Fraud Fighters: Using Serverless Architecture and Next.js to Fight Fraud

Moral Frameworks for Integrating Autonomous Weapon Systems in the Military

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 Computer Science

By
Jeffrey Bukont

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

Kent Wayland, Department of Engineering and Society

Briana Morrison, Department of Computer Science

General Research Problem: The Morality of Adopting New Computing Technologies

What kinds of moral questions do early adopters of new technologies face?

Early adopters of new technologies can often reap the benefits of increased efficiency and decreased cost. An example of the benefits of early technological adoption can be seen at Capital One, where an early adoption of cloud computing led to decreased cost and increased development efficiency. The move to cloud computing was an easy decision because it was not morally questionable and increased efficiency by decreasing development time and increasing service uptime. However, other parts of society, like the military, face more difficult moral questions when considering adopting the latest computing technologies, particularly A.I.

The military has already begun integrating A.I am into many different systems for the obvious increases in capability it provides. However, these systems still require a human's input to function. Making semi-autonomous weapons systems fully autonomous could have a massive benefit by removing humans from combat zones and increasing the overall proficiency of the military. These benefits must also be balanced with the incredible dangers of autonomous weapon systems. My STS paper will delve into the different moral frameworks that groups use to argue against and for the integration of autonomous weapon systems into the military. Whereas my technical report will focus on my internship project at Capital One, where I used Serverless Architecture and Next.Js to increase the efficiency of testing fraud-fighting tools.

Fraud Fighters: Using Serverless Architecture and Next.js to Fight Fraud

Capital One manages fraud by creating flags on suspicious transactions; these flags are internally referred to as concerns. In their previous flagging system, if a concern needed to be

created manually, it required filling out a form with information from various sources. As summer interns, we were tasked with creating a system that would automatically import account and credit card information. This automatic importing would make creating manual concerns faster, which in turn would help with the development/testing of fraud-fighting applications. We decided to leverage AWS Lambda, S3, and Next.js to build and deploy a web application which integrated multiple APIs to gather account and credit card information.

We chose Next.js because our manager tasked us with using server-side rendering. Server-side rendering moves some of the burden of webpage rendering from a user's computer to a server. Server-side rendering helps to standardize performance across a wide range of devices which is optimal in a business environment. NextJS comes with this feature built-in through a function called Server-Side Props, so we thought it was an obvious choice.

We used a combination of AWS Lambda and S3 to avoid using EC2 servers because a serverless architecture (Lambda + S3) would increase uptime and decrease maintenance costs for our application. AWS lambda is a tool which allows code to be run on a server in response to a certain event happening. For example, if a user clicks the upload button on a webpage, then Lambda can run the code to upload the data to the database. However, crucially, Lambda is not a server since the owner doesn't have to worry about provisioning compute power or memory. Lambda runs your code on servers managed by AWS, and you are billed for how long and how often your code runs. This is great for web applications which will be used with varying frequency but require high levels of uptime to be useful. S3 is a storage service which allows users to store files in buckets. We used S3 to store the front end of our website in a bucket and made the bucket accessible by URL using another AWS service called route53. This meant when the user went to

the URL, the HTML files were rendered by the user's browser. When the user clicked on a button that required fetching new information Lambda would be notified and send back the relevant data.

Lastly, we integrated Capital One's account and credit card information fetching APIs using NodeJS. We finished our application but ran into problems with server-side rendering during deployment. We needed to use the Serverless Next.Js framework to deploy to AWS Lambda, but Capital One's pipeline had not approved the serverless framework, so we had to change to Client-Side Rendering. After switching to client-side rendering, our project worked very well, decreasing the time to create a concern by over 90%. Our manager even said our intern project would be built upon by a full-time team after we left. Although we successfully developed and deployed our project, one aspect of our app that could have been improved was the process of adding new teams. Currently, if a new team wanted to use our application, it would require adding the team's account credentials to Capital One's password management system. The process of adding credentials manually takes a while compared to adding a built-in login system.

Moral Frameworks for Integrating Autonomous Weapon Systems in the Military

What Moral Principles are being used when considering integrating Autonomous Weapon Systems into the Military?

My STS paper will analyze what moral principles are being used to justify whether Autonomous weapons should be integrated into the military. This is important because by agreeing to a set of moral principles, we can lay out rules for the development, testing, and deployment of autonomous weapons. In addition, we can seek to encourage these rules globally and work to call out nations that don't follow them. If we don't analyze and agree on moral

principles ahead of time, we could end up in an A.I arms race with weapons that could cause unneeded suffering on purpose or even simply because of poorly trained models.

Background

Artificial Intelligence is a massively growing field, particularly in the military (Morgan et al., 2020). Currently, most systems are limited to enhancing human capability and decision-making; however, as A.I systems improve, it becomes feasible to implement autonomous decision making. In fact, Israel has already developed the mini harpy, a loitering drone that can act fully autonomously (HARPY Autonomous Weapon for All Weather). This technology brings the frightening prospect of autonomous robots making combat choices without human supervision. This prospect brings up many ethical questions both from the perspective of researchers, the military, and the public.

Literature Review

The arguments against allowing autonomous weapon systems into the military can be broken into three separate categories human dignity and control, international law, and international stability (Sharkey, 2018). The first category of argument is based on the idea that only humans have enough control to make the decision to kill another human being and that robots killing humans would lack dignity. For example, Korać (2018) argues that autonomous weapon systems will lead to a depersonalization of killing since only human conciseness can reason between right and wrong.

The second category of argument used against integrating autonomous weapon systems into the military is that they are against International Humanitarian Laws (IHL). An example of this is in the paper by Garcia (2018), where he states that autonomous weapon systems might be

against Article 36 of the 1977 Additional Protocol to the Geneva Conventions. Additionally, even if they are allowed under IHL, they disrupt the current enforcement mechanisms. This is because a precedent hasn't been set for who would be prosecuted if an A.I weapon system committed a war crime. Would it be the soldier, commander, manufacturer, or leader of the country? Garcia's follow-up argument is that autonomous weapon systems threaten international peace and stability. This is the third category of arguments against autonomous weapon systems. This category of arguments states that even if an autonomous weapon system was moral and followed the laws, the ability to wage war without risking human life would result in more conflict outweighing any benefits of autonomous weapon systems.

The main category of argument for autonomous weapon systems is that they will reduce the risk of soldiers dying in combat and can perform better than soldiers (Horowitz, 2016). For example, (Arkin, 2009), the argument is made that soldiers often commit war crimes out of emotion that AI won't be vulnerable to. Additionally, when combat roles are replaced with autonomous weapon systems, soldiers don't have to risk their lives in combat.

Gathering Evidence

To gather evidence, I have found several research papers that are for and against integrating autonomous weapon systems into the military. I will analyze and categorize their arguments and compare their arguments to existing moral frameworks like the IHL around weapons. In addition, I will analyze how A.I am currently already integrated into the military using the congressional research service 2022 report and RAND's "Military Applications of A.I." to see what moral framework the military is currently using. Finally, I have found studies on the public sentiment of A.I based weaponry which I can compare to the moral frameworks of the research papers and the current military implementation.

Conclusion

In conclusion, my technical report focuses on my time as an intern at Capital One, where technologies were used to increase the efficiency of testing fraud-fighting applications. The implementation of these technologies is a no-brainer for Capital One since there are minimal ethical concerns with implementing cloud computing into a fintech company. However, my STS paper will focus on the moral and ethical questions around implementing A.I am into weaponry, particularly fully autonomous systems. I use various papers and polling to analyze the different moral frameworks around autonomous weapons both from the perspective of researchers, the public, and the military.

References

Arkin, R. (2009). *Governing lethal behavior in Autonomous Robots*. Chapman and Hall/CRC. https://doi.org/10.1201/9781420085952

Garcia, D. (2018). Lethal Artificial Intelligence and Change: The future of international peace and security. *International Studies Review*, *20*(2), 334–341. https://doi.org/10.1093/isr/viy029

HARPY Autonomous Weapon for All Weather. Iai.co.il. (n.d.). Retrieved December 12, 2022, from https://www.iai.co.il/p/harpy

Horowitz, M. C. (2016). The Ethics & Morality of Robotic Warfare: Assessing the debate over Autonomous Weapons. *Daedalus*, *145*(4), 25–36. https://doi.org/10.1162/daed_a_00409

Korac, S. (2018). Depersonalization of killing: Towards a 21st-century use of force "Beyond good and evil?" *Filozofija i Drustvo*, *29*(1), 49–64. https://doi.org/10.2298/fid1801049k

Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). *Military applications of Artificial Intelligence: Ethical concerns in an uncertain world* (Report RR-3139-1-AF). RAND. https://doi.org/10.7249/rr3139-1

Sharkey, A. (2018). Autonomous Weapons Systems, Killer Robots and human dignity. *Ethics and Information Technology*, *21*(2), 75–87. https://doi.org/10.1007/s10676-018-9494-0