) in order to be

implemented during warfare (Di Corpo, 2021, pp. 260). Since this technology is in its first stages of development, many ethical concerns rise from the potential of misuse of these weapons. While some government and defense contracting officials argue that developments in autonomous weapons protect national security and military personnel, there is a significant reason for speculation that implementing autonomous weapons into armed combat creates potential situations of mass destruction and casualties. In addition, these fears of misuse are echoed by the American people due to their mistrust in government transparency when it comes to national security. This public perception of government abuse in relation to national security and times of war stems from the 1960s with both the Vietnam War and scandals such as Watergate occurring within the same decade. Although slightly recovered, this mistrust has since continued to decline in the 2000s from the 9/11 terrorist attacks in addition to the government's involvement in the wars in Iraq (Beyond Distrust: How Americans View Their Government, 2020).

Despite this mistrust, the government intends to expand the use of LAWS under their supervision, which was made clear by Bob Work, the US Deputy Secretary of Defense in his introduction of the Third Offset Initiative:

> So, DOD is -- we are going to leverage AI technology, particularly in things like cyber defense, electronic warfare defense, missile defense. But what's also clear to us is that we need to go to huge new levels of human-machine symbiosis, allowing each to do what the other does -- which is to do what they do best (2016, para. 10).

The public perception of government control surrounding technology such as LAWS begets public concerns surrounding the potential misuse of these systems bending the rules of ethics in order to push an agenda under the guise of national security. These systems contain an extensive potential for abuse, which in the hands of the government is far from the control of the public.

ETHICAL DILEMMAS SURROUNDING AUTONOMOUS WEAPON SYSTEMS

In analyzing the developments in autonomous weapons, some of potential issues in autonomous systems, are revealed through Shama Ams:

> These systems carry the risk of algorithmic bias due to flaws in underlying training data and its interpretation, difficulty in maintaining meaningful human control, the potential for more conflict due to fewer barriers to military engagement, and uncertainty in accountability for machine error (2021, para. 1).

Although broad, these four key issues each contain subsets of specific problems that must amount as a result of the unencumbered development of LAWS. Without regulation, these issues quickly amass making it more difficult to place limitations on this technology. This rapidly growing ethical dilemma is demonstrated in Figure 2 below, showing just a small portion of highly debated roadblocks stemming from LAWS technology.

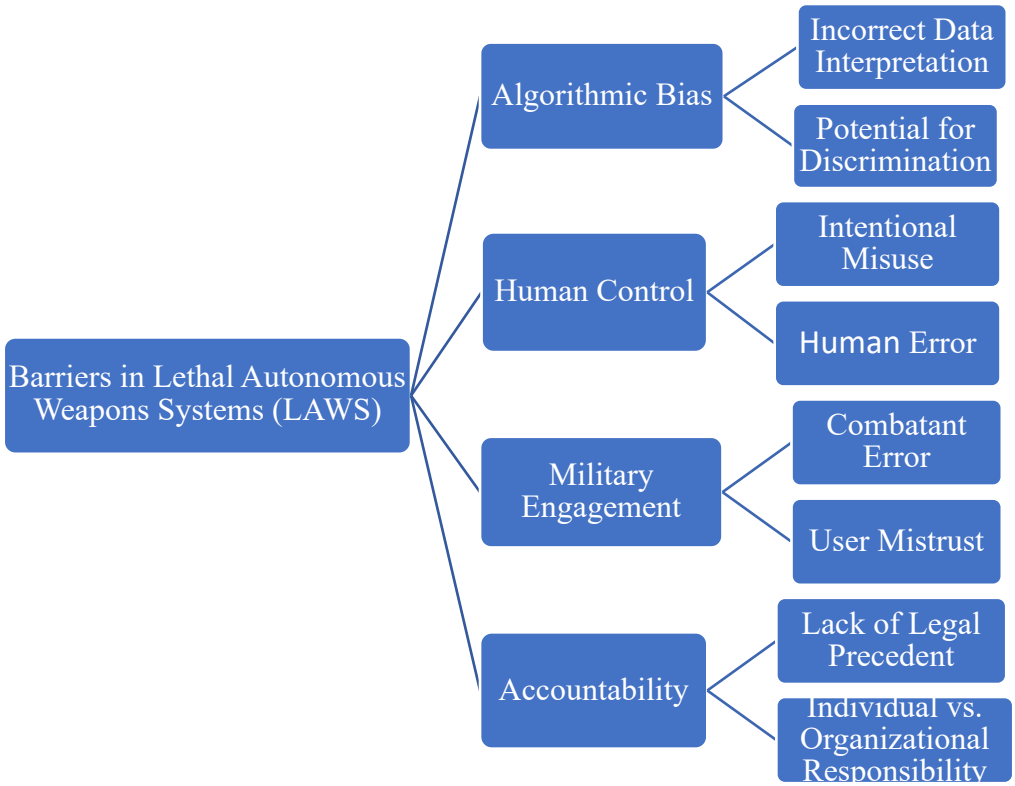

Figure 2: Potential Risk Categories for the Implementation of Lethal Autonomous Weapon Systems (LAWS). Each potential risk category of autonomous weapons contains a multitude of

smaller potential risk factors, demonstrating the numerous ethical dilemmas associated with autonomous weapon systems (Ames, 2021).

While some government and defense contracting officials argue that developments in autonomous weapons protect national security and military men and women, there is a significant reason for speculation that implementing autonomous weapons into armed combat creates potential situations of mass destruction and casualties. Currently, these systems lack an "ethical benchmark" which would "establish rules for armed combat," giving these systems no ceiling for innovation and use (Zacharias, Schmitt, 2021, pp. 2). This "lack of a coherent regulatory regime" creates scenarios for legal uncertainty, making it difficult to hold any individual or organization accountable in the case of human misuse or system error (Hartmann et al., 2022, p. 2). So, the apparent solution comes through government regulation of the development of these systems, however therein lies the conflict. Not only is the government the sole organization that can regulate this technology, but they are also the largest beneficiaries and benefactor of autonomous weapon systems. This conflict of interest, alongside the public concern of "government transparency" poses the largest threat to the development of these systems (Pohle & Audenhove, 2017, p. 3).

MODELING THE NETWORK OF AUTONOMOUS WEAPON TECHNOLOGY DEVELOPMENT

In order to study the implications of autonomous technology, Shi and Zheng suggest making joint research between basic theory and the technology of intelligence the primary goal (2006, p. 811). This would be accomplished through studying the relationship between these systems, being AI, and the end goal, which is replicating human intelligence artificially. In order

for this to be accomplished, a sociotechnical system must be developed, which can be seen in Figure 3 on page 8, in order to form a more holistic view of these systems.

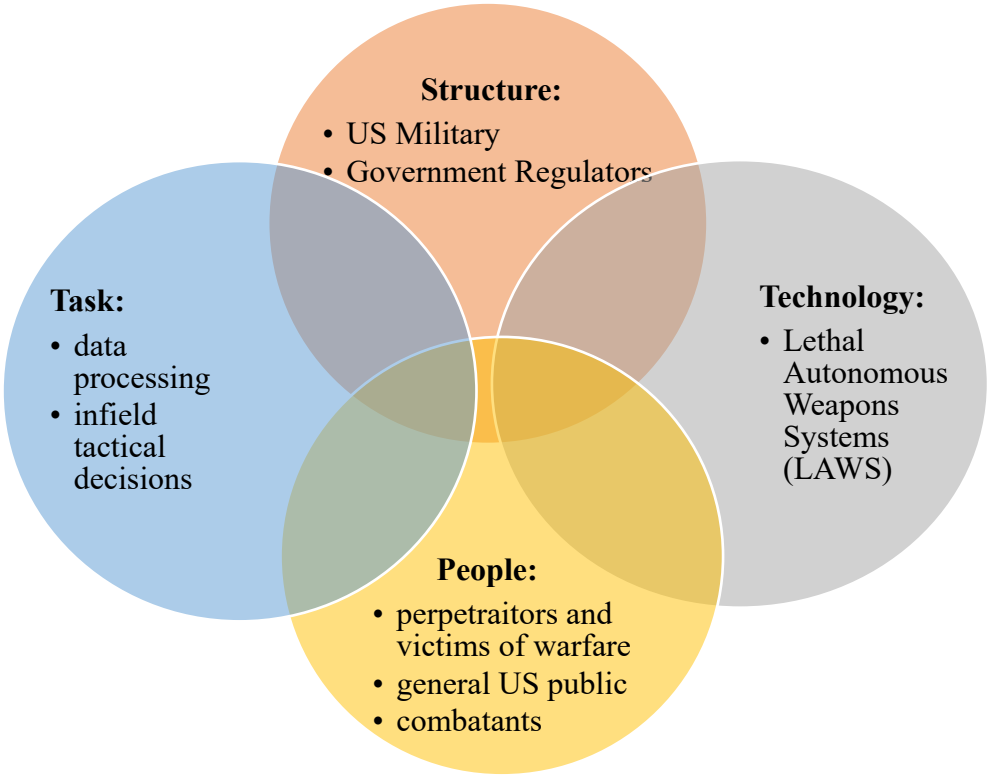

Figure 3: Autonomous Weapons Sociotechnical Model. The development of autonomous weapon systems heavily relies on the interaction between not only the technology itself but also the contributors and environment (Price, 2022).

This model relies on the relationship between four key components: the structure, technology, task and people. The sociotechnical framework provides a system for "modelling and analyzing complex systems" through "humans applying technology to perform work through a process within a social structure" (Oosthuizen & Pretorius, 2016, p. 17). In this case, the technology , which is LAWS, grows and forms within a multifaceted system that consists of both the controlling structure and the people in addition to the task. Within this model, the controlling structure is made up of key users and developers, which consists of both government regulators who influence the trajectory of innovation and the US military, who are the primary users of weapon technology. Closely related are the people, who in the case of the military are the

combatants who make up the primary users of autonomous weapon technology. In opposition are the victims of these complex weapons systems in addition to the US public who will be informed on the outcomes that the introduction of such weapons causes. Finally, there is the influence of the task, which consists of the design specifications of the autonomous system such as target identification, data processing, and data analysis. In order for this system to develop in tandem into a fully functioning basis for LAWS, there needs to be a reliable sense of sociotechnical trust, which stems from an agreement between the actor's models and the actor's trust of the architecture of the system (Paja et al., 2013, p. 342). This means that each of these actors/components of the model have to work equally, without one component drawing too much of the development responsibility. The weight and function of each of these actors can be seen in Figure 3, demonstrating how each component influences the other.

The social context for the usage of the sociotechnical model seen in figure 3 on page 8 is demonstrated through Actor-Network Theory (ANT), which can be seen below in figure 4 on page 10. Actor-Network Theory provides a larger context for the development of complex technical systems and their corresponding interactions with humans and society (Crawford, 2020). Further emphasizing the usefulness of the sociotechnical model, ANT highlights the complexity of the larger working system associated with LAWS. This framework conceptualizes the mutual shaping that occurs between the different actors within the network. In terms of LAWS, figure 4 on the following page provides a visualization of the four larger societal aspects that play a role in the network (seen in orange) in addition to the various networks within each larger actor (seen in light blue, green, and red). These four broad actors within the network are: the users, designers, policymakers and industry development. Within these actors there are interconnected networks that influence each other, which can be seen through examples of

engineers who not only make up the primary designers of LAWS, but also push innovation in Machine Learning which influences the development of that field. Each of these factors directly influence not only the development of autonomous combat but each other, demonstrating that there is "no longer separation between science and society, as various social actors can influence the course of science and technology" (Crawford, 2020). The development of models such as ANT and the sociotechnical model provide a basis for the development of legislation in order to regulate and provide a scope for the usage of LAWS.

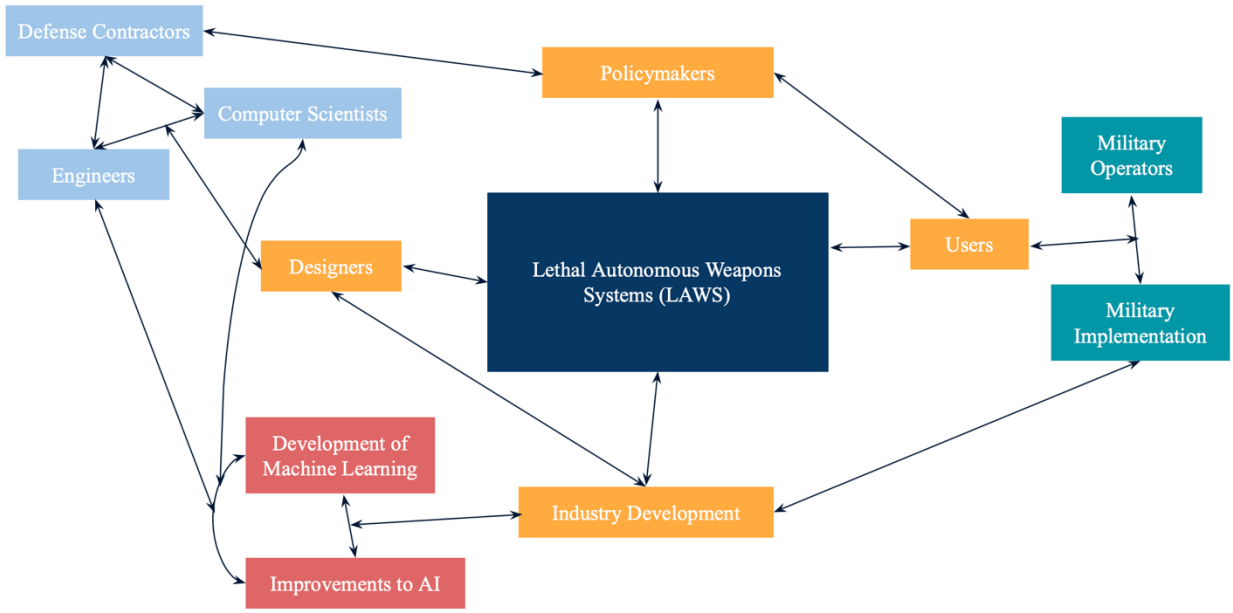

Figure 4: Autonomous Weapons Actor-Network Theory Model. The social context of autonomous weapon systems is provided through the lens of an interconnected web through various actors ranging from human to technical (Price, 2022).

INTEGRATION OF THE TECHNICAL AND STS PROJECTS

The goal of this research into the implications of introducing autonomous technology into warfare is to curb the potential negative consequences of using this technology that result from system malfunction and user misuse. Through acknowledging the potential ethical conflicts that

arise from this technology, there is an opportunity to develop alternative pathways of innovation in order to avoid these negative consequences. This STS research will be conducted in the form of a scholarly article outlining the potential ethical pitfalls of LAWS in an attempt to prevent any large-scale harm that can result as a consequence of this technology.

This STS topic will focus on the ethics behind the developments of warfare technology, or more specifically, autonomous combat technology. This topic is closely related to the technical topic which studies and creates an embedded system that is used for target location. The STS topic will primarily focus on the implications of recent advancements in autonomous technology while the technical topic will focus on studying and producing such technologies. The development of the technical topic will aid in encouraging ethical decision making when it comes to armed combat by assisting the autonomous vehicle in correctly identifying targets in order to reduce casualties caused by target locating errors. In tandem, these two topics address the weaknesses in the current developments of autonomous combat technology while aiding in improving the technology itself.

REFERENCES

Ams, S. (n.d.). Blurred lines: The convergence of military and civilian uses of AI & data use and its impact on liberal democracy. *International Politics*. https://doi.org/10.1057/s41311-021-00351-y

Atesoglu, H. (2004). Defense spending and investment in the United States. *Journal of Post Keynesian Economics*, *27*(1), 163–169.

Brunette, E., Flemmer, R., & Flemmer, C. (2009). *A Review of Artificial Intelligence* (G. Gupta & S. Mukhopadhyay, Eds.; WOS:000269688000118; pp. 650–657).

Cao, Z. (2017). *Development and Application of Artificial Intelligence* (Z. You, Ed.; WOS:000426730000126; Vol. 70, pp. 701–704).

Crawford, T. Actor-Network Theory. Oxford Research Encyclopedia of Literature. https://oxfordre.com/literature/view/10.1093/acrefore/9780190201098.001.0001/acrefore-9780190201098-e-965.

Di Corpo, R. (2021). Autonomous Technology and the ethics of Non-Power. *Peace Review*, *33*(2), 256–262. https://doi.org/10.1080/10402659.2021.1998858

Fiott, D. (2018). America first, third offset second? *Rusi Journal*, *163*(4), 40–48. https://doi.org/10.1080/03071847.2018.1529893

Fiott, D. (2017). A revolution too far? US defence innovation, europe and NATO's military-technological gap. *JOURNAL OF STRATEGIC STUDIES*, *40*(3), 417–437. https://doi.org/10.1080/01402390.2016.1176565

G. Badakis, M. Koutsoubelias and S. Lalis, "Robust precision landing for autonomous drones combining vision-based and infrared sensors," 2021 IEEE Sensors Applications Symposium (SAS), 2021, pp. 1-6, doi: 10.1109/SAS51076.2021.9530091.

Hampshire, E. (2015). Margaret Thatcher's first U-turn: Francis Pym and the control of defence spending, 1979-81. *CONTEMPORARY BRITISH HISTORY*, *29*(3), 359–379. https://doi.org/10.1080/13619462.2014.974566

Hartmann, J., Jueptner, E., Matalonga, S., Riordan, J., & White, S. (2022). Artificial intelligence, autonomous drones and legal uncertainties. *European Journal of Risk Regulation,* 1-18.

Jaeger, K., & Bers, K.-H. (2001). image-based 3D scene analysis for navigation of autonomous airborne systems. *SPIE Proceedings*. https://doi.org/10.1117/12.444197

Kaghan, W., & Bowker, G. (2001). Out of machine age?: Complexity, sociotechnical systems and actor network theory. *Journal Of Engineering And Technology Management*, *18*(3–4), 253–269. https://doi.org/10.1016/S0923-4748(01)00037-6

Kollias, C., & Paleologou, S. (2015). Defence and non-defence spending in the USA: stimuli to economic growth? Comparative Findings From A Semiparametric Approach. *Bulletin Of Economic Research*, *67*(4), 359–370. https://doi.org/10.1111/boer.12011

Korb, L., & Evans, C. (2017). The third offset strategy: A misleading slogan. *Bulletin of the Atomic Scientists*, *73*(2), 92–95. https://doi.org/10.1080/00963402.2017.1288443

K. Zacharias and K. Schmitt, "Canada's policy approach to "killer robots" and the ethics of autonomous weapons systems," 2021 IEEE International Symposium on Technology and Society (ISTAS), 2021, pp. 1-4.

Melancon, A.-A. (2020). What's wrong with drones? automatization and target selection. *Robotics, Autonomous Systems and Contemporary International Security*, 111–131. https://doi.org/10.4324/9781003109150-6

Oosthuizen, R., & Pretorius, L. (2016). Assessing the Impact of New Technology on Complex Sociotechnical Systems. *South African Journal of Industrial Engineering*, *27*(2), 15–29. https://doi.org/10.7166/27-2-1144

Paja, E., Chopra, A. K., & Giorgini, P. (2013). Trust-based specification of sociotechnical systems. *Data & Knowledge Engineering*, *87*, 339–353. https://doi.org/10.1016/j.datak.2012.12.005

Pew Research Center. (2020, May 30). *Beyond distrust: How Americans view their government*. Pew Research Center - U.S. Politics & Policy. Retrieved from https://www.pewresearch.org/politics/2015/11/23/beyond-distrust-how-americans-view-their-government/

Pitrat, J. (1992). The symbiosis between artificial-intelligence and cognitive science. *Technique Et Science Informatiques*, *11*(2), 9–24.

Pohle, J., & Audenhove, L. V. (2017). Post-snowden internet policy: Between public outrage, resistance and policy change. *Media and Communication*, *5*(1), 1–6. https://doi.org/10.17645/mac.v5i1.932

Shi, Z., & Zheng, N. (2006). Progress and challenge of artificial intelligence. *Journal of Computer Science And Technology*, *21*(5), 810–822. https://doi.org/10.1007/s11390-006-0810-5

Smith, J., & Tuttle, M. (2008). Does defense spending really promote aggregate output in the united states? *Defense and Peace Economics*, *19*(6), 435–447. https://doi.org/10.1080/10242690701701950

Tarzie. (2017). Edward Snowden, Frenemy of the State. *American Journal of Economics and Sociology*, *76*(2), 348–380. https://doi.org/10.1111/ajes.12179

Wizner, B. (2017). What Changed After Snowden? A US Perspective. *International Journal of Communication*, *11*, 1–5.

Work, B. (n.d.). *Remarks by deputy secretary work on third offset strategy*. U.S. Department of Defense. Retrieved from https://www.defense.gov/News/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/

Wu, H. (2017). *Thinking about Artificial Intelligence* (L. Zhu & T. Zheng, Eds.; WOS:000414864800117; Vol. 138, pp. 627–630).