Granite Journal

The University of Aberdeen Postgraduate Interdisciplinary Journal

Breaking the Boundaries: Interdisciplinary Research Approaches & Methods

Aquinas' Malware: How Old Theologies Can Shape the Ethical Use of New Weapons

Ian Clark (Department of Theological Ethics, University of Aberdeen)

Abstract: Emerging military technologies and weapon systems, such as cyber warfare, increasingly rely on the strategic use of deception for their effectiveness. While deception has long played a central role in armed conflict, ethicists and theologians have historically sought to distinguish between its just and unjust applications. While cyber weapons may represent a uniquely modern warfighting tool, this article argues that longstanding moral and theological frameworks, namely the just war tradition and the foundational thought of Saint Thomas Aquinas, remain well-suited for assessing the ethical character of deceptive military practices in the domain of cyberspace.

Keywords: Military Ethics, Deception, Cyber Warfare, Aquinas, Good Faith, Just War

1 Introduction

The Book of Joshua, the sixth book of the Hebrew Bible and the Christian Old Testament, recounts the fall of the city of Ai. In it, God speaks directly to Joshua (the leader of the Israelites) as he and his army prepare for their attack against the city. Joshua is instructed by the voice of the Lord to "set an ambush against the city" (Joshua 8:2). Joshua does as the Lord instructs by hiding a team of warriors on the outskirts of

Ai. Later, Joshua engaged Ai with his primary forces but feigned a retreat. When the defenders of Ai follow them, the ambush team "entered the city, took it, and at once set the city on fire" (Joshua 8:19). Then, when "Joshua and all Israel saw that the ambush had taken the city and that the smoke of the city was rising, then they turned back and struck down the men of Ai" (Joshua 8:21). The strategic victory of the Israelites was the result of an act of military stratagem and highlights the central role that deception has long played in warfighting. That the story is found within sacred scriptures is a reminder that military deception also has a moral dimension which is worthy of ethical and theological analysis.

The centrality of subterfuge within warfighting (both historical and modern) has long generated ethical debate around the moral limits of such deceptive tactics. After all, while deception may be necessary for battlefield success, it is also true that almost all moral theories and religious traditions restrict the act of intentionally misleading another party (Mattox, 2002:5). Today, this debate is especially relevant as new forms of weaponry – such as cyber weapons – become increasingly capable of generating real-world harm on a significant scale and can increasingly be effectively disguised. Indeed, many of these weapon systems rely on deception for their effectiveness and are intentionally designed with deception as a core attribute (Singer and Friedman, 2014:68-69).

Before progressing too far into an ethical treatment of deception in the context of cyber warfare, it will be helpful for me to address what is meant more broadly by 'cyber weapons' and 'cyber warfare.' Doing so is not easy, as varying degrees of harm can be generated through malicious uses of the internet. Not all of these harms can reasonably be understood to rise to the level of "warfare" or "violence." (Droege, 2012: 542). It is equally difficult, as the scholar George Lucas points out, to distinguish between criminal acts and acts of warfare in cyberspace (Lucas, 2017:1-15). Modifying slightly a definition of cyber warfare proposed by Lucas (Lucas, 2017:6), I will suggest the following working definition of cyber warfare for the purpose of this assessment: cyber warfare is a politically significant cyberattack(s) which causes, or has the potential to directly or indirectly cause, physical damage to people and objects in the real world. Cyber weapons, by contrast, are the means of executing such an attack and often take the form

of malicious software (malware) such as computer viruses, worms, and trojans. In other words, I propose that cyber weapons aim to achieve strategic military aims that historically would have required a soldier or conventional weapon system.

While cyber warfare and other emerging military technologies may be new additions to the history of warfare, this article will argue that longstanding moral and theological frameworks, namely the just war tradition (hereafter referenced as JWT) and the foundational thoughts of Saint Thomas Aquinas (1225-1274), remain well-suited for assessing the ethical character of deceptive practices in modern warfare. To achieve this, section two of this article will provide an overview of the JWT and Aquinas' views on deception in warfare. Section three will explore the distinction between just and unjust uses of deception in warfare, while section four will examine ethical challenges presented by warfighting in the domain of cyberspace. Finally, section five will propose two clear ethical standards militaries could use to ensure that deception in cyberspace is undertaken justly.

2 Aquinas, Just War, and Deception

An uneasy tension exists between New Testament precepts – which emphasise peace-making – and the reality of armed conflict. Even within the early Church, it is clear that many people of faith struggled to reconcile their beliefs with the task of warfighting (Clough and Stiltner, 2007:43). As Oliver O'Donovan notes in his work *The Just War Revisited*, Christian theology broadly agrees that peace is both the "original ontological truth of creation" as well as "the goal of history" (O'Donovan, 2003:2). However, our world – existing as it does between the peace of creation and the peace of an eschatological future – is often characterised by injustice and conflict, both of which are realities that the Christian faith compels adherents to respond to and struggle against.

This tension has resulted in a great diversity of theological conclusions relating to the extent to which warfare is compatible with Christian discipleship. Arguably, the most dominant ethical tradition on this matter is the JWT, which finds its source in the theological conclusions of thinkers such as Saint Augustine and Saint Thomas Aquinas. The JWT proposes that armed conflict can be compatible with Christian discipleship under certain restraining circumstances. The doctrine is primarily expressed as

possessing two sets of guiding criteria. The first – *jus ad bellum* (Latin for "the right to go to war") – identifies the criteria which must be satisfied for a war to be waged. The second – *jus in bello* ("right conduct in war") – examines the attributes of moral behaviour in the context of warfare. These two segments of the JWT possess broadly agreed-upon component parts (Lazar, 2016). While this article will focus on the JWT as expressed in the Christian context, readers need to be aware that scholars have rightly noted that numerous pre-Christian societies have also developed doctrines and standards for the ethical use of warfare. For instance, the *Mahabharata*, an Indian epic poem likely composed beginning in the 3rd century BCE, and the *Bhagavad-Gita*, both present approaches to thinking about the morality of warfare, many of which have similarities to what would become the Christian JWT (Kosuta, 2020:189-191). Similarly, contemporary non-Christian religious traditions also espouse their own renderings of just war. Nonetheless, the Christian expression of JWT has had a significant impact on contemporary laws of armed conflict and humanitarian law, such as the Geneva Conventions.

Aquinas, writing within the *Summa Theologiae* (Secunda Secundæ Partis, Question 40), identifies three *jus ad bellum* principles which he believes must be satisfied if a war is to be considered licit within the Christian tradition: a proper or legitimate authority, a just cause, and a right intention (Aquinas, 285-286). The first criterion – proper authority – indicates that God has endowed governments with specific duties and rights which are not afforded to individuals, among them the right to "protect the republic" from both internal and external threats by way of "the material sword" (Aquinas, 285). For Aquinas, the just war is something of a corrective and restoring act, for war can only be waged in response to "some fault" by another party (just cause) and must be waged with the intent to "promote the good and to avoid evil" (right intention) (Aquinas, 285-286). While Aquinas does not explicitly define what is meant by "some fault," he does support his argument by citing Augustine who argues that "Just wars are normally defined as wars that avenge injuries, where the nation or city to be punished is one that has either neglected to make amends for what was done unjustly by its subjects or refused to restore what was lost through injury" (Aquinas, 285).

Of notable importance to the subject of this article is Aquinas' requirement that war be carried out only by a proper or legitimate authority, which he likens to "the authority of the prince," for it is this authority, as opposed to a "private person," who is justified to "call together a multitude, which has to be done in war" (Bauerschmidt, 2021:217-218). I suggest that this is of particular importance because it would seem to presume that wars, even those which use deception, must still be carried out by known and recognised belligerents responding to a particular injustice with the ambition of restoring peace. A recognised leader is assumed to fight under their own banner. This would also seem to require or generate a certain degree of ownership, accountability, and responsibility for military activity and the conduct of operations on the part of the state which elects to fight. I contend that Aquinas would likely find anonymous military action or military action presenting itself as the work of another nation or kingdom to be illicit due to its incongruity with his requirement that a legitimate and representative ruler carry out warfare. For Aquinas, there appears to be a linkage between the principle of legitimate authority and responsibility for the harms of war.

Within the *Summa Theologia*, Aquinas' treatment of *jus in bello* principles is less developed and requires more inference from readers. However, he does offer some explicit guidance relating to the use of force by the clergy, ambushes and deception, and warfighting on holy days (Buzar, 2020:1300-1301). *Jus in bello* principles, as they have since become widely accepted, relate to war's minimisation of harm to non-combatants. *Jus in bello* principles include discrimination, which holds that directly targeting non-combatants is impermissible, and two principles related to collateral impacts on non-combatants, proportionality, and necessity. The former requires that any act of war which may harm civilians may only be carried out if the harms incurred are proportionate to the mission's goals (which is assumed to be just). The latter criterion – necessity – requires that militaries select the least harmful means available to them, while still enabling them to achieve their objectives (Lazar, 2020).

For this assessment, Aquinas' remarks on ambushes in war (Secunda Secundæ Partis, Question 40, Article 3) (which are included within his wider treatment of warfare) are highly relevant because they most explicitly address deception. Aquinas states that ambush tactics are "ordered toward deceiving one's enemies" (Aquinas, 288). He does

not, however, provide readers with a blanket condemnation or endorsement of deception in the context of war. Instead, he notes that there are just and unjust uses of deception in warfare. In particular, Aquinas notes that it is "always impermissible" to deceive through intentional lies or by breaking promises (such as peace treaties), noting that "there are certain 'rights of war' and pacts that are to be honoured even among enemies themselves" (Aquinas, 288). Nonetheless, Aquinas simultaneously holds that it is legitimate to deceive through non-disclosure of strategically sensitive information. "This sort of secretiveness," Aquinas argues, "belongs to the nature of the insidious tactics which it is permissible to use in just wars" (Aquinas, 288). Aquinas distinguishes between lying and concealment (Reichberg, 2018:288). For Aquinas, the aforementioned ambush on the city of Ai would likely have represented a justified use of concealment instead of an intentional act of lying. Had Joshua agreed a peace treaty with the people of Ai under false pretences and subsequently attacked the city, this would have almost certainly been viewed as an illegitimate use of deception by Aquinas because it utilised intentional lying.

Modern warfare adds a unique "middle ground" challenge to this paradigm. Whereas Aquinas may have seen deception through the lens of lying or concealment, cyber warfare often makes use of published information which is intentionally misleading or false as a means of camouflage or disguise. For instance, a cyber weapon may be designed to appear to a system user as an innocuous or routine file, perhaps by appearing to come from a recognisable or trusted source. Do such acts represent "impermissible" intentional lies which are contrary to the Christian virtue of honesty? Or do they represent the "permissible" use of secretiveness and concealment inherent within warfare? While it is difficult to state with certainty how Aquinas would parse out these questions, it is essential to note that Aquinas' remarks are being shared in the context of "insidious tactics" and ambushes. They are offered in response to proposed objections relating to fraudulent misrepresentations. Aquinas understands what is at stake: ambushes result in death and injury but may also help a party that is fighting for a just cause to gain a competitive advantage. I propose that, for Aquinas, context is what matters most. Deception – to include the sharing of misleading or erroneous information – may be justified when it occurs outside of a context where an adversary could reasonably expect peace-making efforts to occur, such as in a formal diplomatic

discussion. I would generally argue that designing a cyber weapon in a manner which enables it to "blend in" with a given information technology ecosystem and thus avoid easy detection would be more closely related to camouflage (a well-known tool of concealment) than it would be to lying in a manner which reflects bad faith (*mala fides*) between warring parties. It is one thing for an instrument of war to be easily overlooked. It is another thing to falsely lead an adversary into a belief that they are afforded a particular protection. For these reasons, it is unlikely that Aquinas would have rejected all forms of concealment and deception in cyberspace. Nonetheless, there are forms of deception in cyber warfare which degrade good faith interactions between adversaries to which Aquinas would likely have strenuously objected.

3 Just and Unjust Uses of Deception Today

Like the Greek soldiers concealed within their wooden horse at the gates of Troy (Virgil, 75), cyberweapons today provide militaries with a means of attacking an adversary covertly and sometimes anonymously (Goines, 2017:86-87). The payload of a cyberweapon is deployed quietly within an exploited vulnerability of a critical information technology system. Often, the weapon is passed from user to user, system to system, without any awareness by system operators. This style of engaging the enemy through concealment and surprise resembles the military tactic of an ambush and broadly conforms to the JWT as understood and articulated by Aquinas.

Cyberweapons are designed to "disrupt the information systems upon which armed forces' operations increasingly depend – on land, at sea, in the air, even in orbit – or take aim at the control systems that run power, water, and other infrastructure in countries around the world" (Arquilla, 2021:2). These weapons are used, in an adaptation of Clausewitz's famous definition of the intention of war, "to impose the cyber aggressor's political will upon its adversaries through non-political means" (Lucas, 2017:9). As Brian Orend notes, those who deploy cyberweapons for these purposes "go out of their way to hide their tracks and conceal the ultimate source of the strike" (Orend, 2014:178).

Deception, in one form or another, is an essential and normative characteristic of warfighting as adversaries must, by necessity, seek to gain a strategic advantage over one another. Warfighting has long used deceptive practices and camouflaging

technologies (such as stealth technology and Ghillie suits). Nonetheless, the extent to which deception can be employed in war is constrained by ethical and legal considerations. While deception may be a central characteristic of stratagem, commanders are not free to deceive in an unmitigated manner. In this sense, contemporary laws of armed conflict and normative military ethics reflect the distinctions drawn by Aquinas.

Militaries – and the laws and conventions they are expected to adhere to – have long sought to distinguish between just and unjust uses of deception. In *Binary Bullets: The Ethics of Cyber Warfare*, Heather Roff modernises the distinction between just and unjust uses of deception proposed by Aquinas. The scholar notes a legal difference between *ruse de guerre* (ruse of war) and perfidy. Ruse, Roff explains, "permits a belligerent to engage in any type of deceptive activity that does not violate a law or use and pervert the law in such a way to endanger the protections provided by LOAC (laws of armed conflict)." Perfidy, by contrast, "constitutes an act whereby a belligerent uses the laws of armed conflict to make its adversary believe he has been accorded some protection with the intent to breach that trust through killing, wounding, or capturing" (Roff, 2016:204). The armed forces of the United States offers this definition: "Acts of perfidy are deceptions designed to invite the confidence of the enemy to lead him to believe that he is entitled to, or is obliged to accord, protected status under the LOAC (laws of armed conflict), with the intent to betray that confidence" (Joint Chiefs of Staff, Publication 3-13.4). Scholars generally agree that "international law prohibits only those perfidious acts intended to result in death or injury" (Schmitt, 2017:122.2). Aquinas likely would have understood perfidy as being morally disordered because it undermines the essential mutual trust that must be maintained even amongst enemies by way of intentional lying.

Roff provides a helpful example of this distinction in examining some permissible and impermissible actions in naval warfare. She notes that warships are permitted to fly false flags up until the moment that they commence hostilities. They can also "use deceptive lighting techniques, where they disguise themselves to look like civilian ships." They may use "dummy ships and other armament, decoys, simulated forces, feigned attacks and withdrawals, ambushes, false intelligence, electronic deceptions,

and use of enemy codes, passwords and countersigns" to mislead their adversary (Roff, 2016:204). These actions represent a ruse. A warship may not, however, feign a distress signal to draw another vessel to it under the false pretence of an emergency. Doing so represents perfidy. Article 37 of *Additional Protocol I of the Geneva Conventions* identifies other examples of perfidy, which include falsely flying a flag of truce or surrender, pretending to be sick or injured, disguising oneself as a non-combatant, or fraudulently identifying oneself as a neutral party, such as falsely wearing the uniform or symbols of a United Nations peacekeeper (International Humanitarian Law Databases, 1977).

It is important to note that there is, on occasion, a tension between the position of ethics and the rule of law. Warships, as noted, may legally use deceptive lighting to appear as civilian (non-combatant) vessels until they commence hostilities. However, the Geneva Conventions prohibit disguising oneself as a non-combatant. Roff explains, "that the law of the sea does not explicitly forbid such acts, and that they did not result in the injury, killing, or capture of enemy combatants, does not necessarily make such acts morally permissible, though they are legally so" (Roff, 2016:206). An act can simultaneously be legal and immoral.

The differentiation between just and unjust modes of deception and disguise necessitates a certain degree of trust and mutual respect between armed belligerents engaged in conflict. At the very least, it requires a shared belief that some things, even in war, are sacrosanct, such as caring for injured personnel and adhering to terms of surrender. This sense of trust can be, and often is, degraded through war crimes, torture, and other unjust uses of force. Such actions are broadly considered illegal under international law and run far beyond ethical norms while simultaneously fostering an environment that degrades the mutual trust necessary for diplomacy to prevail. This is why an ethical standard should be advocated for and upheld, even amidst the so-called fog of war.

4 Deception in Cyber Warfare

Cyberweapons, by design, operate deceptively out of necessity. No user would knowingly download or install military-grade malware on their computer or information

system that they understood to be harmful to their cause. Cyberweapons are characteristically designed to exploit vulnerabilities that are difficult to notice or detect. This includes zero-day exploits, which target vulnerabilities in cyberspace which have yet to be discovered by critical vendors of an operating system. Unsurprisingly, the term "Trojan Horse," borrowed from Homer and Virgil, has become a standard industry term for malware that disguises its true intent from users. Nations which are responsible for cyberattacks generally take care "to conceal their identities when such obfuscation is politically useful" are rarely take responsibility for their actions once a mission is completed (Brown and Fazal, 2021:401).

Given the actual and potential impact of cyberweapons on people, property, and data, it is necessary for modern militaries to grapple with the ethical implications of deception in cyberspace and to design cyberweapons which leverage just uses of subterfuge. The JWT holds that war may be waged with a strategic mindset and that it may leverage deceptive practices. However, it also emphasises that real constraining limits exist around these practices to protect the rights and dignity of vulnerable people and ensure that a pathway to peace and diplomacy remains intact.

Let us consider a real-world, non-cyber example as a thought experiment: In April 2017, Taliban fighters dressed as injured soldiers entered an Afghan army base. Once on base, the disguised Taliban fighters proceeded to kill or injure up to 170 people (Titterton, 2022). This is a clear example of unjust deception, as the combatants assumed the identity of injured personnel requiring medical care. In clear violation of Article 37.1.b of the Geneva Conventions, these combatants feigned incapacitation and committed perfidy. They misled the Afghan military, operating with a modicum of mutual trust, to provide humanitarian assistance to these individuals with the intent to mislead and cause grievous harm. Had the Taliban fighters identified themselves as combatants and attacked the Afghan army base through strategic surprise (*ruse de guerre*), their actions would have been seen as a deception, which could reasonably be expected in combat, even if the total number of casualties were the same. As such, the ethical delineation between a just and unjust act of deceptive military violence relates to the context and pretences under which the violent act is carried out, not simply to the result of the action.

Legal and moral restrictions on deceptive practices do not exclude the domain of cyberspace, especially when cyberspace can be militarily exploited in a manner that generates real-world harm and adds strategic value to a broader warfighting effort. Like any morally justified military operation, using cyberweapons against an adversary can and should reflect *jus ad bellum* and *jus in bello* principles governing conduct in war.

For cyberweapons to be effective, they must gain access to a target network, machine, or software. As the computer scientist Ian Trump (2012:7) notes, "Cyberweapons… have a similar characteristic in that they need a human to deliberately infect, by error, omission, naivety, or conspiracy a computer system, which was not directly on the Internet." Other cyberweapons do not require human intervention. However, all "enter a network or software program through seeming "friendly" or authorised means, but with deceptive and potentially malicious intent" (Roff, 2016:210). As Cordula Droege notes, "anonymity is the rule rather than the exception" when it comes to cyber warfare (Droege, 2012: 541).

Often, this apparently "friendly" appearance is accomplished by disguising the cyberweapon as a civilian (non-combatant) tool or presenting it as originating from a friendly country or organisation (Roff, 2016:211). One might consider the case of Stuxnet, a cyber weapon deployed against the Iranian nuclear program. Discovered in 2010, Stuxnet was responsible for the physical destruction of hundreds (perhaps thousands) of Iranian nuclear centrifuges. It is widely understood that the weapon was designed and deployed through a joint effort between the United States and Israel. Stuxnet is particularly notable for being the first known example of a cyber weapon causing physical damage (Lucas, 2017:58-59). In her landmark study of this attack, *Countdown to Zero Day*, investigative journalist Kim Zetter notes that the malicious computer worm was disguised to appear as though it were utilising legitimate digital certificates from a company called RealTek Semiconductor, a trusted Taiwan-based manufacturer, and "each time Stuxnet infected a system it 'phoned home' to one of two internet domains masquerading as soccer fan sites…the domain names, registered by someone who used fake names and fraudulent credit cards, pointed to servers in Denmark and Malaysia…" (Zetter, 2014:27). The militaries using the weapon disguised themselves as other friendly nations and civilian organisations during the execution of

the attack. This mode of deception disguised the weapon as non-combatant in nature (a soccer fan site, a concocted private individual, a semiconductor manufacturer) and falsely identified itself as being connected to nations not a party to the conflict (In this case, Denmark and Malaysia).

Other forms of cyber deception leverage real or real-seeming mirror sites, masquerading as non-combatant private websites, such as popular news sites or search engines (Roff, 2016:212). Again, authentic weapons of war cannot be disguised in the "uniform" of a non-combatant entity as they engage an adversary. This deception would lead a reasonable person to believe they are engaging with someone, or some party, "entitled to…protected status" (Joint Chiefs of Staff, Publication 3-13.4). The just war principle of non-combatant immunity clarifies that civilians are classified within a "protected status." Deceptive practices like this, while operationally effective, may shift the conduct of a military operation closer to an unjust use of force because their destructive purposes are disguised to appear as civilian or neutral-nation infrastructure or personnel. When malware is designed in this manner, the ethical character of the concealment begins to shift towards bad faith engagement, as the proper or legitimate authority is no longer accountable for their actions and the potential for more significant harm is elevated by potentially exposing innocent parties to retaliation. Such actions also undermine the ability of the international community to assign responsibility to a party to a conflict or an individual. As Droege notes, "all law is based on the allocation of responsibility," especially as it relates to international humanitarian law (Droege, 2012: 541).

Contrary to conventional weapon systems designed to generate lethal force, cyberweapons have been utilised in the military context to kill operations, control systems, and production, not people (Trump, 2015). Nonetheless, cyber-attacks are increasingly targeting critical utilities upon which non-combatants may rely for safety. For instance, in 2015, a cyberattack against Ukraine's power grid degraded access to electricity amidst the Ukrainian winter (CISA, 2021), and in 2021, a ransomware attack on the Colonial Pipeline in the United States impacted fuel availability across the eastern seaboard of the United States (Easterly, 2023). This signals an increasing ability to degrade critical infrastructure through a cyberattack. While these events may not

directly relate to the death or injury of individuals, they can carry damaging second-order effects. For instance, a cyberattack deployed against a power grid could undermine a hospital's ability to treat patients or cause vulnerable people to be impacted by the heat or cold, while a cyberattack against a water filtration plant could leave communities without safe drinking water. In addition, the likelihood of human death or injury occurring in the future is ever-increasing, especially as the internet of things continues to proliferate. What is undoubtedly clear is that many cyberattacks originate from deceptive practices which falsely present the cyberweapon as being aligned with an individual, group, or nation with "protected status," a strategy which would almost certainly have been rejected as illicit by Aquinas because it undermined the responsibility of a legitimate authority for conducting warfighting, degraded the notion of non-combatant immunity, and damaged the trust necessary for peace-making. The fact that this routinely occurs in a manner which is covert or anonymised, without after-action claims of responsibility, makes it difficult or impossible to assign accountability.

5 A Simple Proposal for Enhancing the Ethical Character of Cyber Warfare

Ethical constraints on the conduct of militaries in war exist to limit harm, protect innocent people, and ensure that a pathway to peace is maintained. While deception is normative, unjust deception can erode mutual trust so significantly as to reduce the likelihood of good-faith diplomatic engagement (Roff, 2016:220). This creates an environment where hostilities are likely to continue in a more unchecked manner.

Regarding cyberweapons, this article presents two steps militaries could undertake to help ensure that deception in cyberspace is undertaken justly. Those two steps are:

- (1) Avoidance of False Association with Protected Peoples, Nations, or Organisations
- (2) After-Action Claims of Responsibility

Avoidance of False Association with Protected Peoples, Nations, or Organisations

Unjust deception might include armed soldiers disguising themselves as injured civilians before enacting violence on an unsuspecting adversary or a warship feigning a distress call to compel an opponent into a strategically vulnerable position. However, analogous practices are common in the cyber domain to persuade adversaries to engage with malicious software. The Tallinn Manual (2.0) notes that "it may be perfidious to make such websites (or other cyber entities) appear to have civilian status with a view to deceiving the enemy to kill or injure" (Schmitt, 2017:122.12) and that "an operation that is masked in a manner that invites an adversary to conclude that the originator is a civilian or other protected person is prohibited if the result of the operation is death or injury of the enemy" (Schmitt, 2017:122.13). Care should therefore be taken to ensure that deceptive practices related to the use of cyber weapons do not rely on presenting false attribution information, which could conceivably lead a recipient to reasonably believe that they are engaging with a civilian, a neutral nation, or a protected organisation (such as the Red Cross, a religious organisation, or a healthcare provider).

While perfidy represents a particular form of illegal and unjust deception to be strictly avoided in armed conflict, it also provides militaries with essential characteristics that define unjust conduct. Compliance with the laws of armed conflict is a necessary component of justice in warfighting, but so is adherence to a more expansive set of ethical norms. As such, nations which leverage deceptive practices in their cyber operations should avoid weapon designs which falsely attribute the software to a protected person or people group, nation, or organisation.

After-Action Claims of Responsibility

Accountability, both public and legal, is an essential deterrent to immoral or illegal activity in war. Militaries will commonly publicly claim responsibility for covert military strikes using conventional arms after they have been carried out. For example, President Barack Obama publicly claimed responsibility for the secret military raid in Pakistan which resulted in Osama Bin Laden's death. President Joe Biden claimed responsibility for a missile attack in Afghanistan in 2022, which killed Bin Laden's successor, Ayman al-Zawahiri. In both examples, the United States was not involved in formal hostilities

with the countries where the attacks occurred. While these claims of responsibility occurred *ex post facto*, they nonetheless enabled public, political, legal, and moral discourse, which could shape future actions.

Militaries which deploy cyber-attacks should claim responsibility for those attacks once their strategic goals have been met. With cyber warfare, such claims of responsibility are rare. For instance, while cyber forensics have largely concluded that the Stuxnet computer worm which impacted Iran's nuclear program was a collaborative effort between the United States and Israel, neither nation has formally acknowledged this as accurate (Lucas, 2017). Brown and Fazal note that states rarely accept responsibility for cyberattacks, potentially out of concern that doing so would increase the risk of escalation (Brown and Fazal, 2021:415). But this presents its own paradox: the lack of accountability which results from this practice only contributes towards the proliferation of anonymous and potentially unjust military activity in the cyber domain.

Taken together, these two suggested steps help to strengthen a connection with Aquinas' *jus ad bellum* principle requiring warfighting efforts to be clearly undertaken by a legitimate and recognised authority while simultaneously enacting reasonable safeguards against *jus in bello* prohibitions against unjust uses of deception and the proliferation of violence. Notably, adopting these steps may help safeguard good faith between warring parties, which is essential for restoring peace (Mattox, 2002:8-9).

6 Conclusion

It is not difficult to see why militaries are increasingly drawn to the cyber domain. As a space vital to everyday life, government continuity, economic health, and communication, it is critical for defence and national security. For these same reasons, it is an increasingly strategic domain for an attack. Cyberweapons offer militaries a tool by which they can degrade their adversary's capabilities while simultaneously placing fewer personnel in direct danger. What is more, cyberweapons can be easily disguised.

Cyberweapons are still weapons, and war is still war. As Stuxnet demonstrated in Iran, cyberweapons can generate physical destruction, and one can imagine them causing significantly greater destruction in the future as technological capabilities and vulnerabilities expand. For these reasons, militaries should utilise these weapon

systems in a manner that accords with established principles on ethical conduct in war. This is particularly true today as it might be suggested that we are setting up a de facto precedent for how these categories of weapons will be utilised in the future.

While it is undoubtedly true that cyberweapons present unique ethical and operational realities, it is also true that well-established *jus in bello* principles have long proven their adaptability to emerging weapons, novel tactics, and previously unseen technologies. Militaries seeking to engage their adversary in a manner which reflects a justified use of violence would do well to actively apply prohibitions against unjust deception within the design, coding, and deployment of cyberweapons. Doing so demonstrates a commitment to the principle of non-combatant immunity and a more consistent application of codified legal and ethical norms, such as those enshrined within the Geneva Conventions. A just war, by definition, must be directed towards the goal of peace-making. This goal is only attainable when belligerents have some common understanding of justice and some level of diplomatic trust.

Avoiding unjust deception helps to enable the trust that is necessary for proactive peace-making. As Saint Augustine writes, "*fides etiam hosti servanda*" (faith must be kept even by the enemy) (Roff, 2016:203). This, of course, is not something that comes easily between warring parties. Nonetheless, a posture of distrust by one party does not require the other to abandon its moral foundation. It has long been demonstrated that militaries can fight both strategically and ethically. As the ethicist Michael Walzer eloquently notes, "Moral concepts and strategic concepts reflect the real world in the same way…and without them we would have no coherent way of talking about war" (Walzer, 2015:14). It is true, then, that when we speak of deception we must necessarily speak of its strategic and moral character.

The JWT has long recognised and, in principle, supported deception in armed conflict, as Aquinas makes clear in his treatment of the issue. However, this support is tempered by calls for restraint regarding deceptive practices undermining humanity's ability to seek reasonable refuge from conflict through non-combatant status, surrender, truce, incapacitation, or distress signals. Perfidy, which relates to exploiting these protected statuses for strategic gain, is one area where the JWT strongly objects. However, in a much broader sense, unjust deception can degrade pathways to peace

while putting innocent people at an increased risk of harm and is prohibited under this moral tradition. Just as medieval thinkers such as Saint Thomas Aquinas articulated, intentional lies and the breaking of promises can represent an injustice in war. Today, ethics demands that a promise of justice between combatants and non-combatants be maintained. While there may be the temptation to vacate this ethical responsibility when engaged in conflict with an adversary who holds no such moral standard, militaries would do well to remember Grotius' maxim "faith must be kept even with the faithless" (Neff, 2012:423).

Cyberweapons provide nations with a unique and highly customisable warfighting instrument. To be effective, this new category of weapon must be deceptive. It must infiltrate the information technology architecture of an adversary's systems and remain undetected. However, when this deception is carried out in a manner which places non-combatants at risk while degrading pathways to peace, it represents an injustice which betrays the JWT.

7 References

1. *Article 37 - Prohibition of perfidy. (*1977). *International Humanitarian Law Databases*. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-37 (Accessed: 27 November 2023).
2. Arquilla, J. (2021). *Bitskrieg: The New Challenge of Cyberwarfare*. Cambridge: Polity Press.
3. Attridge, H.W. and Society of Biblical Literature. (2006). *The HarperCollins Study Bible: Fully Revised & Updated*. New York: HarperCollins.
4. Bauerschmidt, F. (2021). The Essential Summa Theologiae: A Reader and Commentary. Grand Rapids: Baker Academic.
5. Brown, J.M. and Fazal, T.M. (2021). '#SorryNotSorry: Why states neither confirm nor deny responsibility for Cyber Operations', *European Journal of International Security*, 6(4), pp. 401–417. https://doi:10.1017/eis.2021.18
6. Buzar, S. (2020). 'The principle of double effect and just war theory,' *Philosophia*, 48(4), pp. 1299–1312. https://doi:10.1007/s11406-020-00209-2
7. Clough, D. and Stiltner, B. (2007). *Faith and Force: A Christian Debate about War*. Washington, D.C: Georgetown University Press.
8. *Cyber-attack against Ukrainian critical infrastructure: CISA*. (2021). *Cybersecurity and Infrastructure Security Agency CISA*. 2021. Available at:

https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (Accessed: 27 October 2023).

9. Droege, C. (2012). 'Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians', *International Review of the Red Cross*, 94(886), pp. 533–578. https://doi:10.1017/s1816383113000246
10. Easterly, J. (2023). *"The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." Cybersecurity and Infrastructure Security Agency CISA*. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (Accessed: 5 November 2023).
11. Freddoso, A. (2023). *New English Translation of St. Thomas Aquinas's Summa Theologiae (Summa Theologica)*. Available at: https://www3.nd.edu/~afreddos/summa-translation/TOC.htm (Accessed: 27 October 2023).
12. Goines, T.M. (2017). 'Overcoming the Cyber Weapons Paradox', *Strategic Studies Quarterly*, 11(4), pp. 86–111.
13. Kosuta, M. (2020). 'Ethics of war and ritual: The Bhagavad-Gita and Mahabharata as Test Cases', *Journal of Military Ethics*, 19(3), pp. 186–200. https://doi.org/10.1080/15027570.2020.1824578
14. Lazar, S. (2016). *War*, *Stanford Encyclopedia of Philosophy*. Available at: https://plato.stanford.edu/archives/spr2020/entries/war/ (Accessed: 27 October 2023).
15. Lucas, G.R. (2017). *Ethics and cyber warfare the quest for responsible security in the age of Digital Warfare*. New York, NY: Oxford University Press.
16. Mattox, J.M. (2002). 'The moral limits of military deception,' *Journal of Military Ethics*, 1(1), pp. 4–15. https://doi:10.1080/150275702753457389
17. *Military Deception. (*2012). *Joint Forces Staff College*. Available at: https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf (Accessed: 27 October 2023).
18. Neff, S.C. (2012). *Hugo Grotius on the Law of War and Peace: Student Edition*. Cambridge: Cambridge University Press.
19. O'Donovan, O. (2003). *The Just War Revisited*. Cambridge: Cambridge University Press.
20. Orend, B. (2014). 'Fog in the Fifth Dimension: The Ethics of Cyber-War', in L. Floridi and M. Taddeo (eds.) *The Ethics of Information Warfare*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-04135-3_1
21. *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1). (1977). United Nations Human Rights Office of the High Commissioner*. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and (Accessed: 27 October 2023).

22. Reichberg, G.M. (2018). *Thomas Aquinas on War and Peace*. Cambridge: Cambridge University Press.

23. Roff, H.M. (2016). 'Cyber Perfidy, Ruse, and Deception', in F. Allhoff, A. Henschke, and B.J. Strawser (eds.) *Binary Bullets: The Ethics of Cyberwarfare*. New York: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190221072.003.0011

24. Schmitt, M.N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

25. Singer, P.W. and Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

26. Titterton, J. (2022). *Deception in Medieval Warfare: Trickery and Cunning in the Central Middle Ages*. Boydell & Brewer, Inc.

27. *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years: CISA*. (2023). *Cybersecurity and Infrastructure Security Agency CISA*. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (Accessed: 27 October 2023).

28. Trump, I. (2012). 'Surviving a Cyberapocalypse', *EDPACS*, 46(4), pp. 1–14. https://doi:10.1080/07366981.2012.724997

29. Virgil. (2006). *The Aeneid*. Translated by R.W.F. Fagles. London: Penguin Classics.

30. Walzer, M. (2015). *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: Basic Books.

31. Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first Digital Weapon*. New York: Crown Publishers.