The Military Tech Complex and Cyberwarfare: Ethical and Anticipated Ethical Issues

Richard L Wilson[1] and Noah Donnelly[2]
[1]Department of Philosophy/Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA
[2]Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA

wilson@towson.edu
ndonnel1@students.towson.edu

Abstract: In this analysis we examine how the military-industrial complex has now been expanded into the digital realm, forming what's often called the *military-digital complex* (MDC). The ecosystem of MDC links defense contractors, governments, and Big Tech companies to the development and deployment of cyberwarfare capabilities. The capabilities of the MDC are of information technology weapons that are of both an offensive and defensive nature. How does the Military Tech Complex Connect to Cyberwarfare? The development of the MDC has led to the Militarization of cyberspace. Governments and militaries treat cyberspace as a battlefield. The U.S. created *Cyber Command* to oversee offensive and defensive cyber operations, including hacking, digital espionage, and electronic warfare. Partnerships with Big Tech Companies like Microsoft, Google, Amazon, and Apple provide cloud infrastructure, AI tools, and cybersecurity expertise. These partnerships blur the line between civilian use of technology and military applications. Defense contractors and startups Traditional defense firms (Lockheed Martin, Raytheon) now invest heavily in cyber tools, while Silicon Valley startups receive Pentagon funding to innovate in specific areas like AI-driven cyber defense. When the intentions of rational agents within government and corporations are connected to duties, conflicts arise with government having duties to civilians and corporates having duties to investors. This conflict of duties is what is focused on in our discussion which relates to how intentions and duties are linked in deontological ethics. This analysis begins by examining technical issues including the Cloud as a Battlefield, the "Kill Chain" and Algorithmic Warfare and The Zero-Day Economy and VEP. The analysis continues with a discussion of ethical issues related to The Principle of Distinction (Just War Theory), The troublesome Incentive of the "Cyber-Industrial Complex," and Accountability and Epistemic Opacity. Three case studies are then presented that give examples of the technical and ethical issues presented in the earlier parts of our analysis. This is followed by an anticipatory ethical of potential future developments and four recommendations are then made related to the concepts previously discussed and the case studies we have examined before we conclude we propose the following four reforms to help overcome how the MDC government and corporate partnerships act in collusion to intentionally blur the line between civilian use of technology. This original research and analysis is concerned with how Big Tech companies profit from cyber warfare contracts and how nation-states weaponize AI in cyber conflicts and finally with the ethical and anticipated ethical issues that arise because of these developments.

Keywords: Military-digital complex, Cyber warfare, Project Maven, JEDI/JWCC, NSO Group, Zero-Day Exploits, Anticipatory Ethics, Sociotechnical imperative, Dual-use technology, Vulnerability equities process

1. Introduction

At the end of his presidency, in 1961, President Dwight D. Eisenhower gave his final address to the nation. Within his final address Eisenhower issued a prescient warning: "In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex" (Eisenhower, 1961). Eisenhower was worried that the nation, due to the power of democratic representatives being eroded by their debts owed to the companies that funded their campaigns. Eisenhower was more specifically talking about military contractors. Sixty-five years later, the military-industrial complex has further evolved into the military digital complex. The focus of the defense industry is no longer confined to just manufacturing steel and ballistics; it has transformed into developing code and synthesizing data. This is the basis of the Military-Digital Complex (MDC).

The MDC can be described as the symbiotic relationship between national defense agencies (the Pentagon and US Cyber Command), and traditional defense contractors (Northrop Grumman, Lockheed Martin), and "Big Tech" companies (Google, Microsoft, Amazon, Oracle). During the cold war, the government was the primary innovator, DARPA created the internet and (ARPANET) and GPS. That dynamic has changed in the era of information. The private sector is innovating at a speed which the government could never keep up with. The military is now reliant on "Commercial Off-The-Shelf" (COTS) technology to operate and conduct warfare (O'Mara, 2019).

This shift to the MDC with it dangerous and unignorable implications. American tech companies develop their products on commercial infrastructure, the same infrastructure that previously was used for streaming, now

hosts the command-and-control systems for drone warfare. Similarly operating systems that are used in hospitals now also power missile defense technologies. This paper argues that integrating Big Tech into the military "kill chain" fundamentally blurs the formerly clear distinction between civilian and combat infrastructures. This integrates a convergence of technologies into what is known as a "hyperscale" vulnerability, which violates the Sociotechnical Imperative and Just War Theory principles. We claim that economic incentives of the MDC create a perpetual loop of cyber insecurity, where the private sector profits from both the development of weapons systems, and the development of systems that defend against those same weapons.

2. Technical Issues

The development of the MDC creates a multitude of ethical risks, but to understand ethical risks, the technical structure of the MDC and the issues related to its architecture must first be understood. Three distinct technologies that are employed by designers as central to the development of MDC are: Cloud Computing, Algorithmic Warfare (AI), and the Zero-Day Exploit market. We assume Bratman's BDI (belief-desire-intention) model as providing a framework for identifying the beliefs-desires-intentions of designers of technology.

2.1 The Cloud as a Battlefield (JEDI & JWCC)

As of 2022, the US military was only processing 2% of the data it acquired (Aranke, 2022), the modern military needs the capability of processing exabytes of data in real time. To meet this requirement, the United States Department of Defense (DoD) intentionally initiated the Joint Enterprise Defense Infrastructure (JEDI), which became the Joint Warfighting Cloud Capability (JWCC) (D3V Tech, 2020; FedBiz Access, 2020). The JWCC is a multi-billion dollar project to move the DoD's computing and data storage infrastructure from closed and secure servers that exist in the premises to commercial cloud computing servers that are provided by companies like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Oracle (Oracle, n.d.). This consolidation in the cloud creates for adversaries a singular, centralized target. Aggregating military logic onto commercial platforms creates a potentially dangerous Single Point of Failure. If an adversarial state actor were to successfully disrupt AWS or Azure servers to hurt the US economy, they may also unintentionally or intentionally hurt the US militaries abilities to operate to its fullest extent. This is in effect like placing a military base in a residential neighborhood, aligning military targets with civilians (Conger & Sanger, 2019).

2.2 The "Kill Chain" and Algorithmic Warfare

The second technical issue created by the MDC is the automation of the "Kill Chain," which is the process of identifying a target and engaging it (EBSCO, 2024). The kill chain employs Computer Vision and Machine Learning (ML). Machine Learning is the focus of AI algorithms that are learned from training data and neural networks (IBM, n.d.) instead of being explicitly programmed. Computer Vision is a subset of AI that allows machines to process visual inputs like images and videos, it uses ML to help computers process meaningful information from visual data (IBM, n.d.). The old version of the kill chain operated with a "Human-in-the-loop" (where a human makes the final decision to fire), which is now shifting to a "Human-on-the-loop" (where a human supervises an autonomous system) (Scharre, 2018). These AI systems are opaque, which means that the system is intentionally designed to act with the systems operating as a so called "Black Box." The designers of neural networks are unable to explain why they identified a target; they merely identify one. These AI systems are also brittle, adversarial machine learning attacks would be able to fool these systems by visually crafting "noise" which leads to targeting errors (Pasquale, 2015).

2.3 The Zero-Day Economy and VEP

Software bugs form the third pillar of the intentional weaponizing these dual use systems. A "Zero-Day" is a software vulnerability that is unknown to the vendor or public. This is an issue because, normal bugs can be patched and the issues are solved, but zero-day vulnerabilities which have been identified, leave "zero days" for a fix to be made, so they can be used to hack any system running that software. These exploits lead to a gray market of sorts. Hackers find the exploits, and brokers (like Zerodium) sell them to governments for millions of dollars. The US government is intentionally stockpiling weapons for offensive use as opposed to reporting the bugs and having them patched (Perlroth, 2021). The U.S. governments protocol for this is called Vulnerability Equities Process (VEP). The VEP is how the government decides what vulnerabilities should be disclosed and what should be kept secret (White House, 2017). Critics of the VEP argue that it is biased towards "No-Bus" (Nobody but Us), which means the government intentionally leaves insecurities in civilian infrastructure so the NSA can use these vulnerabilities when necessary to hack adversaries (Caulfield, 2018).

What is common to these three technical issues is how in the MDC government and corporate partnerships act in collusion to intentionally blur the line between civilian use of technology and military applications.

3. Ethical Issues

The technical architecture of the MDC introduces several ethical issues, particularly regarding the laws of war and how they relate to corporate responsibility. To understand these ethical issues, we introduce distinctions developed by Furrow. As Furrow states, ethics is related to evaluating actions, and actions are performed by those capable of being moral agents. As Furrow says, “When we evaluate an action, we can focus on various dimensions of the action. We can evaluate the person who is acting, the intention or motive of the person acting, the nature of the act itself, or the consequences.” (Furrow, 2005) A moral agent can justify their intentions, actions and outcomes produced by actions by referring to ethical principles. The themes discussed below revolve around how in MDC the laws of war are related to corporate responsibility and how they are intentionally conjoined.

3.1 The Principle of Distinction (Just War Theory)

In the realm of International Humanitarian Law, the Principle of Distinction in just war theory is incredibly important, it mandates that belligerent nations in armed conflicts must distinguish between military and civilian targets, at all times, with no exceptions (ICRC, n.d.). The MDC intentionally designs and creates what is known as a “Dual-Use” infrastructure, systems or items are used by both the civilian population and the military. If Microsoft provides the “War Cloud,” military data stored in part of the Microsoft cloud, its data centers now become military assets. The ethical problem arises when those military assets are stored right next to civilian data such as when patient records belonging to a hospital and the financial data for the banking system are stored next to military data. In kinetic warfare, bombing a hospital is a war crime, but if the military is using that hospital for military operations, it loses its protected status. Since these same servers are being used for civilian infrastructure, the internet, as we know it, loses its protected status. The MDC makes it impossible to target the military without producing an outcome that causes "Cyber Collateral Damage" (Schmitt, 2017).

3.2 The Troublesome Incentive of the "Cyber-Industrial Complex"

Private and public companies are first and foremost concerned with maximizing shareholder value, which is a fiduciary responsibility companies have to their investors. For a weapons manufacturer, peace is never as profitable as war. Conflict between the government’s best interest and intentions and the defense contractor’s best interest lies exactly between these two arenas, peace and war. Defense contractors and cybersecurity firms profit from the insecurity created by global conflicts to create profit, they don’t intend to participate, they want to sell and profit from both offensive and defensive weapons. The more dangerous a digital cyber landscape is (ransomware, state-sponsored hacking), the more demand there is for their products (Singer & Brooking, 2018). This is the digital equivalent of the Cold War arms race. Tech companies intentionally sell the offensive cyber capabilities to governments in forms like zero-day exploits and then turn around and intentionally sell defensive capabilities like threat intelligence and patches to the victims of cyber-attacks. This effectively makes cyber warfare a commodity for these companies, and cyber conflict within the MTC incentivizes the continuation of cyber risks as opposed to their resolutions (Deibert, 2020).

3.3 Accountability and Epistemic Opacity

Normal military operations have a form of accountability that follows the chain-of-command model, where responsibility lays with the commanding officer, the person who gave the orders. This chain of command is impossible when algorithms driving these cyber operations are proprietary and owned by private companies. For example, if an AI falsely flags a civilian as an enemy combatant and then causes civilian casualties, accountability becomes obscured. Instead of a commanding officer being held responsible, the military can claim it was a glitch, the vendor can then claim that the software is a protected trade secret which avoids auditing, therefore no one can be held accountable. The epistemic opacity of AI is related to who should be held responsible for civilian casualties. This "Black Box" of AI argument prevents democratic oversight of lethal force (Pasquale, 2015).

What is common to these 3 ethical issues is how the MDC government and corporate partnerships act in collusion to intentionally blur the line between civilian use of technology and military applications. When intentions are connected to duties conflicts arise with government having duties to civilians and corporates having duties to investors.

4. Case Studies

The following case studies illustrate how due to ethical issues related to intentions, MTC and the MDC function in specific circumstances, and how the functions of these entities conflict with governmental issues such as national security and corporate issues related to profit.

4.1 Project Maven (2018)

In 2018 Google entered a contract with the pentagon called Project Maven. The idea behind Project Maven was to use Google's AI called TensorFlow to analyze drone footage with the intentional goal of improving their targeting. This decision resulted in the employees revolting. Over 4,000 of Google's employees signed a petition that stated, "Google should not be in the business of war." Google's motto at that time was "Don't be evil." The employees argued that performing this contract and integrating consumer AI into the militaries kill chain was a violation of Google's motto (Shane & Wakabayashi, 2018; Suchman et al., 2018). Google ultimately decided that they should not renew the contract. Google later went on to release "AI Principles" that intentionally left subtle loopholes for working with the military (IT Pro, 2018). This case is a demonstration of tech employees exercising "Moral Agency" (Ahlstrom-Vij, 2013). This would involve assessing the intentions, actions and outcomes related to a company's policies. Contrary to traditional defense company workers, tech employees see themselves as civilians working for the betterment of humanity, rather than working for the military part of the state. The eventual replacement of Google by the government with vendors like Amazon and Microsoft shows that MDC is resilient even when individual companies protest.

4.2 SolarWinds (2020)

Russian intelligence (SVR) compromised the software build system of SolarWinds, a private company that manages IT. What was supposed to be a routine surface update, became a major cyber security event when SolarWinds inadvertently installed a backdoor called SUNBURST. Both the U.S. government and the military relied on SolarWinds, and through this backdoor the hackers were able to gain access to the Pentagon, the Department of Homeland Security, and the Treasury (FireEye, 2020). This is a clear demonstration of how "Outsourcing Defense" can be a fragile exercise. The U.S. government's security was only as strong as that of a private companies update server. In the MDC, the Solar Winds case demonstrates that "Attack Surface" of the nation includes every private vendor in the supply chain that it relies on (Zetter, 2021). The goal must include closing loopholes in the attack surface of supply chain vendors.

4.3 NSO Group: Pegasus

The NSO group is a private Israeli firm, most notorious for developing Pegasus, which is a "zero-click" spyware capable of infecting iPhones without the user even touching the device. The NSO group acted as a digital black-market arms dealer, intentionally selling Pegasus to governments without concern for how Pegasus would be used. Later investigations revealed that countries like Saudi Arabia and Mexico used this software for more than counterterrorism purposes. Pegasus was used against human rights activists, journalists and political dissidents (Amnesty International, 2021; Council of Europe, 2021). This case demonstrates how the barrier of entry for cyber warfare has been lowered. In previous years, only powers like the US (NSA) or Russia (GRU) had that powerful of a tool. The MDC allowed for the sale of "NSA-level" technology to any regime willing to pay. This privatization of zero-day spyware intentionally bypassed the terms of traditional arms control treaties (Perlroth, 2021).

4.4 FoxBlade (2022)

In February of 2022, mere hours before Russian armor pushed into Ukraine, Russian cyber units deployed a piece of malware called FoxBlade (Redmond Mag, 2022) which was intended to destroy Ukrainian government networks. As soon as this occurred, the Microsoft Threat Intelligence Center (MSTIC) detected the anomaly and patched it. Microsoft is the main cloud source provider for the Ukrainia government (Microsoft then established a secure line to Kyiv to deploy the defenses they developed, which stopped what was in effect a cyber-invasion of Ukraine by Russia (Smith, 2022). What was essentially a cyber version of the iron dome, developed and deployed by a U.S. corporation, was unilaterally decided upon by Microsoft alone for intervening in a foreign war. While this was beneficial for Ukraine, it raises concerns of Digital Sovereignty. If Microsoft defends a nation involved in a war, could Microsoft then be interpreted as being a belligerent in that war? This signifies a shift of power from nation states to the "Techno-State" (Lucas, 2017).

What links the preceding case studies is the way in which governments and corporate entities have intentionally unified and become intertwined. Given the ways in which MDC works with Governments and corporate entities working together it is important see the future outcomes that can come about due to this intertwining.

5. Anticipatory Ethics

Anticipatory Ethics is a future oriented ethical framework that studies potential ethical issues that arise from new and emerging technologies before they are fully integrated into society. As defined by Phillip Brey, Anticipatory Technology Ethics (ATE) requires that we move beyond reactive judgements about the effects of technologies after an event has occurred to a proactive forecasting of the dangers that these technologies pose. This section analyzes the failure of corporations to apply basic Anticipatory Ethical principles to analyze to the Military Tech Complex and Cyberwarfare. Applying the "Moral Responsibility for Computing Artifacts" framework by Miller et al. (2011) allows us to foresee and map the ethical obligations of the MDC (Brey, 2012). The preceding cases show how technological developments with the MDC have led to a series of ethical issues.

5.1 Rule 1: The Foreseeability of Effect

Rule one of Moral Responsibility for Computing Artifacts states that "The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact" (Miller et al., 2011). It is foreseeable that the stockpiling of Zero-Day exploits (like the *EternalBlue* exploit kept by the NSA) can lead to zero-day exploits being stolen and weaponized against their civilian population. This is evident in the WannaCry ransomware attack (Cloudflare, n.d.). The government and their contractors did not consider the possible blowback of these being discovered. By prioritizing offensive capabilities over the defensive architecture of their nation, they bear the moral responsibility for any collateral damage caused by those tools leaking.

5.2 Rule 4: The Sociotechnical Imperative

Rule four says that the "People who design... can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded" (Miller et al., 2011). AI tools that have been developed by big corporations were designed for an environment of commercial use, they prioritize efficiency, ad targeting and logistics. When these tools are embedded into the military sociotechnical system of kinetic warfare without redesigning the underlying technology, it violates the sociotechnical imperative. Consumer-grade code is not nearly up to military standards, so using it for nuclear command and control could have devastating consequences, including enemies gaining access to the second largest nuclear arsenal in the world. Tech corporations that fail to rework their software from the security required for civilian use, to the level of security required for military use put the entire internet ecosystem at risk.

5.3 Rule 2 and 3: The Issue of Epistemic Paternalism

The rise of the MDC has introduced a new dilemma about who controls the battlefield, is it the state? Or is it the software designer? This conflict should be analyzed through Rule two and three of the "Moral Responsibility for Computing Artifacts" framework. Rule 2 states that "The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact... This responsibility includes being answerable for the behaviors of the artifact." (Miller et al., 2011). Private companies like Microsoft and SpaceX have deployed technological artifacts like cloud infrastructure and satellite internet that are now widely used and relied upon for modern warfare. Adhering to rule 2, these companies cannot claim to be neutral parties. When Microsoft detected FoxBlade infecting Ukrainian networks, their decision to intervene was them exercising moral responsibility over their artifact and subsequently siding with Ukraine. This creates an issue involving Epistemic Paternalism, where a private company decides which nation's cyber systems are worthy of being defended by an intervention. By accepting the JWCC contract, big tech corporations have effectively become a geopolitical player. Geopolitical players in the western world typically require a democratic mandate, tech companies do not have one. The responsibility for your technological artifact does not stop at moral responsibility, but also carries the responsibility defined by Rule 3: "The people who design... computing artifacts have a moral responsibility to retract or recall those artifacts if they are found to cause harm that cannot be mitigated." Rule 3 is directly applicable to the NSO Group. It became clear after some time that the Pegasus spyware was being used to target journalists and activists, who are typically protected as civilians, which is a completely foreseeable effect of selling cutting edge spyware to authoritarian regimes. The NSO group under Rule 3 had a moral duty to recall the weapon. Recalling a software weapon can be done through revoking the user's license. They failed to do this and subsequently relinquished moral responsibility by claiming "client

sovereignty," which is a direct violation of the principles of Anticipatory Ethics as stated above. The NSO Group refused to acknowledge that they still bore moral responsibility after the deployment of their artifact.

What links the preceding the concepts in the cases analyzed above is the way in which governments and corporate entities have intentionally unified and become intertwined. Given the ways in which MDC works with governments and corporate entities working together it is important to examine the potential future outcomes that can come about due to this intertwining.

6. Recommendations

An analysis of the preceding 4 cases and the ethical problems arising from them culminating in an anticipatory ethical analysis of the MDC reveals an ecosystem where the economic incentives favor cyber insecurity and technical architectures that favor obscurity, while also not allowing for proper accountability. Since we cannot revert to a pre-internet era, we must design a regulatory and technical framework that would reclaim the distinction between the civilian and military worlds. Based upon our ethical analysis we propose the following four reforms to help overcome how the MDC government and corporate partnerships act in collusion to intentionally blur the line between civilian use of technology.

6.1 Sovereign Cloud

To restore the principle of distinction (between military and civilian actors), the mixed-use infrastructure that is created by the JWCC and JEDI, which allows military data to reside in the same logical regions as civilian commercial data, must be reworked. The principle of distinction would require the Department of Defense to enforce a "Sovereign Cloud" mandate. This requires a physical and logical air gap between military and civilian digital infrastructure. Cloud providers currently offer "GovCloud" regions, which technically are logically separated, but they often share the same hardware resources such as power and backbone fiber. The Sovereign cloud would require Hardware Isolation and Spectrum Separation. Hardware Isolation would be the act of making military data centers physically distinct from civilian ones. They must use different power grids and cooling systems to ensure that a kinetic or cyber-attack on the military servers would not cause cascading failures that extend to the civilian domain. Current military communications use the same 5G and satellite networks that the commercial network does, this is where Spectrum Separation comes into play. This mandate would require that dedicated, encrypted military spectrums be created and separate from consumer-grade routing protocols like BGP which are notoriously vulnerable to hacks. This recommendation restores the Principle of Distinction. The segregation of military and civilian infrastructure reduces the risk of collateral damage. If a belligerent nation e.g. attacks a US military server, it should not degrade the ability of hospitals accessing patient records from the same provider (Schmitt, 2017).

6.2 Reforming the Vulnerability Equities Process (VEP)

The current Vulnerability Equities Process (VEP) creates a moral hazard because of governments stockpiling Zero-Day exploits for offensive operations, which potentially leaves their own civilian infrastructure vulnerable. We propose a move from "No-Bus" (Nobody but Us) doctrine to one of defense primacy. This would legally require software vulnerabilities to be disclosed to the vendors within an absolute timeline. The first change would be a 90-day statute. This is modeled after Google's Project Zero disclosure policy; the US Cyber Command would be legally obliged to disclose and purchase or report found zero-day vulnerability to the relevant vendor within 90 days. This would allow for a small strategic window for high-value intelligence operations but would also prevent indefinite hoarding of exploits that can lead to global instability. The second implementation would be cyber market intervention. The government is currently distorting the market by paying high prices for exploits. This reform would reverse this tendency by redirecting those funds to pay bounties, this would grant researchers premium rates to patch bugs as opposed to exploiting them. This would create incentives for online mercenary blue teams as opposed to the current red teams (Caulfield, 2018). This applies Rule 1 of Anticipatory Ethics. It is foreseeable that stockpiled software can be leaked, by prioritizing patching over hoarding, the government fulfills its social contract to protect their citizens' digital infrastructure.

6.3 Algorithmic Accountability

The current proprietary nature of AI algorithms creates a "Black Box" where accountability is approaches impossibility. The DOD should reject the trade secret defense in the development of lethal autonomous weapons systems (LAWS). We propose a "Glass Box" Standard for all military AI contracts. There are three technical implementations that can solve this: Introspection API's, Model Cards and Provenance, and Adversarial testing. Introspection APIs (Application Programming Interfaces) would be applied to all AI models deployed in combat

zones. These would simply allow independent military auditors to query the model and understand why it made a classification decision (e.g., why is this classified as a tank and not a car). Borrowing from Google's ethical AI research, every military algorithm must have a "Model Card" that details the training data, biases, and limitations of its model. Cryptographic Provenance must also be used to sign the code, ensuring no supply chain attacks like SolarWinds have altered algorithms before deployment on the battlefield. Finally, adversarial testing would require that before deployment, algorithms must undergo a "Red Teaming" process to probe for vulnerabilities against adversarial examples (e.g., placing a sticker on a stop sign to fool a computer vision system). These technical implementations would address the issues of Epistemic Opacity and uphold the Sociotechnical Imperative. By requiring explainability, it is ensured that the "Human-on-the-loop" has meaningful control over the AI system. Without this, the humans are simply those who "rubber stamp" a machines decision, which removes their moral agency (Pasquale, 2015; Miller et al., 2011).

6.4 Digital Geneva Convention and Attribution Council

Cyberwarfare is currently defined ambiguously in the eyes of international law. In 2017 Microsoft proposed to the international community the establishment of a Digital Geneva Convention. Unfortunately, such a treaty is useless without enforcement. Therefore, we propose the creation of an International Cyber Attribution Council (ICAC). The convention needs to explicitly define the internet's backbone neutral territory. This neutral territory would include DNS Root Servers, SWIFT financial clearinghouses, electoral systems, and healthcare networks. Attacks on these systems would be war crimes regardless of intent. The ICAC serves as a replacement for biased attributors which originate from intelligence agencies like NSA or GCHQ that carry a bias towards their government, or private companies like Microsoft and Mandiant which are profit driven. The ICAC would be impartial and independent modeled after the International Atomic Energy Agency (IAEA), which is comprised of technical experts from neutral party nations. Their sole purpose would be to investigate and publicly attribute attacks to groups or nations supported by verifiable evidence (Taddeo & Floridi, 2018).

7. Conclusion

Future work should include and expansion of this analysis to cover the domain of "Hyper-War" and "Agentic AI." These factors will contribute to a domain where speed of conflict may require removing human oversight entirely, which raises questions about the morality of the math in the algorithms (Scharre, 2018). Additionally, research is needed into the privatization of space involving corporations like Starlink and how the neutrality of corporations interacts with state sovereignty during kinetic conflicts (Mac & Chang, 2023). The transformation of the Military-Industrial Complex into what has become the Military-Digital Complex (MDC) represents a shift in how to enact national security. The combination of Silicon Valley's speed and innovation with the lethality and resources of the Pentagon, means the United States has created the most powerful war machine to ever exist. This merger has come about with a high ethical price tag. It has eliminated the principle of distinction by creating a "Dual-Use" infrastructure where hospitals and missile systems use the same cloud. It has incentivized the stockpiling of software vulnerabilities instead of patching them. And it has introduced Epistemic Paternalism, where shareholders, not elected officials, determine the rules of engagement. This paper argues that these consequences are not unavoidable, they are not guaranteed by technical progress but are choices have been made by prioritizing efficiency over ethics. The reliance on software stockpiles and obscure algorithms has created a fragile environment where the tools of war are a few lines of malware away from being used for common cyber-crime. To correct the current course, we must reject the normalization of the MDC's current architecture. We need to implement a "Sovereign Cloud" that respect civilian-military boundaries. We must have a "Defense Primacy" mindset that prioritizes patches holes over exploiting vulnerabilities in software. And we must require a "Glass Box" accountability for the algorithms to which we delegate lethal force. A nation's defense must not come at the cost of the internet's integrity. We must construct a firewall between the civilian and military digital targets and ensure that the digital future is defined by a resilience of our shared sociotechnical systems, and not the cyber forever war. By implementing these recommendations, we can begin to alter and overcome the atmosphere the MDC creates where government and corporate partnerships act in collusion to intentionally blur the line between military and civilian uses of technology.

Ethics Declaration: No human participants or personally identifiable information were involved. All data sources were publicly available.

AI Tools Declaration: ChatGPT 5.1 for drafting and refinement. Human authors verified all content. Gemini 3.0 pro used for aiding in sourcing.

References

Ahlstrom-Vij, K. (2013). Epistemic paternalism. In H. LaFollette (Ed.), *International encyclopedia of ethics*. Wiley-Blackwell. https://doi.org/10.1002/9781444367072.wbiee294

Amnesty International. (2021). *Forensic methodology report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Aranake, S. (2022, April 25). Military lagging in data processing capabilities. *National Defense Magazine*. https://www.nationaldefensemagazine.org/articles/2022/4/25/progress-on-military-data-processing-capabilities-continue-to-lag

Bratman, Michael. (1999) Intention, Plans, and Practical Reason, Center for the Study of Language and Information.

Brey, P. A. E. (2012). Anticipatory ethics for emerging technologies. *NanoEthics*, 6(1), 1–13.

Caulfield, T. (2018). The U.S. vulnerabilities equities process: An economic perspective. *Lawfare*. https://www.tristancaulfield.com/papers/VEP.pdf

Cloudflare. (n.d.). *What is WannaCry ransomware?* https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Conger, K., & Sanger, D. E. (2019, October 25). Oracle and the Pentagon's cloud computing contract. *The New York Times*.

Council of Europe. (2021). *Pegasus spyware and its implications on human rights.* https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8

D3V Tech. (2020). Microsoft wins Pentagon's JEDI cloud contract (again). *D3V Tech Blog*. https://www.d3vtech.com/cloud-news/microsoft-wins-pentagons-jedi-cloud-contract-again-after-lengthy-battle/

Deibert, R. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi Press.

EBSCO Information Services. (2024). Kill chain. *Research Starters: Computer Science*. https://www.ebsco.com/research-starters/computer-science/kill-chain

Eisenhower, D. D. (1961, January 17). *President Dwight D. Eisenhower's farewell address*. National Archives. https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address

FedBiz Access. (2020). The Pentagon's $10 billion JEDI enterprise cloud saga explained. *FedBiz Access*. https://fedbizaccess.com/the-pentagons-10-billion-jedi-enterprise-cloud-saga-explained/

FireEye. (2020). *Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with SUNBURST backdoor*. FireEye Threat Research.

Furrow, Dwight. Ethics Key concepts in Philosophy, Continuum Press, 2005.

IBM. (n.d.-a). *What is computer vision?* IBM Think. https://www.ibm.com/think/topics/computer-vision

IBM. (n.d.-b). *What is machine learning?* IBM Think. https://www.ibm.com/think/topics/machine-learning

International Committee of the Red Cross (ICRC). (n.d.). *The principle of distinction*. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf

IT Pro. (2018). *Google publishes ethical code for AI following Project Maven fallout*. https://www.itpro.com/machine-learning/30891/google-publishes-ethical-code-for-ai-following-project-maven-fallout

Lucas, G. R. (2017). *Ethics and cyber warfare: The quest for responsible security in the age of digital warfare*. Oxford University Press.

Mac, R., & Chang, K. (2023, February 9). Elon Musk's refusal to provide Starlink support for Ukraine attack. *The New York Times*.

Microsoft. (2017). *A digital Geneva Convention to protect cyberspace*. Microsoft Policy Papers.

Miller, K. W., Wolf, M. J., & Grodzinsky, F. S. (2011). Moral responsibility for computing artifacts: 'The Rules'. *IT Professional*, 13(3), 57–59.

O'Mara, M. (2019). *The code: Silicon Valley and the remaking of America*. Penguin Press.

Oracle. (n.d.). *Joint Warfighting Cloud Capability (JWCC)*. https://www.oracle.com/defense-intelligence/jwcc/

Ostiller, Nate. (2023) Minister: Microsoft to provide free cloud services to Ukrainian government for another year. Minister: Microsoft to provide free cloud services to Ukrainian government for another year.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing.

Redmond Mag. (2022). *Microsoft IDs FoxBlade malware attack hours before Russia's invasion*. https://redmondmag.com/articles/2022/03/01/microsoft-ids-foxblade-malware.aspx

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Shane, S., & Wakabayashi, D. (2018, April 4). The business of war: Google employees protest work for the Pentagon. *The New York Times*.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan/Houghton Mifflin Harcourt.

Smith, B. (2022, June 22). Defending Ukraine: Early lessons from the cyber war. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Suchman, L., et al. (2018, May 16). Google's march to the business of war must be stopped. *The Guardian*. https://www.theguardian.com/commentisfree/2018/may/16/google-business-war-project-maven

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 558(7709), 296–298.

White House. (2017). *Vulnerabilities equities policy and process for the United States government*. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

Zetter, K. (2021, January 5). The SolarWinds hack is the most important hack of the decade. *The Intercept*.