National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

INFORMATION ETHICS: A BRIDGE INTO THE CYBERSPACE DOMAIN

Squadron Leader Samantha Couper

JCSP 46	PCEMI 46
Solo Flight	**Solo Flight**
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n’engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.
© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2020.	© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2020.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

INFORMATION ETHICS: A BRIDGE INTO THE CYBERSPACE DOMAIN

By Squadron Leader Samantha Couper

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 5,092

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Nombre de mots : 5.092

INFORMATION ETHICS: A BRIDGE INTO THE CYBERSPACE DOMAIN

INTRODUCTION

> *Every age has its own kind of war; its own limiting conditions; and its own peculiar preconceptions.*
>
> - Carl Von Clausewitz, *On War*

In the 2016 Defence White Paper (DWP), the Australian Government, as part of its long-term planning for Australia's defence, recognized the emerging requirement for an ADF Cyberspace capability. A subsequent Strategic Policy Statement for Cyber was released in June 2018 to provide overarching guidance to the Department of Defence.[1] The DWP recognizes that "beyond the increasing military modernization, the strategic environment of the next 20 years will be shaped by complex non-geographical threats, such as…cyberspace and space."[2] The ADF is preparing for a security environment which in peacetime and during armed conflict, will feature increased threats from offensive cyber and space-based capabilities. ADF cyber systems, workforces and education programs are being strengthened to protect the ADF's warfighting and information networks to counter the threat of cyber-attack.

To understand the challenges facing a new generation of Commanders in the ADF, this paper will utilise theoretical concepts of war and ethics to identify the complexities of command decisions in the cyber domain. First an ADF perspective of Cyberspace Warfare is explored and the fundamentals of Just War Theory (JWT) as it applies to Cyber Operations is broached. Second, where JWT proves ambiguous to Cyber Operations, the application of a nuanced and complimentary ethical framework is

[1] Strategic Policy Statements (classified) provide overarching guidance to the Department of Defence and sit directly under Defence White Papers and Defence planning Guidance.

[2] Commonwealth of Australia, *2016 Defence White Paper* (Canberra: Australian Government, Department of Defence, 2016), 51 – 89.

explored to understand how Commanders may address the complexities associated with defensive and offensive measures in Cyber warfare. The ADF Cyber workforce and employment training is then analyzed to determine outstanding deficiencies in ethics education which limit the effectiveness of Cyber Commanders. This paper will demonstrate that there are current legal and policy deficiencies in cyberspace operations and that the application of Information Ethics would greatly improve the ability for Commanders to make effective, efficient military decisions when operating in this domain.

CYBERSPACE WARFARE - AN ADF PERSPECTIVE

> *Superiority in the physical environment is of little value unless it can be translated into an advantage in the information environment.*
>
> - *Sir Lawrence Freedman*

The ADF is currently awaiting endorsement of Australian Defence Doctrine Publication (ADDP) 3.24 Cyberspace Operations. ADDP are authorized joint doctrine for the guidance of ADF operations, and state the ADF's philosophical military approach to the operational environment. More implicitly, ADF doctrine is a description of the application of force to achieve Australia's national interests both domestically and internationally. Doctrine unlike policy, is not prescriptive and therefore has no legal standing, however it does provide authoritative and proven guidance. With Cyberspace doctrine awaiting endorsement, and due to the classified nature of ADF Cyber activities, the following provides a sanitized conceptual overview of ADF Cyber philosophy and impending capability.

Cyberspace warfare is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace by direct action.

Cyberspace as a capability may be defined as the global domain within the information environment consisting of information technology structures, internet communication networks, computer systems, and data.[3] While part of the information environment, cyberspace, remains dependent upon the physical domains of maritime, land, air and space to achieve mission success through reliance on networked or stand-alone information technology (IT) and platform specific technology systems.

Cyberspace warfare differs from physical warfare with the advantages of being able to impact all domains synchronously; it is not geographically constrained and time approach is zero.[4] Taddeo and Glorioso make the further distinction that within Cyberspace warfare "the nature of actors and targets involves artificial and virtual entities alongside human beings and physical objects and their level of violence may range from non-violent to potentially highly violent phenomena."[5] However, attribution in the Cyber domain is complex, while not nuclear weapons; cyber weapons are existential threats. "A cyber-attack can seriously degrade military capability or affect the lifestyle of a nation…but cyber by itself does not threaten the survivability of a country or its population."[6] Unlike a physical force in a tangible environment, cyber does not openly represent a posture or the ability to execute traditional kinetic effects as either a deterrence or offensive measure. Therefore, cyberspace operations used *in isolation* will not win a war.

[3] Australian Defence Force, *ADDP 3.24 Cyberspace Operations*, (Canberra: Department of Defence, 2020).

[4] Source: Larry Burger, 'Cyberspace,' US Army Space and Missile Defense Command, Future Warfare Center, Huntsville, AL, Slide 6. All domains include: sea, land, air, cyberspace and space.

[5] Mariarosaria Taddeo and Ludovica, *Ethics and Policies for Cyber Operations* (Switzerland: Springer International Publishing, 2017), introduction page x.

[6] Craig Stallard, *At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force* (Canberra: Commonwealth of Australia, 2014), 44.

Cyberspace operations can be either defensive or offensive. Defensive cyberspace operations (DCO) are conducted to defend friendly force cyberspace and enable mission assurance at key points in time for the supported commander. DCO includes the ability to use friendly force cyberspace to protect resident data and IT from active threats against networks and mission systems, including returning compromised networks to a secure and functional state.[7]

Offensive cyberspace operations (OCO) are missions intended to project power into and through cyberspace. OCO may exclusively target adversary cyberspace capabilities or create first-order effects in cyberspace to initiate controlled cascading effects into the information environment or other domains i.e. adversary weapon systems, command and control processes, or logistics nodes. OCO requires a carefully considered scope, to ensure Rules of Engagement (ROE) and the moral requirements associated with justifiable warfighting are considered by Commanders.[8] As demonstrated, Cyberspace operations are inherently complex and demand unique and specialized education and training in order to ensure proficiency in rapid and ethical decision making.

RULES OF WARFARE: JUST WAR THEORY

The key concepts of Just War Theory (JWT) are categorized by the criteria for both going to war (*jus ad bellum*) and justifiable fighting throughout a war (*jus in bello*). JWT contends one's motive/s need to be ethically proper and no futile war should be undertaken. JWT ad bellum factors are considered by either state legislative or executive branches, and in bello factors are aimed at military decision makers who are required to

[7] Australian Defence Force, *ADDP 3.24 Cyberspace Operations*, (Canberra: Department of Defence, 2020).

[8] *Ibid*.

adhere to laws (International Human Law (IHL) and the Law of Armed Conflict (LOAC)). While both ad bellum and in bello rules are part of LOAC, JWT, as a "theory of ethics, levies two additional moral requirements: [right intention and probability of success]".[9] Through understanding JWT as applied to traditional physical warfare, one may consider how the theoretical principles may apply to emerging forms of technologically advanced warfare such as the Cyberspace domain e.g. the ethical implications of targeting, attack and harm in multidimensional warfare, specifically the non-physical of cyber.

Tenets of Just War

The purpose of *Jus ad Bellum* rule is to determine when and if states may enter the realm of warfighting. More broadly, Orend contends "[JWT] opines that while war can be morally permissive, [JWT] views war dimly and dangerously, [insisting] it's too risky and lacking in restraint to allow for anything goes."[10] The principles of *jus ad bellum* include: just cause; public declaration of war by a proper authority; last resort; and proportionality**.** Reviewing cyberspace attacks through the lens of these principles, in conjunction with the moral requirements of right intention and probability of success, allows one to identify the ethical issues associated with warfare in the information environment, specifically Cyber.[11]

[9] Brian Orend, "Fog in the Fifth Dimension: The Ethics of Cyber-War," in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 13. Right Intention while not part of international law, attempts to measure if one's motives are 'ethically proper' through determining one's potential ulterior motive to avoid instances of unnecessary aggression. Probability of success pertains to not initiating a futile war – attempts to prohibit pointless killing and suffering.

[10] *Ibid*., 10.

[11] Cyberspace attack is a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the intent to seriously compromise national security, stability or economic prosperity.

Just Cause

Three general principles apply to just cause; right to go to war in self-defense from aggression; right of other-defence/collective security to aid or assist any country victimized by aggression; and any other force as approved by the United Nations Security Council (UNSC) i.e. preemptive strike or armed humanitarian intervention.[12] When considering Cyberspace warfare, cyber-strike does not necessarily constitute aggression in the traditional sense of the term due to a direct lack of kinetic effect, or more specifically placing human lives in direct jeopardy.[13] However, Orend does posit that aggression may be met when cyber-attacks *lead* to physical damage including loss of life, and or when a cyber strike might be more damaging than a physical strike. “The key concept here is that our thinking as to what constitutes aggression needs to keep pace with the times and new technologies.”[14] Therefore, the ADF needs to be flexible in the way it detects and treats these technological threats. This flexibility in thought and action also supports Orend’s definition of JWT ‘right intention’ and ‘probability of success’ whereby ADF Cyberspace operations will “prohibit pointless killing and suffering” and be constrained by actions related to deterring, foiling and punishing aggression, and nothing more.[15]

[12] Brian Orend, “Fog in the Fifth Dimension: The Ethics of Cyber-War,” in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 11. Further, “aggression” in this sense is defined as any unjustified use of force against another country.

[13] Patrick Lin., Fritz Allhoff., and Keith Abney, “Is Warfare the Right Frame for the Cyber Debate,” in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 41.

[14] Brian Orend, “Fog in the Fifth Dimension: The Ethics of Cyber-War,” in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 14.

[15] *Ibid*., 13.

Public Declaration

Traditional wars are declared by a state's governmental branch which holds the "power" to assert force and warfare. In non-traditional warfare i.e. Counter Insurgency (COIN) or Cyberspace Warfare, the majority of attacks or conflicts are asymmetrical, and predominately non-attributable and therefore violate the public declaration rule of war. Due to the characteristics of cyberspace, attribution of malicious cyberspace activity to a specific threat actor can be difficult to trace. Therefore, when a non-declared and anonymous attack is affected and a highly probable offender suspected, but not explicitly known, the problem of attribution does not permit a retaliatory attack under JWT. The difficulty of attribution, along with the possibility that an apparent threat may actually be an attempt at misdirection, increases the risk of a response against the wrong threat, particularly a nation-state or a target within a nation-state.

Last Resort

States should only enter war as a last resort i.e. when all diplomatic efforts have failed such as economic incentives and sanctions. Simplistically, a State is expected to exhaust all avenues before engaging in warfighting. This is where the danger of Cyberspace strikes lay – levels above diplomacy and incentives, yet not as aggressive as kinetic attack (force). What if cyber-attacks are not considered as a last resort, rather a "first strike capability" that is inclined to work in conjunction with a kinetic attack?[16] Many countries have considered this scenario, and in the absence of International Law or Treaties regarding Cyberspace warfare, a number have declared that any "severe" cyber-

[16] *Ibid*., 15.

attack against them will be considered *casus belli* (an act provoking or justifying war).[17] The resultant conundrum – despite cyberspace-attacks being non attributable under International law or neatly defined within a hierarchy of foreign policy tools to prevent war, they can be viewed as a provocation depending on a recipients own interpretation or biases.[18]

Proportionality

Proportionality decrees the use of a like for like response to an attack. Specific to Cyber, this measure should constitute only strikes and responses in the same dimension – kinetic responses would not be considered a response in kind. However, as Cyber is often utilized as a precursor to enable kinetic attack, the challenge lies in determining whether a targeted body will respond in anticipation under preemptive strike.[19] Another complexity associated with cyber-attacks and proportionality is the "unintended proliferation and possibility of widespread conflict as attacks and counter attacks may spread beyond intended victims."[20] The ensuing ethical dilemma pertains to how one determines the appropriate counter attack to either a stand-alone cyber-attack or one where a subsequent kinetic attack is anticipated.

Concepts of Just Warfighting

The purpose of *Jus in Bello* rule is to guide military personnel throughout warfighting and serve as an accountability framework post conflict to determine if war

[17]Troy E. Smith, Trinidad and Tobaga, "Cyber Warfare: A Misrepresentation of the True Cyber Threat," *American Intelligence Journal Vol 31,* no. 1 (2013): 82, https://www.jstor.org/stable/26202046 In 2011, the Pentagon declared that cyber-attacks would act as casus belli.

[18] Such biases can include, differing cultural, political, religious, social and ethical influences.

[19] While no longer acceptable under the UN Charter unless specific prior approval is granted by the UNSC, pre-emptive strike should remain a consideration when States are engaging with all parties.

[20] Patrick Lin., Fritz Allhoff., and Keith Abney, "Is Warfare the Right Frame for the Cyber Debate," in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 43.

crimes have been committed. Violations can be processed “either domestically through their own military justice system or internationally through The Hauge.”[21] *Jus in Bello* are numerous and predominately apply to kinetic warfare, however the two principles of *Discrimination* and *Noncombatant Immunity* remain highly pertinent to Cyberspace warfare. The purpose of both principles is to ensure every effort is made to prevent civilian involvement in warfare and that only legitimate military targets are engaged during attacks.

Discrimination and Noncombat Immunity

Discrimination and Noncombat Immunity refers to distinguishing between legitimate and illegitimate targets and the rule that civilians are “immune” from intentional attack. The latter does not provide failsafe immunity from warfare, rather it works to prevent the killing of civilians. The principle of discrimination determines who can be killed and/or what may be destroyed. Proportionality and necessity determine the amount of damage permissible. More specifically, civilians are only entitled to “due care” in an effort to protect civilian lives and limit the identification and destruction of “dual use targets” i.e. basic infrastructure – sewers, oil and gas pipeline, electricity power and telephone lines.[22] When considering civilians and basic infrastructure, this is where the concept of *Jus in Bello* becomes strained in the Cyber domain as “Cyber warfare concentrates on the striking of an adversary’s power, communication, transportation and

[21] Brian Orend, “Fog in the Fifth Dimension: The Ethics of Cyber-War,” in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 15.

[22] Articles 51(2) and 52(1) of Additional Protocol I, decrees civilians, the civilian population and civilian objects ‘shall not be part of an *attack’*. With regard to other military operations, only a more general obligation of ‘constant care…to spare the civilian population, civilians and civilian objects’ applies (Additional Protocol I, 1977, Article 57(1).

financial infrastructures."[23] However, when considering cyberspace warfare, a strike does not need to violate non-combatant immunity or amount to the wide spread destruction of a kinetic strike. For example, in 2010 a computer worm (malware that replicates itself without human interaction) called STUXNET was responsible for the destruction of a significant number of centrifuges being used in the Iranian nuclear industry. The worm targeted components within numerous centrifuges and its control software which provided unexpected commands resulting in self destruction, all the while providing a return loop of normal operating system values to users. It took Iranian officials' months to determine why the centrifuges were failing which ultimately disabled the nuclear reactor and forced a shut down for an estimated 1 year. Moreover, the virus was programed to "evaporate" once the task was completed with no further damage incurred. Whilst the virus disappeared from its target, it infected hundreds of thousands of computers worldwide and the worm remains active across the Internet. Had a traditional approach to warfare been engaged, a kinetic attack would have involved the loss of many lives, both military and civilian.[24]

Currently, there is no definitive universal law or agreement that addresses the ethical dilemma associated with conducting Cyberspace Operations as part of Cyber Warfare. JWT, as a theory of ethics, levies the moral requirements of right intention and probability of success through which we may identify aspects of cyber-attacks that do not conform with the war rules traditionally applied to regular, physical warfare. These

[23] John Arquilla, "Ethics and Information Warfare," in *Strategic Proposal: The Changing Role of Information Warfare*, ed Zalmaym Khalilzad and John P White, (California: RAND Corporation., 1999), 388.

[24] Australian Defence Force, *ADDP 3.24 Cyberspace Operations*, (Canberra: Department of Defence, 2020).

aspects have been identified as technological aggression, anonymity of cyber weapons, subjective interpretation of intent, unintended proliferation, and the fundamental targeting of basic societal infrastructure. Therefore, in the absence of an agreed legal framework to determine if/what aspects of cyber may constitute a justifiable act of war and subsequent war fighting, a nuanced approach to ethical decision making is recommended to bridge the gap.

ETHICS

Coleman defines ethics " [as] a branch of philosophy which examines questions about human conduct, specifically addressing questions of what is right and wrong, just and unjust, virtuous and non-virtuous in such conduct." [25] Following this logic, any decision that involves an ethical component may be surmised as an ethical decision. International law and LOAC, as influenced by JWT, have been identified as the fundamental instruments by which the ADF adhere regarding ethical decision making, in relation to going to war (*jus ad bellum*) and war fighting (*jus in bello*). When examining these laws, regulations and theories it is also important to understand the broader societal conditions that permit a military to control the use of legitimate force. Conley and Ouellet offer "for a group of people to have the monopoly over legitimate means of violence (i.e. the armed forces), it must be seen as *deserving* such a *privilege* if it wants to keep a monopoly without facing challenges from its parent society".[26]

Conley and Ouellet further reference Richard Scott's institutional analysis framework as a guide to understanding how a military's legitimacy and that of its leaders

[25] Stephen Coleman, "Ethical Dilemmas and Tests of Integrity," in *Key Concepts in Military Ethics*, ed Deane-Peter Baker, (Sydney: NewSouth Publishing, 2015), 8.

[26] Devin Conley and Eric Ouellet, "The Canadian Forces and Military Transformation an Elusive Quest for Efficiency", *Canadian Army Journal* vol 14.1 (2012): 71.

may be influenced by societal norms and behaviors. The framework considers how three pillars of institutional legitimacy - Regulative, Cognitive and Normative may shape a military and the actions of its leaders. Collectively the pillars consider

> both the written and unwritten rules within an institution that can be invoked for justifying and legitimizing a decision…common thought patterns and world views within an institution serve to maintain social cohesion and legitimacy…how both values and norms are deeply embedded in the ethical notions "good" and "evil" provide a powerful way to justify and legitimatize decisions.

Society and politics can shape law, and as "law influences politics through legal structure and traditions", all collectively shape a military's purpose and strategic intent.[27] Additionally, as a military that supports the rules-based international order, the ADF's approach to warfare may be further influenced by regional security, trade agreements, immigration protocols and cultural arrangements.[28]

Therefore, when gaps in legislation and ethical guidance regarding warfare and *jus ad bellum* and *jus in bello* are created due to advances in technology, such as Cyberspace operations, ADF institutional alignment and practices are subject to a restricted and outdated focus. By understanding the essence and ethical limitations of JWT and legislation in the Cyberspace domain, ADF Cyberspace Commanders will be better placed to consider supplementary frameworks for legitimate and moral decision making which also consider broader societal and government principles.

[27] Goldstein, Evan, Law Shapes Politics: How Legal Structure Influences Political Discourse and Policymaking at All Levels of Governance (October 23, 2014). Available at SSRN: https://ssrn.com/abstract=2514055 As previously established the ADFs purpose and strategic intent for Cyberspace Operations is articulated through the 2016 Defence White Paper and Strategic Policy Statements

[28] United Nations Association of Australia, *The United Nationals and The Rules-Based International Order.* Last accessed 15 April 2020. https://www.unaa.org.au/wp-content/uploads/2015/07/UNAA_RulesBasedOrder_ARTweb3.pdf

As previously argued, JWT does not sufficiently consider the ethical nuance of Cyberspace warfare. Taddeo contends this is the case due to JWT focusing on "the use of force in international contexts and surmises sanguinary and violent warfare occurring in the physical domain."[29] Moreover, JWT "[focuses] on human rights and disregards all non-human entities… [and therefore] does not provide sufficient means for addressing [cyberspace warfare]."[30] Dipert propels this view further concluding "that cyber conflict is so utterly unlike conventional war, and its weapons and tactic so novel and unprecedented, that an entirely new regime of governance is called for."[31] A more measured approach, or assessment of the situation, is perhaps offered by Denning and Strawser who propose the applicability of cyber weapons is open to interpretation due to the JWT principles governing LOAC predating cyberspace capabilities.[32] The shared conclusions affirm that JWT alone is not a coherent framework for evaluating Cyberspace Warfare.

The international and collaborative creation of the '*Tallinn Manual*' further supports the view that there are deficiencies in JWT and international law in relation to cyberspace warfare. The *Tallinn Manual*, as a product "results from an expert-driven process designed to produce a non-binding document applying existing law to cyber warfare'.[33] The process focused on whether or not existing laws, both International and

[29] Mariarosaria Taddeo, "Just Information Warfare," in *Ethics and Policies for Cyber Operations*, ed Mariarosaria Taddeo and Ludovica Glorioso, (Switzerland: Springer International Publishing., 2017), 73.

[30] *Ibid*.

[31] George R. Lucas, "Permissible Preventative Cyberwar: Restricting Cyber Conflict to Justified Military Targets," in The *Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing., 2014), 75

[32] Dorothy E. Denning and Bradley J. Strawser, "Moral Cyber Weapons," in *The Ethics of Information Warfare*, ed Luciana Floridi and Mariarosaria Taddeo, (Switzerland: Springer International Publishing, 2014), 86.

[33] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable To Cyber Warfare* (New York: Cambridge University Press, 2013) 16. In 2009, the NATO Cooperative Cyber Defence Centre of

LOAC, applied to cyber warfare, and if so, how? Particular, attention was paid to complex legal issues surrounding cyber operations involving *jus ad bellum* and *jus in bello*.[34] However, the *Tallinn Manual* is limited to providing specialist guidance that assists in understanding the complexity of cyber operations, as separate to kinetic operations. An international regulatory framework that heeds a just war approach and LOAC for Cyberspace warfare remains nonexistent. As evidenced by academic and subject matter expert views, the author advocates that current international law, as situated by JWT, is not sufficient in assessing the unique ethical complexities of cyberspace warfare. Prior to exploring a proposed framework to address JWT insufficiencies, the author identifies the following to be the most prominent challenges faced by emergent Cyber Commanders in the ADF.

Ethical Complexities of a Cyber Commander

As with all other military missions, Cyberspace operations must be conducted in accordance with appropriate domestic and international authorities, such as military orders, government policy, ROE and status of forces agreements. Additional guidance as provided by the Tallinn Manual, recognizes significant differences in linguists, legal foundations and authorities between nations, regarding the non-physical nature of Cyberspace operations. Further, undetected or unforeseen linkages in cyberspace make calculating second and third-order effects of a cyberspace operation difficult to predict. Therefore, it is imperative that Commanders, planners and operators understand the

Excellence invited an international group of experts to produce a guidance manual on the law governing cyber warfare. The manual is not an official document and does not represent the views of NATO – it remains an academic study conducted by experts.

[34] *Ibid*., 18-19. The Tallinn Manual addresses both international and non-international armed conflict. It indicates when a particular Rule is applicable to both categories of conflict, limited to international armed conflict, or of an uncertain application of both. The manual is not intended for use in considering kinetic to cyber operations – this is already covered by LOAC.

relevant legal framework and comply with the core principles of military necessity, proportionality, distinction and unnecessary suffering when conducting cyberspace operations.[35] From an ADF perspective, the most ethically challenging Cyberspace issues for commanders are proposed as: subjective interpretation of intent; technological aggression; anonymity of cyber weapons; unintended proliferation; and the targeting of basic infrastructure.

Subjective Interpretation of Intent

Can Cyberspace warfare be undertaken ethically? In determining an answer, Miron contends just cause, proportionality and discrimination must be answered in conjunction with determining if the use of traditional forms of military force may be used in retribution, or whether it is more appropriate to launch a counter cyber-attack.[36] Therefore, in the absence of a framework that provides a moral value to a non-physical entity i.e. national IT network, a commander is required to determine the intent of a cyber-attack, based on one's own interpretation. Leading to further consideration as whether one should respond in kind or consider a preemptive defensive strike against an *assumed* timely, kinetic attack.

Technical Aggression

Will the use of non-physical force lead to physical damage, loss of life, or be more damaging than a kinetic attack? Determining the immediate or consequential effects of a cyberspace operation requires a commander to be aware of possible physical and non-physical effects. Scope of consideration should also include the permanency of effects.

[35] Australian Defence Force, *ADDP 3.24 Cyberspace Operations*, (Canberra: Department of Defence, 2020).

[36] Marina Miron, "Cyber Warfare," in *Key Concepts in Military Ethics*, ed Deane-Peter Baker, (Sydney: University of New South Wales Press Ltd, 2015), 227.

ADF Cyberspace doctrine affirms permanency of effects as particularly crucial to the planning of offensive cyberspace operations, as it determines how long an effect maybe applied.[37] Permanent effects risk a response from an adversary or proliferation while non-permanent effects may be recalled, recovered or terminated resulting in lower risk to undesired consequences or retaliation.

Anonymity of Cyber Weapons

Cost effective and rapid, Cyberspace's unregulated and limitless bounds make cyber operations "an attractive instrument of aggression".[38] Teamed with the advantageous ability to operate anonymously within the Cyberspace domain, inability for attribution and whether or not a cyberspace activity was an attempt at misdirection is as complex as it is subjective.

Unintended Proliferation

Cyberspace operations have the potential to result in either intended or unintended kinetic effects beyond a commander's targeted scope. Miron contends unintended effects are highly susceptible to violating the principles of proportionality and discrimination. For example, malware could inflect an International Air Traffic Control system that supports both military and civilian activities, leading to an aircraft crash in which civilians would die.[39]

[37] Australian Defence Force, *ADDP 3.24 Cyberspace Operations*, (Canberra: Department of Defence, 2020).

[38] Marina Miron, "Cyber Warfare," in *Key Concepts in Military Ethics*, ed Deane-Peter Baker, (Sydney: University of New South Wales Press Ltd, 2015), 226.

[39] *Ibid*., 229.

Targeting of Basic Infrastructure

Depending upon the strategic and operational situation, an order or applicable ROE may limit cyberspace operations to actions that are likely to result in no or low levels of collateral effects i.e. striking of an adversary's electrical power and communication networks. Limiting the damage and destruction of dual use targets such as basic infrastructure also requires a Commander to understand aspects of the targeted environment in relation to cultural and social norms and economical drivers.[40] Additional consideration by the ADF would also include adherence to enforceable determinations such as United Nations Security Council Resolutions (UNSCR) which may uniquely impact operational or targeting considerations of a Commander i.e. UNSCR 1325 recognizes the changing nature of warfare in which civilians, in particular women and girls, are increasingly targeted and differentially impacted during conflict.[41]

Commanding cyberspace operations requires the innate ability to deconflict multiple activities across physical and informational networks. This requires a command and control capability that can rapidly consider the ethical implications of possible cyber effects at a tempo that matches cyberspace operations. As with kinetic warfare, "effects and intentions are the desiderate for moral evaluation of cyber war".[42] As a result, the author proposes an alternate theory of ethics, known as Information Ethics, be considered as a supplement to JWT to address the identified challenges of commanding and leveraging non-physical entities within the cyberspace domain. With the training in and

[40] Dual use target refers to an object or entity used both a military and civilians.

[41] Resolutions by the Security Council are legally binding . Article 25 of the Charter states that "The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter" United Nations Charter (1945), article 25.

[42] Colonel James Cook, "Just War under CyberGaia," Routledge Handbook on Military Ethics. (2015): 421- 43, http://ebookcentral.proquest.com

application of Information Ethics, Cyberspace Commanders will be better placed to make legitimate and ethical decisions which consider international peace and security requirements and societal and government pressures,

Information Ethics

With the information revolution we witnessed a shift, that has brought the non-physical domain to the fore, and has made it as important and valuable as the physical one. Subsequently, the development and use of new technologies such as cyber raise a number of ethical issues that are not captured by JWT or international law. Information Ethics is a macro-ethics, which is concerned with the whole realm of reality and provides an analysis of ethical issues by endorsing an informational perspective – it attributes a moral value to all the existing entities (both physical and non-physical).[43] The moral value of an entity is further defined by the "potential contribution to the enrichment and the flourishing of the informational environment – [the Ionosphere]." [44] Consisting of all, the ionosphere considers entities and the relationships between them. As with all relationships, the health of the Ionosphere is assessed by its ability to flourish or its level of corruption or destruction. "Information ethics considers the duty of any moral agent in the information environment, and any action that affects the environment through corruption or damaging informational objects as an occurrence of entropy."[45]

Based upon this theory, Information Ethics draws on four principles to identify the actions of right and wrong by a moral entity. It determines that Ionospheric entropy: ought not be caused, ought to be prevented, and ought to be removed to ensure the

[43] Mariarosaria Taddeo, "Just Information Warfare," in *Ethics and Policies for Cyber Operations*, ed Mariarosaria Taddeo and Ludovica Glorioso, (Switzerland: Springer International Publishing., 2017), 78.

[44] *Ibid*., 79

[45] *Ibid*., 80. Entropy is defined as a decline into disorder.

preservation and flourishment of all informational entities.[46] The four principles of Information Ethics enables us to consider all entities affected by an act of military force as a moral recipient. Following information ethics theory, the moral value of an action is quantified based on its effect regarding a recipient's existence and its ability flourish which in turn enables prosperity of the ionosphere. When drawing a parallel to Cyberspace operations, Information Ethics enables us to consider how to avoid damage or destruction to non-physical entities vice physical objects alone.

As entropy ought to be prevented and/or removed within the Ionosphere, the offensive measure of targeting malicious cyberspace entities may be deemed legitimate and just. Consequently, Information Ethics enables us to identify and consider the non-physical aspects of Cyberspace operations through a more comprehensive lens. Information Ethics extends the scope of JWT by providing an ethical framework through which a Cyberspace Commander may consider the maintenance, engagement and destruction of non-physical objects, vice physical warfare alone.

ADF CYBER WORKFORCE

> *Resources must be allocated for the education and training, and equipping of cyber warriors, including both individual and collective training, as well as simulation systems.*
>
> - Brigadier Marcus Thompson, *The ADF and Cyber Warfare*

In response to policy settings in the Defence White Paper 2016, the ADF is establishing the organisation, training and capabilities required to fight and win in the information environment. In 2017, the ADF established Information Warfare Division (IWD) as a means to "combat threats to Australia's national interests in the information

[46] *Ibid*.

environment".[47] IWD consists of five branches: Information, Surveillance, Reconnaissance, Electronic Warfare and Cyber (ISREW & Cyber), Space and Communications, Joint Command and Control (JC2), Defence Signals Intelligence and Cyber Command (DSCC), and Joint Influence Activities Directorate. Following the formal establishment of IWD, on 01 July 2017, the Joint Cyber Unit (JCU) was created to plan and conduct both offensive and defensive cyberspace operations and support the normalization of cyberspace operations in the ADF.

Cyberspace warfare, as a new and emerging capability, required the implementation of new employment groups created from both within the ADF's existing workforce and through targeted selection of skilled candidates both civilian and military. Subsequently, the ADF Cyberspace Workforce project commenced in January 2018 and remains tasked with the design and implementation of common workforce methods, approaches and practices to deliver a high-caliber cyber workforce to meet the needs of the ADF. Key drivers of the workforce project include: an integrated and interoperable cyberspace workforce that can support joint, Whole of Government and Allied operations while meeting industry standards; and a "high caliber, healthy and diverse talent pipeline to ensure the cyberspace workforce can contribute effective to the ADF mission".[48]

Education and Training

To guide workforce and training practices, the ADF utilizes a Cyberspace Professional Framework. The ADF framework, while based on the National Initiative for

[47] Department of Defence - Joint Capabilities Group, "Information Warfare Division," last accessed 28 April 2020, https://www.defence.gov.au/jcg/.iwd.asp

[48] Department of Defence – Joint Capabilities Group. ADF Cyberspace Workforce Project Plan (classified source).

Cybersecurity Education (NICE) that supports working at a Whole of Government level, has modified its approach to an Australian military context.[49] The framework consists of functions, roles, tasks, knowledge and skills and acts as the ADF standard. It is a holistic tool that articulates both core technical expertise, and all supporting and enabling functions for the cyberspace workforce.

To enable personnel to achieve the capability requirements of an employment group, ADF workforce planning methodology includes a Learning Requirements Specification (LRS) to specify the workplace tasks that require implementation of formal learning and development activities. The LRS in conjunction with the Employment Profile (EP) and the Training and Assessment Strategy (TAS) form the Cyber Warfare Personnel Development Strategy. Due to ADF Cyberspace capability occurring within the classified realm, the full extent of training objectives cannot be broached in this paper. Following a collective review of ADF workforce documents pending endorsement and/or approval it remains clear that cyber presents new challenges not covered by traditional learning models such as Employment Training or Professional Military Education (PME).[50] As established throughout this paper, one of the most prominent challenges in the cyberspace environment pertains to the ethical decision making of Commanders.

[49] Australian Cyber Security Growth Network, "National Initiative for Cybersecurity Education (NICE) Workforce Framework," last accessed 30 April 2020, https://www.austcyber.com/resources/dashboards/NICE-workforce-framework
The workforce framework as established by NICE establishes a "taxonomy and common lexicon that describes cyber security work…it includes the knowledge, skills, abilities and tasks of cyber security roles".

[50] Activities/ areas reviewed: cyber employment tasks, performance levels required, the difficulty/importance and frequency of tasks, Initial Employment Training and Learning and Development activities, Professional Military Education and experienced based job training.

Due to impending training methodology and guiding frameworks, future Cyberspace Commanders will be more technically apt in relation to cyberspace operations. Yet, at this time, there appears to be no specified approach as to how cyber ethics may be addressed and cultivated outside of traditional warfare education. The importance of educating military leaders "to cope with ethical, legal and political challenges" associated with Cyber warfare was identified as early as 2010 at the 10th Annual McCain Conference on Military Ethics and Leadership, US Naval Academy, 22-23 April 2010.[51] The conference identified significant ethical cyber concerns relating to attribution, misperception, mistaken retaliation, unpredictable effects, and indiscriminate or disproportionate actions. Significantly, recommendations were made in relation to PME to address the concerns identified. The recommendations proposed the sharing of Allied and partner course curriculum and sources in relation to ethics, law and leadership, and inclusion of elective courses in non-technical PME to "develop an informed assessment of [cybers] promise and prospects" to prepare military leaders for complex and challenging decision making in the Cyberspace domain.[52]

As proposed, the joint training framework for Cyberspace Warfare is not yet mature enough to distinguish its approach to understanding the ethical considerations associated with Cyberspace warfare. Noting this proposed deficiency and the McCain Conference recommendations, providing Commanders with a form of education in

[51] LtCol Edward Barrett, "Executive Summary and Command Brief," Journal of Military Ethics Vol.9, No. 4 (2010): 424-431, https://doi.org/10.1080/15027570.2010.54089 The Conference was convened to address potential ethical issues associated with emergent military capability including cyber warfare. Opinions and findings were garnered from leading world experts and educators from nation service academies and war colleges to discuss ethical and leadership challenges associated with identified technologies.

[52] *Ibid*.

relation to Information Ethics is key. It is fundamental the ADF provide training and education on Information Ethics. While Information ethics will enable a commander to develop the intellectual scrutiny required to assess the moral value of an entity based on its informational nature, Schoonhoven cites "real ethical teaching requires engaging with issues in a critical way".[53] Therefore, the training must include hands-on, practical and timely decision making within Cyber operations to familiarise and educate Commanders. As to the medium in which the ADF may deliver training i.e. a full synthetic cyber warfare training environment, to gap the void in ethics education for the cyberspace workforce, this falls outside of the scope of this paper.[54]

CONCLUSION

This paper has explored the theoretical basis of JWT in relation to Cyber as a fifth dimension. It has concluded that there is a clear need for improved conceptual grounding for new ethical regulations, education and training in the ADF. Cyberspace threats are dynamic in that they can rapidly emerge, transform and are persistent. It was determined, that while JWT principles remain valid in traditional warfare, they are insufficient in the evolving domain of cyberspace. This is due to JWT focusing on use of force in international contexts and violent warfare in the physical domain. In the Cyberspace environment, JWT becomes less direct and intuitive, highlighting ethical issues associated with the possible declaration of war. While the unique issues of Cyberspace operations are explored and comprehensively considered in subject matter expert guidance such as

[53] Richard Schoonhoven, "The Ethics of Military Ethics Education," Routledge Handbook on Military Ethics. (2015): 49, http://ebookcentral.proquest.com

[54] Full synthetic Cyber Warfare training environments may include but are not limited to the combinations of simulated cyber operations, live and virtual applications and equipment and kinetic warfare training simulators

the *Tallinn Manual,* an agreed international regulatory framework remains nonexistent. As a result, the application of Information Ethics is proposed as a solution for bridging the divide between JWT principles and Cyberspace warfare. Information Ethics theory will move current ethics training beyond that of JWT and the consideration of societal and political influences, to provide a holistic and current approach for inclusion within the joint training framework for the cyber workforce. Through providing education in Information Ethics, Cyberspace Commanders will be better placed to make rapid and ethical decisions in relation to cyberspace-based effects in multidimensional warfare.

BIBLIOGRAPHY

Australian Cyber Security Growth Network. “National Initiative for Cybersecurity Education (NICE) Workforce Framework,” last accessed 30 April 2020. https://www.austcyber.com/resources/dashboards/NICE-workforce-framework

Australia. Department of Defence. ADDP 3.24, *Cyberspace Operations*. Canberra: Department of Defence Australia, 2020.

Arquilla, John. “Ethics and Information Warfare.” In *Strategic Appraisal: The Changing Role of Information Warfare*, edited by Zalmaym Khalilzad and John White, 379-401. California: RAND Corporation, 1999. https://www.rand.org/pubs/monograph_reports/MR1016.html

Barrett, Edward. “Executive Summary and Command Brief,” Journal of Military Ethics Vol.9, No. 4 (2010): 424-43. https://doi.org/10.1080/15027570.2010.54089

Baylon, Caroline. “Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare.” in *Ethics and Policies for Cyber Operations*, edited by Mariarosaria Taddeo and Ludovica Glorioso, 213-230. Switzerland: Springer International Publishing, 2017.

Coleman, Stephen. “Ethical Dilemmas and Tests of Integrity,” in *Key Concepts in Military Ethics*, edited by Deane-Peter Baker, 8-11. Sydney: NewSouth Publishing, 2015.

Collier, Jamie. “Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom.” In *Ethics and Policies for Cyber Operations*, edited by Mariarosaria Taddeo and Ludovica Glorioso, 187-212. Switzerland: Springer International Publishing, 2017.

Conley, Devin and Eric Ouellet. “The Canadian Forces and Military Transformation an Elusive Quest for Efficiency.” *Canadian Army Journal* vol 14.1 (2012) 71-83.

Cook, James. “Just War under CyberGaia,” Routledge Handbook on Military Ethics. (2015): 421- 431. http://ebookcentral.proquest.com

Cornish, Paul. “Deterrence and the Ethics of Cyber Conflict.” in *Ethics and Policies for Cyber Operations*, edited by Mariarosaria Taddeo and Ludovica Glorioso, 1-16. Switzerland: Springer International Publishing, 2017.

Denning, Dorothy E and Bradley J Strawser, “Moral Cyber Weapons,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 85-103. Switzerland: Springer International Publishing, 2014.

Department of Defence - Joint Capabilities Group. “Information Warfare Division,” last accessed 28 April 2020, https://www.defence.gov.au/jcg/.iwd.asp

Dipert, Randall R. “The Future Impact of a Long Period of Limited Cyberwarfare on the Ethics of Warfare.” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 25-37. Switzerland: Springer International Publishing, 2014.

Goldstein, Evan, Law Shapes Politics: How Legal Structure Influences Political Discourse and Policymaking at All Levels of Governance (October 23, 2014). Last accessed 22 April 2020. SSRN: https://ssrn.com/abstract=2514055

Happa, Jassim., and Graham Fairclough. “A Model to Facilitate Discussions About Cyber Attacks.” in *Ethics and Policies for Cyber Operations*, edited by Mariarosaria Taddeo and Ludovica Glorioso, 169-185. Switzerland: Springer International Publishing, 2017.

Howard, Don. “Virtue in Cyberconflict,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 155-168. Switzerland: Springer International Publishing, 2014.

Hywel Evans, Andrew Williams. “ADF Offensive Cyberspace Operations and Australian Domestic Law: Proprietary and Constitutional Implications.” Federal Law Review. 2019 Vol 47 No 04. Last accessed 01 April 2020. https://doi.org/10.1177/0067205X19875011

Jody M. Prescott. “Building the Ethical Cyber Commander and the Law of Armed Conflict.” Rutger Computer and Technology Law Journal 40. 2014 No 1.

JSTOR, “Strategic Proposal: The Changing Role of Information Warfare,” last accessed 05 March 2020, https://www.jstor.org/stable/10.7249/mr1016af.21

Lee, Steven P. “The Ethics of Cyberattack,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 105-122. Switzerland: Springer International Publishing, 2014.

Lin, Patrick., Fritz Allhoff., and Keith Abney. “Is Warfare the Right Frame for the Cyber Debate.” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 39-59. Switzerland: Springer International Publishing, 2014.

Lucas, George R. “Permissible Preventative Cyberwar: Restricting Cyber Conflict to Justified Military Targets,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 73-83. Switzerland: Springer International Publishing, 2014.

McCormack, Wayne., and Deen Chatterjee. “Technology, Information, and Modern Warfare: Challenges and Prospects in the 21st Century.” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 61-70. Switzerland: Springer International Publishing, 2014.

Miron, Marina. “Cyber Warfare,” in *Key Concepts in Military Ethics*, edited by Deane-Pater Baker, 225-230. Sydney: University of New South Wales Press Ltd, 2015.

Orend, Brian. “Fog in the Fifth Dimension: The Ethics of Cyber-War.” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 3-23. Switzerland: Springer International Publishing, 2014.

Ormrod, David, and Benjamin Turnbull. “The cyber conceptual framework for developing military doctrine.” Defence Studies. 2016 Vol 16 No 03. Last accessed 02 March 2020. http://doi.org/10.1080/14702436.2016.1187568

Ramsey, Benjamin. *An Ethical Decision Making Tool for Offensive Cyberspace Operations*. Air and Space Power Journal. Fall 2018. Last accessed 05 March 2020. http://www.airuniversity.af.mil/ASPJ/

Rocini, Marco. “Military Objectives in Cyber Warfare.”. in *Ethics and Policies for Cyber Operations*, edited by Mariarosaria Taddeo and Ludovica Glorioso, 99-114. Switzerland: Springer International Publishing, 2017.

Schoonhoven, Richard. “The Ethics of Military Ethics Education,” Routledge Handbook on Military Ethics. (2015): 47- 53. http://ebookcentral.proquest.com

Schmitt, Michael N. *Tallinn Manual on The International Law Applicable To Cyber Warfare* (New York: Cambridge University Press, 2013).

Simpson, Thomas W. “The Wrong in Cyberattacks,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 141-154. Switzerland: Springer International Publishing, 2014.

Stallard, Craig. *At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force*. Commonwealth of Australia. 2014.

Taddeo, Mariarosaria. “Information Warfare and Just War Theory,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 123-138. Switzerland: Springer International Publishing, 2014.

Taddeo, Mariarosaria, and Ludovica Glorioso. *Ethics and Policies for Cyber Operations*. Switzerland: Springer International Publishing, 2017.

Taddeo, Mariarosaria. “Just Information Warfare.” in *Ethics and Policies for Cyber Operations*, edited by Mariarosaria Taddeo and Ludovica Glorioso, 67-85. Switzerland: Springer International Publishing, 2017.

United Nations Association of Australia, *The United Nationals and The Rules-Based International Order*. Last accessed 15 April 2020. https://www.unaa.org.au/wp-content/uploads/2015/07/UNAA_RulesBasedOrder_ARTweb3.pdf

Vallor, Shannon. “Armed Robots and Military Virtue,” in *The Ethics of Information Warfare*, edited by Luciana Floridi and Mariarosaria Taddeo, 169-185. Switzerland: Springer International Publishing, 2014.

Wardrop, Christopher. *Bridging the Gap Between Cyber Strategy and Operations: A Missing Layer of Policy*. Australian Defence Force Journal. 2018 Issue No 204.