The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios [1]

Abstract

Cyber attack against Critical National Infrastructure is a developing capability in state arsenals. The onset of this new instrument in national security has implications for conflict thresholds and military ethics. To serve as a legitimate tool of policy, cyber attack must operate in accordance with moral concerns. To test the viability of cyber attack, this paper provides a new perspective on cyber ethics. Cyber attack is tested against the criteria of the Common Good. This involves identifying the four core components of the common good from a conflict perspective: respect for the person; social wellbeing; peace and security; and solidarity. The fate of these components is assessed in relation to the six key characteristics of cyber attack from a moral standpoint: security; the role or absence of violence; discrimination; proportionality; cyberharm; and the threshold of conflict. It is concluded that the common good must be incorporated into developing state cyber strategies.

Introduction

Cyber intrusion is a daily occurrence. Government and business networks are probed millions of times a day (Work 2015: 1). [2] For the most part, these attacks

[1] This research was conducted as part of the ESRC-funded project 'Common Good: Ethics and Rights in Cyber Security'.

are a criminal problem or an expensive inconvenience. To be sure, the economic costs of cybersecurity are considerable. The global cybersecurity industry is estimated to be worth somewhere between $80 billion and $150 billion annually (Singer and Friedman 2014: 163). Nonetheless, aside from the most serious espionage operations and attempts at political interference, most cyber incidents do not individually threaten national security. However, another form of cyber attack has been developing. Evidenced in incidents such as Stuxnet, Shamoon, Wiper, Bronze Soldier, BlackEnergy and Energetic Bear, states are acquiring the ability to conduct significant cyber attacks against Critical National Infrastructure (CNI) and high-value targets. The effects of this new form of attack are normally restricted to the virtual domain. Yet, as the Stuxnet operation against the Iranian nuclear programme reveals, the effects of an attack can extend to the physical realm. Stuxnet destroyed 984 Iranian centrifuges (Zetter 2014, Lindsay 2013). Moreover, socio-economic wellbeing is increasingly dependent upon a complex symbiotic relationship between the informational and physical domains.

As this new form of offensive power embeds itself in national security policy, the many implications for international security must be discussed. One important debate surrounds the strategic utility of cyber attack. Whether or not it represents an effective means to pursue policy is open to question (Brenner & Lindsay 2015, Gartzke 2013, Rid 2012, Valeriano & Maness 2015, Lonsdale 2016). Additionally,

[2] The security challenge is only going to increase with the development of ‘the Internet of things’, ‘next billion users’ and increasing exploitation of ‘zero-day exploits’.

as governments fire up their offensive capabilities the ethics of cyber attack and the impact on the causes of conflict must be properly addressed. This is especially important because cyber attack is seen in some quarters as a less dangerous, more acceptable alternative to traditional forms of war (Valeriano & Maness 2015: 75). Indeed, cyberwar is being promoted as an ideal form of war (Jenkins 2016: 89), waged with 'purely ethical weapon[s]' (Lucas 2016: 28). Left unchallenged, such claims could lead to cyber attack being regarded as a new and more potent form of virtuous war, with all of the attendant dangers (Banta 2011, Der Derian 2000 & Ignatieff 2000). Thus, the moral claims surrounding cyberwar need to be tested. It is one thing to develop a cyber offensive capability, but to be a legitimate instrument of national security cyber attack must fulfil certain moral criteria.

Initial discussion on the ethics of cyber attack has tended to fall within two complementary perspectives. The first applies the established war convention to cyberwarfare (Walzer 2015). This approach takes both a legal and moral philosophical approach. The legal approach is most comprehensively outlined in the *Tallinn Manual* (Schmitt 2013). Other notable authors in the war convention mould, many of whom inject a moral philosophical component, include Rowe (2007), Henschke and Lin (2014), and Jenkins (2016). In general, the war convention approach equates to applying the principles of *jus ad bellum* and *jus in bello* to cyberwar, focusing on such issues as proportionality, discrimination, and what constitutes the threshold of 'armed attack' in the cyber domain. Leading works in this field include, *Binary Bullets: The Ethics of Cyberwarfare*; *Cyberwar: Law and Ethics for Virtual Conflicts* (Allhof, Roff, and Strawser 2016); and *Ethics* *and Cyber Warfare* (Lucas 2017). The second perspective seeks to provide a new normative framework, redefines casus belli, identifies the moral value of virtual and informational objects, and introduces the concept of 'cyberharm'. Leading exponents of this approach are Mariarosaria Taddeo (2014) and Randall Dipert (2010).

Both of these approaches have promoted important developments in the embryonic cyberwar ethics discourse. Despite this, neither of these approaches deals effectively with cyber post-bellum considerations. [3] Consequently, this paper builds upon the existing perspectives and presents a third original approach, one that provides a more comprehensive understanding of the moral implications of cyber attack. In this way, the paper makes a much-needed contribution to advance what Randall Dipert (2016: 59) termed a 'full ethics of cyberwarfare'. This new approach is centred on the 'common good'.

[3] Notable exceptions being Brian Orend's work, 'Postcyber: Dealing with the Aftermath of Cyberattacks', in Fritz Allhoff, Adam Henschke, Bradley Jay Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare*, (Oxford: Oxford University Press, 2016) and a Masters thesis, Maribel Cisneros, *Cyber Warfare: jus post-bellum*, (Naval Postgraduate School, Monterey, California, 2015), http://calhoun.nps.edu/bitstream/handle/10945/45169/15Mar_Cisneros_Maribel.pdf?sequence=1&isAllowed=y

In the complex world of policy choice, the common good provides an effective analytical framework that enables us to appreciate the moral implications of policy action at both the individual and community level. Moreover, conceptions of the common good are especially relevant to the increasing focus on jus post bellum (Bellamy 2008, Orend 2007, Lasiello 2004, Williams and Caldwell 2006). In this sense, the common good provides a broader and longer-term appreciation of the effects of policy actions. The common good has a long history in political thought. It encompasses the work of Aristotle, St. Augustine, St. Thomas Aquinas, British Idealism (especially T.H. Green), Kant, the contractual approach (found in Rawls and Rousseau), and the social doctrine of the Catholic Church. In particular, the latter invoked the notion of 'a global common good' (Hehir 2007: 17). Despite this venerable heritage, the common good is underused in ethical discourse.

In order to establish this new approach to cyber ethics, the paper begins by identifying the four core components of the common good: respect for the person (premised on the right to life); social wellbeing (requiring functioning essential infrastructure); peace and security; and solidarity (within and between states). The fate of these components will be assessed in relation to the six key characteristics of cyber attack from a moral standpoint: security; the role or absence of violence; discrimination; proportionality; cyberharm; and the threshold of conflict.

The main body of the paper is then structured around the six characteristics of cyber attack, and analyses the various ways by which cyber attack both promotes and undermines the core components of the common good. The fate of the four components will be summarised in the concluding section of this paper. Based on this analysis, we can then assess whether the common good will suffer or prosper in an age of cyber attacks. In turn, this speaks to the moral implications of cyber attack, the impact of virtual interactions on the prospects for peace and conflict in international security, and the legitimacy of cyber attack as a tool of policy.

Conceptual Basis for the Analysis

The common good is a suitable instrument in our efforts to understand the moral standing of policy action: 'The global common good bridges ethical obligation and policy practice.' (Fuchs and Buckley 2007: 6) For the purposes of this paper, the four mutually reinforcing core components of the common good are largely based on Catholic social teaching and British Idealism (Libreria Editri Vaticana 1994: 1906-1909). It is recognized that conceptions of the common good will differ amongst groups and even individuals. The framework used here has been constructed on the basis that it represents a viable foundation for moral discourse on military ethics (Lonsdale 2016).

At its core, and as a theory for social and political action, the common good seeks the creation of an environment that allows the individual and group to flourish and reach their full potential. For T. H. Green, the common good is an ideal that is worked towards through material goods and services (Nicholson 1990: 58, 81-82). This includes material wellbeing and security (Tyler 2006: 59).

The genesis of the common good is the realization that the human person is the centre of social life. Each person has inalienable rights and freedoms, with the most fundamental being the *right to life* and the right to flourish. Although the rights of the person are central, individualism is rejected: "Do not live entirely isolated, having retreated into yourselves, as if you were already justified, but gather instead to seek the common good together" (Libreria Editri Vaticana 1994: 1905, Tyler 2012: 273). Thus, the common good seeks the harmonious development of both the individual and the *social wellbeing* of the group.

The conditions required for the advancement of the individual and the group must be protected. As evidenced in many recent conflicts, including Iraq, Afghanistan and Syria, the conditions for social justice can be undone by conflict. Hence, *peace and security* are essential enablers of the common good. As a result, security policy will have a critical impact on the fate of the common good. In relation to peace, *solidarity* is a crucial enabler. It is clear from history that conflict can undermine the cohesion of political communities. War can have a similarly disruptive effect on solidarity in the international community. Thus, we see how the four components of the common good interact, that they need maintenance, and how they may be affected by the spectre of conflict.

The six characteristics of cyber attack have been chosen because in some way they all relate either to the outbreak or moral consequences of conflict. In the current epoch, *security* has an important cyber dimension. A new form of state power – cyber power – is exercised to promote security in and through the virtual domain.

As a result, aggressive cyber operations are becoming an increasingly important component of security policy and the pursuit and maintenance of peace (via coercion and deterrence). [4] This raises two questions. Is cyber attack an effective means to pursue security? Does cyber attack threaten stability (and hence security) in international relations? Stability is potentially threatened by the effect of cyber aggression on the *threshold of conflict*.

When considering the moral effects of conflict, the pursuit of policy through *non-violence* is one of the key promises of cyber attack. And yet, the non-violent characteristic of cyber attack may be less absolute and/or more harmful than envisaged. As will be discussed later, escalatory dynamics could push a virtual conflict into the physical realm. Moreover, even if cyber attack remains an informational activity, it can still undermine the common good through the infliction of *cyberharm*. Finally, we can seek to understand the moral consequences of cyber attack within the context of *jus in bello*. Specifically, is cyber attack able to operate in a *proportionate* and *discriminatory* manner? As evidenced below, all of

[4] This is evident, for example, in the UK's 2017 warning to Russia that Britain would respond to cyber intrusions with retaliatory cyber attacks. Jason Groves, 'Boris's Cyber War Threat to the Kremlin', *Mail Online* (21 December, 2017) http://www.dailymail.co.uk/news/article-5204151/Borish-Johnson-Britain-ready-hit-back.html Coercion via cyber attack is discussed in Erica D. Borghard & Shawn W. Lonergan, 'The Logic of Coercion in Cyberspace', *Security Studies*, 26:3 (2017) pp. 452-481.

these characteristics impact in some way on the four core components of the common good, and in doing so have post-bellum implications.

The Six Key Characteristics of Cyber Attack in relation to the Common Good

Security

Peace and security are essential enablers for the other components of the common good. Does cyber attack promote security, and thus contribute to the maintenance of peace? Security now clearly has a cyber dimension. It is axiomatic to claim that social and economic wellbeing is dependent upon the free flow of information across networks. Most critical services are reliant upon computer networks, and E-commerce totals over 10 trillion dollars in annual sales (Singer & Friedman 2014: 15). Thus, for a modern society with aspirations to the common good, cybersecurity is an essential enabler.

Despite considerable efforts to bolster cybersecurity, including a $19 billion *Cybersecurity National Action Plan* in the US (White House 2016) and £1.9 billion investment over the next five years in the UK (HM Treasury 2015), results are somewhat mixed. As illustrated by the Office of Personnel Management and Yahoo hacks, massive data thefts continue to occur in the public and private sectors (Hirschfeld 2015). GCHQ reports that it is monitoring cyber threats from high-end adversaries against 450 companies across the aerospace, defence, energy, water, finance, transport and telecoms sectors (HM Treasury 2015). Thus, it seems that information-reliant states have some way to go to achieve their objective of being secure information environments within which to do business and promote cyber-related development (Cabinet Office 2011).

Evidently, defensive cyber measures are under strain. In this environment, cyber attack has two primary security functions. First, in a bid to preserve security and avoid conflict, cyber attack contributes to deterrence. This is achieved by providing a cyber means of response within a flexible cross-domain retaliatory capability. If, as in the Cold War nuclear standoff, there is mutual vulnerability to cyber attack, then stability (and hence security) may be maintained via Mutual Assured Disruption. Second, and reflecting the interplay of offensive and defensive operations, cyber attack promotes security via damage limitation. The latter refers to a counterforce attack that degrades an enemy's ability to inflict harm, either within or prior to hostilities. 'Search and destroy' and 'offensive security' are emerging cyber capabilities, whereby attackers are identified, tracked and then neutralised with DoS (Denial of Service) attacks or malware (Information Week 2013).

Evidence of state restraint, especially in relation to major cyber attacks, suggests that deterrence may be playing a greater role in cybersecurity (Valeriano & Maness 2015). However, the continued proliferation of low-to-medium threats suggests that deterrence requires even greater levels of flexibility and potency. Thankfully, as reflected in both the US and UK strategies, cyber deterrence is maturing. Increasingly, deterrence includes defensive security measures for denial, norms against aggressive behaviour, and commitment to cross-domain retaliatory capabilities. [5]

Within this new deterrence model, cyber punishment undoubtedly faces a number of challenges (Singer 2015, Lindsay 2015b, Denning 2015, Libicki 2009, Iasiello 2014). Most significantly, cyber retaliation suffers from the attribution problem, blowback, and the difficulty of predicting effects. These challenges reinforce the general point that the reliability of deterrence cannot be guaranteed (Payne 1996). That being said, the attribution problem is being tackled through the development of cyber forensics (Rid & Buchanan 2014, Lucas 2016, Boebert 2011, Tsagourias 2013, Davis et al. 2017). Moreover, the absence of physical violence in cyber attack increases credibility of response, which is crucial for deterrence reliability.

Thus, we can conclude that cyber attack has an important role to play in enhancing deterrence (albeit with no guarantees), thereby increasing security, promoting stability, and ultimately providing the required informational environment for the common good to flourish. And, should deterrence fail, cyber attack can be used for

[5] The latter has been reaffirmed by UK Defense Secretary, Sir Michael Fallon. Ben Farmer, 'Britain Prepared to Use Air Strikes or Send in Troops as Retaliation Against Future Cyber Attack', *The Telegraph*, (28 June 2017) http://www.telegraph.co.uk/news/2017/06/27/cyber-attack-could-lead-military-retaliation-says-fallon/?WT.mc_id=tmg_share_tw

damage limitation, which will help protect the means for individual and social development.

The Role or Absence of Violence

The significance of violence for the common good should not be underestimated. Aside from the obvious point that violence tramples on the most basic rights of the individual; by destroying infrastructure and disrupting the normal functions of society it retards development for the whole community. Moreover, the effects of violence have lasting impact on solidarity in domestic and international political systems. This explains why violence has a unique position in the law of armed conflict. For military action to be classified as an armed attack, violence must be present (Schmitt 2013: 106-7). It is significant; therefore, that cyber attack offers the possibility to pursue policy objectives without recourse to violence. This explains why cyberwar has been described as an ideal form of war from an ethical perspective (Jenkins 2016: 89).

In terms of promoting the common good, non-violent cyber attack protects life and physical infrastructure from lasting damage. In this way, it enables states to pursue their policy objectives with less serious repercussions, even in a relationship marked by conflict. It allows strategy to function through a genuinely limited form of war. In the absence of violence some commentators have even questioned whether cyber attack can be classified as war (Rid 2012). Without violence, escalatory dynamics may be retarded, and the potential repercussions of war subdued. Indeed, the United Nations has never classified a cyber attack as a threat to international peace and security (Schmitt 2013: 69). Moreover, the Bronze Soldier attack on Estonia did not trigger Article 5 of the NATO Treaty. This was only possible because the cyber assault, in the absence of violence, was not classified as an armed attack under international law (Schmitt 2013: 75). That being said, this position may not hold indefinitely. In June 2016, NATO clarified that cyber attacks against member states could trigger Article 5 (Stoltenberg 2016).

The policy and strategic implications of non-violence are potentially profound. Cyber attack radically alters the Just War calculus, to the point that it could be classified as an option of first resort (Arquilla 2016: ix). Without the consequences of violence and destruction, cyber attack could be equated more with diplomatic and economic sanctions, rather than considered a form of war. Some are prepared to go even further, arguing that cyberwar may be always justified (Taddeo 2014: 39), and even obligatory from a moral standpoint (Jenkins 2016: 96).

These radical possibilities are premised on the fact that violence does not occur in cyber attack. We have to recognize, however, that violence may occur, and react accordingly. When classifying a use of force as an armed attack, the laws of armed conflict do not distinguish amongst the means of violence. Kinetic force is not required for action to be classified as armed attack. Resultantly, cyber weapons, just as much as chemical and biological agents, are subject to judgement under the law (Schmitt 2013: 106). Given the right targets, cyber attack can produce casualties, potentially on a large-scale. Disrupting power supplies could affect vulnerable members of society. Attacking nuclear power plants or air traffic control would have obvious consequences for the civilian population. Moreover, once malware is released, it often spreads beyond the initial target. This could produce significant, if unintended, casualties (Rowe 2007). Furthermore, in a world of cross-domain reprisals, a cyber campaign could create new targets for physical expressions of force. IT workers, often civilians contracted to the military, could become legitimate targets if they directly participate in hostilities, even if those hostilities are themselves non-violent (Henschke & Lin 2014, Dunlap 2012, Lin, Rowe & Allhoff 2012).

Stuxnet illustrates the intricacies of this issue. Stuxnet has been variously described as an 'absolute game changer', 'a potent new form of warfare', and even the first purely ethical weapon (Singer & Friedman 2014: 118, Valeriano & Maness 2015: 149). And yet, it was designed to produce destructive effects (Lucas 2016: 28). Although Stuxnet was a virtual weapon, it had dramatic physical effects, destroying 984 Siemens centrifuges. Stuxnet is a clear example of how the virtual can become violently manifest in the physical realm.

Cyber attack has also been used to support the delivery of violence. In Georgia in 2008, Russia used cyber attack to disrupt Georgian communications and logistics (Kello 2013). In the previous year, an Israeli air attack on the Syrian nuclear facility at Kibar used cyber attack to disable Syrian air defense (Singer & Friedman 2014: 127). In Iraq, the Americans have used cyber operations to attack insurgent communications and lead them into ambushes via fake emails (Kaplan 2016: 160).

Finally, the escalatory dynamics of cyber conflict need to be taken in to account. In its formal cyber strategy, the US has made it clear that hostile cyber intrusions may be met with a physical response. Indeed, in the 2018 *Nuclear Posture Review*, the United States declared that nuclear response could follow a devastating cyber attack on the country (Secretary of Defense 2018: 72). Hence, what starts as a potential non-violent conflict could rapidly escalate to a shooting war, including the eventual use of nuclear weapons. If we accept the possibility of this escalatory process, then actions in the virtual domain may actually increase the possibility of violent conflict, rather than reducing or replacing it.

We are left to conclude that the relationship between cyber attack and violence is more complex than initially seems to be the case. When it comes to the effects of violence on the common good, cyber attack provides definite opportunities, but with some important caveats. If a conflict is contained within the virtual domain, the effects of violence on the wellbeing of the individual and community can be avoided. Peace and security can be reestablished with minimal or no physical harm. Yet, caution is warranted, either due to the risk of escalation to physical violence, or because cyber attack promises to intensify the potency of violent force. Cyber attack, it seems, is not immune from the violent and escalatory nature of war (Clausewitz 1989).

Discrimination

To do more good than harm, and therefore to be a legitimate instrument of policy in service to the common good, cyber attack must be controllable. The effects of an attack must be predictable. If this is not the case, there exists the risk that non-combatants could be caught-up in the virtual crossfire, thereby affecting the wellbeing of the individual and/or community. Lt. Gen. Edward Cardon, commanding officer of the cyber campaign against ISIS, is conscious of the fact that 'The military is also grappling with the need to avoid harming civilian or noncombatant networks' (Nakashima & Ryan 2015). Arguably, cyber attack has a greater propensity for poor discrimination than some physical expressions of force.

There are four principal reasons why cyber attack could fail the discrimination test. First, as indicated above, it extends the numbers of combatants and targets. Information networks and services can be considered dual-use technology: 'If they participate in military operations – intentionally or not – employees at Facebook, Google, Apple, Microsoft, Yahoo!, Sprint, AT&T, Vodaphone, and many other companies may find themselves considered "civilians directly participating in hostilities" and therefore legitimate targets of war…' (Henschke & Lin 2014) Even though it may not breach the letter of the law, such a potential widening of the combatant category surely raises concerns about the spirit of a law designed to limit suffering.

Second, discrimination is jeopardised by the fact that for technical reasons cyber attack is difficult to predict and control. Malware often bleeds across networks. Due to the interconnectedness of cyberspace, when it comes to the challenges of discrimination cyber attack is almost in a category of its own. Only large-scale nuclear conflict or an especially potent biological weapon could match the reach of a cyber attack. When malware is released into a network, a chain of events is initiated that is potentially beyond human ability to predict or control. This is evidenced in the Stuxnet operation. The target for Stuxnet was very specific: the Supervisory Control and Data Acquisition (SCADA) system for a particular make of Siemens centrifuges. Additionally, the targeted system was air-gapped, and therefore should have been an isolated target. However, and despite the $300 million price tag and extensive planning, Stuxnet still infected an additional 100,000 computers in 155 countries (Valeriano & Maness 2015: 155). The challenge of discrimination is compounded by the limits of target intelligence. As evidenced by the bombing campaigns of the Second World War, predicting the effects of attacking a certain target set within a complex socio-economic entity is difficult in the extreme (Lonsdale 2004: 135-178).

Third, as an instrument of coercion cyber attack encourages, perhaps even demands, attacks or threats against civilian objects. Whether for deterrence or compellence, coercive forms of strategy must be able to damage that which the enemy values. Historically, this has normally been translated into attacks against critical infrastructure to destroy the will and capability of a society to continue waging war. Widespread disruptive attacks (WDA) provide the ability to attack many crucial sectors of society simultaneously. This would clearly be catastrophic from a discrimination perspective. However, WDA is not the only possible form of coercive cyber attack. In a manner not dissimilar to NATO's Kosovo air campaign, a coercive cyber campaign could seek greater discrimination by targeting the interests of the ruling elite (Daalder & O'Hanlon 2000). In this way, cyber coercion could be conducted as a series of precision raids.

Finally, discrimination could be undermined by the challenges of attribution. When 'authentic state agency is notoriously difficult to ascertain' (Lucas 2016: 19) states may opt for more extreme indiscriminate forms of counterattack. This is compounded by the demands of deterrence. Whilst controlled warfighting for deterrence may be the more credible and effective approach (Lonsdale 2017), there is simplicity to some form of cyber Massive Retaliation or Mutually Assured Disruption. In this way, cyber deterrence could be reduced to threats of a doomsday virus, intended to infect large portions of the information environment.

To be an instrument of discrimination, cyber attack clearly has some significant obstacles to overcome. However, and in line with Article 57(1) of Additional Protocol I to the Geneva Convention, with precautions and constant care cyber attack can exhibit extreme levels of discrimination (ICRC 1949 & 1977). Again, Stuxnet is illustrative of this point. Despite spreading to other computers, 'Unless you happen to be running a large array of exactly 984 Siemans centrifuges simultaneously, you have nothing to fear from this worm.' (Singer & Friedman 2014: 119)

Faced with the challenge of discrimination, policy makers responsible for the common good must think long and hard before unleashing cyber attacks into the global information environment. Either by intent or accident, cyber attack could disrupt the services upon which individual and social wellbeing increasingly depends. Moreover, the effects of conflict could spread, thereby harming the cause of solidarity. Finally, by increasing the range of legitimate targets, cyber attack has the propensity to spread the suffering associated with war. If the common good is to be served, the effects of conflict must be restricted.

Proportionality

Proportionality ranks alongside discrimination as a vital ingredient of doing more good than harm. In the absence of proportionality the danger of escalation looms large, and with it increased risks to the common good. For cyber attack, proportionality is concerned not just with escalation to ever-greater levels of cyber conflict; there also exists the spectre of breaching the threshold for physical violence. Alternatively, cyber attack proffers the possibility of enabling radical forms of proportionality. This is especially evident in relation to 'reversibility', whereby the effects of an attack can be instantly reversed, with no lasting harm.

In contrast to physical expressions of force, the effects of certain cyber attacks (such as DDoS or ransonware) can be reversed immediately with no visible signs that conflict ever occurred (Dipert 2010: 392, Henschke & Lin 2014). If realised, this changes the moral calculus of going to war. A war without lasting effect would be a potent legitimate tool of policy. The impact on individual and community wellbeing would be minimal. Moreover, the effects on solidarity would be far less than had lasting damage occurred as a result of violence.

Although reversibility is possible, cyber attack offers plenty of potential for lasting harm, escalation and disproportionate effects. Data, for example, can be destroyed, with significant consequences. Wiper and Shamoon, so-called 'data-destruction' attacks, were aimed at the Iranian Oil Ministry, National Iranian Oil Company, and Saudi Aramco (Zetter 2015). Shamoon wiped 30,000 hard drives, causing massive loss of data and substantial financial losses (Pagliery 2015). At present, data is not considered to be a civilian object by the International Committee of the Red Cross (ICRC), and thus not protected under International Humanitarian Law (IHL) (Schmitt 2013: 127). That may have to change. The ICRC regards loss of function of a physical object as legally equivalent to damaging it (Henschke & Lin 2014). In the cyber age, it seems obvious to afford the same level of protection to the functionality of information processes. It has also been suggested that data should be regarded as cultural property, worthy of protection under the 1954 Hague Cultural Property Convention (Schmitt 2013: 228; Taddeo 2014). This leads us to the issue of cyberharm (discussed in detail below). If data and digital activities have moral value, then they have to be included in any judgement of proportionality. Indeed, some commentators have argued that cybersecurity discourse must encompasses the full scope of human dependency on virtual objects (Canetti, Gross & Waismel-Manor 2016: 169).

Proportionality also reignites concerns regarding the predictability and controllability of cyber attack. If the effects of an attack cannot be accurately predicted, and if unintended consequences are likely to occur, then the proportionality of a cyber attack is uncertain. Of particular significance to proportionality is the issue of whether one can adequately monitor the effects of an attack, and whether an attack can be stopped when conflict ceases (Lin et al 2012, Schmitt 2013: 172). In this sense, we can think of malware as a sort of digital landmine, which may continue to pose risks long after a war is over. Lack of control is exacerbated by the fact that many cyber actions are by necessity automated. The tempo of cyber operations means that humans have to be out of the loop (Danks & Danks 2016: 185).

As with discrimination, the common good is potentially endangered by the disproportionate effects of cyber attack. To serve the common good cyber attack must be a limited and controllable form of aggression. If this is not the case, then individual and social wellbeing is threatened, and the conflict could escalate and/or spread, threatening solidarity. To mitigate harm, escalatory dynamics must be retarded, and data must be afforded proper value and protection in social, economic and cultural forms. If this is achieved, and if discrimination is maintained, cyber attack could be an accurate policy instrument with instantly reversible effects. Cyber power then becomes the preferred means.

Cyberharm

To give cyberharm its rightful place in the contemporary military ethics debate, we need to clarify its significance for realization of the common good. If social activities in the cyber domain are essential for development and flourishing, then cyberharm is an issue of serious concern for the common good. Incorporating cyberharm into military ethics discourse is recognition of the fact that many aspects of our lives are now lived in or through the virtual domain. To give official recognition to cyberharm would, however, require a significant rethinking of IHL. At present, the latter is based exclusively on physical objects, which the ICRC classifies as visible and tangible (Dipert 2016: 63, Schmitt 2013: 126).

One way to incorporate cyberharm into IHL is by recognising the Internet and digital services as essential for life. This would bring them into line with water supplies, for example, which are protected under the laws of armed conflict (Dipert 2010: 399). However, the *Tallinn Manual*, the most comprehensive treatment to date of IHL in the cyber domain, dismisses the indispensability of the Internet Schmitt 2013: 227). This position has drawn criticism. Canetti *et al*., for example, argue that digital services are so woven into our daily lives that to be without them causes severe anxiety, a sense of insecurity, and weakens public faith in the state (Canetti et al 2016: 165). From the perspective of the common good, it is certainly true that connectivity to the virtual domain has become essential for social and economic development, as is recognized by the United Nations (Jackson 2011).

In legal terms, the issue becomes one of whether or not data can be classified as a 'civilian object.' Under Article 52 of Additional Protocol I to the 1977 Geneva Conventions, it is unlawful to directly attack civilian objects (Schmitt & Vihul 2016: 43). In its current form, all examples provided in Article 52 relate to physical objects (Dipert 2010: 400). However, in a world in which most critical services are reliant upon computer networks, it seems anachronistic to limit the status of civilian objects and essential services to physical items. In this way, cyberwar 'brings new intangible objects into the moral discourse.' (Taddeo 2014: 38)

Without reference to the cyber domain in our moral and legal discourse on harm, the common good cannot be properly served. However, whilst it is correct to acknowledge cyberharm, the latter is not commensurate with the damage caused by physical violence. As previously noted, the effects of cyber attack are more reversible and arguably have less long-term effects. As damaging as cyberharm may be, the number of fatalities from cyber attacks remains a reassuring zero (Singer & Friedman 2014: 96). In terms of damage to the common good, physical violence still trumps cyberharm because it violates the right to life - the most basic of rights and the foundation for all other actions towards realising the common good.

The Threshold of Conflict

From the perspective of the right to life, virtual conflict is preferable to physical conflict. Yet, when considering all four components of the common good, all conflict has negative consequences. Conflict clearly acts as a threat to peace and security, has detrimental effects on social wellbeing, and undermines efforts towards solidarity. Thus, we must now assess whether the development of cyber attack makes conflict more or less likely. The first task is to determine the legal and political status of the cyber domain, as this will influence the likelihood of conflict occurring. The cyber domain is often considered to be beyond normal geopolitical considerations, and therefore not subject to the normal flow of conflict events

(Libicki 1999). However, legally this is not an entirely accurate description: 'although no state may claim sovereignty over cyberspace *per se*, states may exercise sovereign prerogatives over any cyber infrastructure located on their territory.' (Schmitt 2013: 16) In common parlance, Cyberspace may be thought of as ethereal; but in fact it is based in the physical reality of existing geopolitical space. Indeed, rather than producing novel conflict relationships, tensions in cyberspace tend to reflect existing points of contention in the physical realm (Valeriano & Maness 2014).

As an instigator of wider conflict, thus far actions in cyberspace have tended to be unremarkable. Dipert (2016: 69-70) reports that much state behavior in cyberspace, including espionage and information disruption, although undesirable, has not crossed the boundaries of generally tolerated behavior amongst actors in the international system. Cyber actions have yet to provide casus belli for a shooting war. The more serious events have tended to be dealt with via criminal proceedings and diplomatic and economic sanctions. However, aggressive cyber actions have intensified tensions between mayor players in the system, most obviously amongst the US, China, Russia and North Korea.

One of the most dangerous features of interactions in the cyber domain is the overlap between actions of varying degrees of hostility. Dipert's optimistic analysis only holds if the thresholds between certain actions are reasonably clear. This is not always the case. At a tactical and operational level, the cyber variants of espionage, crime, or even a simple network probe, are almost indistinguishable from the early stages of a major cyber attack: 'That same insertion of malicious code to steal information could also enable someone to control, compromise, and even destroy the entire system itself.' (Henschke & Lin 2014) Does the insertion of malware provide casus belli? The answer to this question comes down to the difficult judgement of whether the insertion represents a preparatory act or the initial phase of an attack. In IHL, the former is not considered an armed attack if the initiator is simply acquiring the capability to launch an attack in the future. The victim has a right to act in self-defence only if an attack is imminent (Schmitt 2013: 65).

Within cybersecurity, exemplified by everyday techniques such as firewalls and virus scans, self-defence occurs automatically. Thus, from a legal and political perspective the more important issue is that of sovereignty. Since informational infrastructure exists in territorially defined states, strictly speaking, the insertion of malicious code breaches state sovereignty. This distinguishes preparatory actions in cyberspace from similar actions in the other domains. In the physical domain, the preparatory phase of an attack could not include the insertion of forces into enemy territory without initiating conflict. In contrast, preparation in the cyber domain requires a more intrusive approach. As a result, tensions are raised; misunderstanding could follow, and the threshold of conflict is lowered. In the past, conflict would start with troops crossing a border. In the cyber age all it takes is an email attachment.

According to the *Tallinn Manual*, whether or not virtual forms of aggression constitute casus belli is not entirely clear. On the one hand, there is no comfort to be found hiding in the virtual nature of cyber attack: 'the mere fact that a computer … is used during an operation has no bearing on whether that operation amounts to a use of force.' (Schmitt 2013: 42) For a use of force to be regarded as an 'armed attack' – when self-defence is legitimately triggered – we look to the International Court of Justice's (ICJ) judgement in the Nicaragua case. During the latter, it was decided that an armed attack is determined by 'scale and effect'. (Schmitt 2013: 45) It matters not whether the means to create effect are software or kinetic in nature.

On the other hand, at present, scale and effect relates only to tangible, physical effects. Specifically, death and destruction must occur for an action to be classified as an armed attack (Schmitt 2013: 55). Although this interpretation would seem to cover the Stuxnet operation, it does not relate to many other forms of cyber attack. Thus, in determining whether non-violent cyber actions could cause conflict, we must dig deeper. In the Nicaragua case, the ICJ also ruled that the principle of non-intervention is 'part and parcel of customary international law'. (Schmitt 2013: 44) For an act to be classified as intervention, as opposed to mere interference, there must be a coercive element (Schmitt 2013: 45). Based on this understanding of non-intervention, we can rule out simple intrusion into a network as a formal cause of conflict. However, should that intrusion include data destruction or theft to affect political outcomes, it could be classed as coercive, and therefore breach the principle of non-intervention, and potentially trigger conflict.

What is the outcome of this fairly complex legal discussion? Does cyber attack lower the threshold for conflict, and thereby risk undermining solidarity and the common good within the international community? Clearly, not all cyber intrusions provide a formal basis for conflict. The insertion of malware could be interpreted as a breach of sovereignty. However, if that same act of cyber intrusion does not cause death and destruction, is non-coercive, and does not seek to affect political outcomes, then it does not appear to cross the boundary of armed attack or non-intervention. Such an intrusion would likely fall within generally accepted parameters of state behavior, such as espionage, for example.

However, any optimism is tempered by the fact that some forms of cyber attack, including some fairly common ones, do appear to constitute an armed attack or breach the principle of non-intervention. Stuxnet would seem to constitute a fairly obvious form of armed attack. Additionally, DDoS attacks with a coercive intent would seem to fall foul of the non-intervention rules.

The risk of cyber conflict is not restricted to cases in which states directly attack one another. Based on the ICJ ruing on the Corfu Channel case, and assuming that a cyber attack qualifies as an armed attack or intervention, a state can be held responsible for the actions of non-state actors operating from its territory, if the state supports them or has knowledge of their actions (Schmitt 2013: 26). Historically, a number of attacks have been committed by cyber militias who, although nominally not affiliated to the state, are believed to be directed by state institutions or working to promote state interests. This is evidenced, for example, in the 2007 attack on Estonia and the actions of cyber militias in China (Sheldon & McReynolds 2015).

If cyberharm were to be incorporated into IHL, the threshold for conflict is lowered even further. If damage to information, or denial of digital services is classed as grounds to initiate self-defence, then based on current evidence, conflict could be a far more frequent occurrence. This produces a much less stable security environment, with the potential for escalation to the higher levels of cyber attack and physical expressions of force. Furthermore, as evidenced by Stuxnet, cyber attack is a potent means of surprise attack and covert operations (Lin, Rowe & Allhoff 2012). Consequently, states are likely to be increasingly hypersensitive to network probes and the insertion of malicious code. This is especially dangerous because, due to the technical overlap amongst different cyber operations, a simple network breach could be misinterpreted as the start of a major attack.

Much of the above analysis suggests that cyber attack will lower the threshold for conflict, which in turn will have negative consequences for the common good. This negative outlook is somewhat tempered by the fact that since the heady days of Stuxnet, Bronze Soldier and Shamoon, restraint has characterized state actions in cyberspace. This is not to say that cyber attackers have remained dormant. In 2014, Energetic Bear compromised over 1000 organisations in the energy sector, gaining access to sensitive data (Leach 2014). More significantly, BlackEnergy - an attack on Ukrainian electricity utilities in December 2015, was the first instance of a cyber attack causing a power blackout. That being said, the attack was limited. It affected only 80,000 residents for a few hours, and did not destroy any equipment, even though the latter was technically possible (Zetter 2016).

As Energetic Bear and BlackEnergy indicate, the techniques of cyber attack continue to develop. However, state use of the instrument is still relatively muted. In this sense, it has been suggested that cyber actions are a means for states to let off steam or rebalance power relations without the consequences of using physical force (Valeriano & Maness 2015: 75). It is also worth reiterating the point that certain forms of cyber attack, such as DDoS, are non-invasive, and therefore sidestep the breach of sovereignty issue (although, as noted, they can be coercive) (Dipert 2010: 387). In this way, although states may rub up against one another more often in cyberspace, it seems that cyber conflict can be more easily restrained than in the physical realm. Thus, from the perspective of the common good, the dangers of lowering the threshold of conflict are somewhat offset by current evidence suggesting states are learning to cope with new tensions and forms of interaction in cyberspace.

Conclusion - The Fate of the Four Components of the Common Good

The major powers are rapidly developing ever-greater cyber attack capabilities. However, as was evident in the early years of the nuclear revolution, the technology is developing faster than our ability to comprehend the strategic and moral implications. At the time of writing, no state has a fully functioning cyber strategy (Lonsdale 2016). For as Thomas G. Mahnken (2011) notes, 'Despite sweeping pronouncements, the use of cyber means to achieve political aims remains an abstract and underdeveloped topic'.

Nor do we yet have the 'full ethics of cyberwarfare' requested by Dipert (2016: 59). Some progress has been made. The War Convention approach has made great strides defining armed attack in a cyber context, as well as dealing extensively with issues pertaining to *jus in bello*, especially proportionality and discrimination. Indeed, *Tallinn Manual 2.0* has extended the range of enquiry, incorporating discussion of cyber operations below the level of armed attack (Schmitt & Vihul 2016). In addition, the cyberharm discourse usefully extends our understanding of the relationship between the physical and virtual domains. In doing so, it gives moral weight to the informational aspects of our lives and social processes. Taken together, these represent important contributions to the ethics of cyber attack discourse. Nonetheless, these approaches do not provide sufficient understanding of the post-bellum implications of cyber operations.

This paper has sought to develop the cyberwarfare ethics discourse through the conceptual vehicle of the common good. The latter provides a comprehensive and accessible means to understand the implications of any socio-political action, including cyber attack. This includes a consideration of the post-bellum implications of cyber attack, especially in relation to solidarity and effects on future development and wellbeing. Having assessed the six key characteristics of cyber attack from a moral perspective, this paper will now conclude with a discussion of the fate of the four core components of the common good: respect for the person (premised on the right to life); social wellbeing; peace and security; and solidarity.

Respect for the Person

Underpinning the common good are basic human rights and the dignity of each individual. Each person should be afforded the opportunity to develop and flourish. This begins with the right to life. Nefarious cyber activities are a daily occurrence, and yet the most striking statistic about them is that they have never caused a fatality. In this sense, cyber attack, as an alternative to physical expressions of force, helps to promote the common good. Policy objectives can be pursued absent of the terrible consequences of violence.

That being said, the gains of non-violence are somewhat offset by the risk of escalation to physical conflict, as well as the unpredictable and uncontrollable features of cyber attack. The impact of cyber attack on the individual may be less dramatic, but the effects could be more widespread. Proportionality and discrimination may be more difficult to maintain in a cyber operation. Stuxnet, which spread well beyond its intended target network, is illustrative of this. We also have to consider the indirect effects of cyber attack. Whilst software cannot by itself inflict physical harm, death and injury can occur with attacks against certain targets sets.

Social Wellbeing

For the common good to be realised, opportunities for development must be community-wide. In the contemporary age social wellbeing is dependent upon the functioning of the CNI. Cyber attack undoubtedly threatens CNI, and thus can be seen as a threat to the socio-economic underpinnings of the common good. This is doubly so if cyberharm is given proper recognition in legal and moral discourse. Yet, on a more positive note, earlier talk of Armageddon levels of disruption is now being replaced with more balanced appraisal of the cyber threat. In his testimony to the Senate Armed Services Committee, Director of National Intelligence, James Clapper (2015: 2), talked down the possibility of an 'electronic Pearl Harbor'. Instead, he focused on ongoing 'low-to-moderate' level threats. It is also worth reiterating the point that cyber attacks are often non-destructive with entirely reversible effects. Thus, it is possible that the wellbeing component of the common good could emerge reasonably intact in the aftermath of a cyber conflict – although the permanent loss of data and exclusion from social networks (examples of cyberharm) somewhat qualifies this statement.

Peace and Security

When it comes to maintaining peace and security, cyber attack undoubtedly has a developing role. Social and individual development requires a secure, stable and peaceful environment. As a result, participation in military life (virtual and physical) is perfectly compatible with striving for the common good (Pontifical Council for Justice and Peace 2004: 502). To that end, states must be able to operate effectively in the cyber domain to protect the digital components of social activity. Ideally, peace and security will be maintained short of conflict via a credible deterrence posture, which must now contain a potent cyber attack capability. If conflict is unavoidable, cyber attack could help limit damage to the state by degrading enemy attack capabilities. Additionally, it may accelerate a return to peace and security via coercive effect or by acting as a force multiplier to physical military operations.

However, the development of potent cyber attack capabilities risks lowering the threshold of conflict. Due to the overlap between cyber operations of varying degrees of hostility, there may be a blurring of the distinction between war and peace. Small actions in cyberspace could readily breach sovereignty and/or be mistaken for the initial stages of an attack. Moreover, fairly common forms of cyber attack could breach the non-intervention principle of IHL. In addition, the unpredictability of cyber operations is a potential threat to proportionality, with an increased risk of conflict escalation. By such means, preparing for cyber attack risks stimulating conflict and the resultant negative consequences for the common good. Nevertheless, a degree of restraint has emerged in cyberspace. Indeed, it has been suggested that cyberspace provides an environment within which states can address a power imbalance without recourse to political violence.

Solidarity

Solidarity is an essential consideration for the post-bellum environment and for realization of the common good in the international system (Pontifical Council for Justice and Peace 2004: 193). There is no greater threat to solidarity than the long-term effects of violent conflict, which often sour relations amongst states for decades. Cyber attack offers the possibility for states to play out their differences in a manner that avoids the damaging effects of violence. Moreover, mutual vulnerability to cyber attack has forged a degree of international cooperation and the emergence of new international norms (UN Office for Disarmament Affairs). Nonetheless, as evidenced by rising tensions amongst the US, Russia, China and North Korea, cyber intrusions can undermine solidarity. States are increasingly sensitive to dangers to their CNI and cyberharm being inflicted on their citizens. Even relatively minor cyber actions regularly breach sovereignty and violate neutrality via the routing of attacks through third-party countries.

Final Thoughts

In the final analysis, it is evident that cyber attack poses both threats and opportunities for pursuit of the common good. As in any domain, the Clausewitzian nature of war applies in cyberspace. As a result, cyber conflict will be prone to uncertainty, loss of control and escalation, and thus poses a risk to the common good. However, and also in accordance with Clausewitzian theory, cyber attack is not an independent force in international affairs. It is a tool of policy, at the behest of those who use it. Thus, for cyber attack to do more good than harm, it must be used with due care and diligence. States must be fully conscious of the moral component of cyber attack and guided by strong ethical standards in support of the common good. With the common good acting as a guiding framework, states are better placed to pursue peace and security without seriously degrading the rights or development of the individual and society, nor damaging solidarity within the international community.

References

InformationWeek (2013), 'Offensive Cybersecurity: Theory and Reality'. *InformationWeek*, 21 January.

Allhoff Fritz, Henschke Adam, Strawser Bradley J. (eds) (2016), *Binary Bullets: The Ethics of Cyberwarfare*, Oxford: Oxford University Press.

Arquilla John (2012), 'Cyberwar is Already Upon Us': But Can it be Controlled', *Foreign Policy* (March/April).

Arquilla John (2016), ' Foreword', in Allhoff et al, *Binary Bullets: The Ethics of Cyberwarfare*, Oxford, Oxford University Press.

Bellamy A. J. (2008), 'The Responsibilities of Victory: Jus Post Bellum and the Just War', *Review of International Studies* 34:4, 601–625.

Banta Benjamin R. (2011), 'Virtuous War and the Emergence of jus post bellum', *Review of International Studies* 37, 277-299.

Beard Matthew (2016), 'Beyond Tallinn: The Code of the Cyberwarrior', in Allhoff, et al, *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press.

Boebert W. E. (2011), 'A Survey of Challenges in Attribution', in Committee on Deterring Cyberattacks (ed.), Proceedings of a Workshop on Deterring Cyberattacks, Washington DC: National Academies Press.

Borghard Erica D. & Lonergan Shawn W. (2017), 'The Logic of Coercion in Cyberspace', *Security Studies*, 26:3, 452-481.

Brenner Joel and Lindsay Jon R. (2015), 'Correspondence: Debating the Chinese Cyber Threat', *International Security*, 40:1, 191-195.

Cabinet Office (2016), *National Cyber Security Strategy 2016-2021*, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 November.

Canetti D, Gross M. L. & Waismel-Manor I. (2016), 'Immune from Cyberfire? The Psychological and Physiological Effects of Cyberwarfare', in Allhoff, et al, *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press.

Cisneros Maribel (2015), *Cyber Warfare: jus post-bellum*, Naval Postgraduate School, Monterey, California, http://calhoun.nps.edu/bitstream/handle/10945/45169/15Mar_Cisneros_Maribel.pdf?sequence=1&isAllowed=y

Clapper James R. (2015), *Statement for the Record US Cybersecurity and Policy, Senate Armed Services Committee*, Senate Armed Services Committee (29 September).

Clausewitz Carl von (1989), *On War*, Princeton, NJ: Princeton University Press.

Daalder Ivo H. and O'Hanlon Michael E. (2000), *Winning Ugly: NATO's War to Save Kosovo*, Washington DC.: Brookings Institution Press.

Danks David and Danks Joseph H. (2016), 'Beyond Machines: Humans in Cyberoperations, Espionage, and Conflict', in Allhoff, et al, *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press.

Davis II John S., Boudreaux Benjamin, Welburn Jonathan W., Aguirre Jair, Ogletree Cordaye, McGovern Geoffrey, and Chase Michael S. (2017), *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica: RAND.

Department of Defense (2015), *The DOD Cyber Strategy*, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Denning Dorothy (2015), ‘Rethinking the Cyber Domain and Deterrence’, *Joint Force Quarterly*. 77, 8-15.

Der Derian James (2000), ‘Virtuous War/Virtual Theory’, *International Affairs*, 76:4 (2000), 771-88.

Dipert Randall R. (2010), ‘The Ethics of Cyberwarfare’, *Journal of Military Ethics*, 9:4.

Dunlap Charles J. (2012), ‘The Intersection of Law and Ethics in Cyberwar: Some Reflections’. *Air and Space Journal*. 24, 1-17.

Farmer Ben (2017), ‘Britain Prepared to Use Air Strikes or Send in Troops as Retaliation Against Future Cyber Attack’, *The Telegraph*, (28 June) http://www.telegraph.co.uk/news/2017/06/27/cyber-attack-could-lead-military-retaliation-says-fallon/?WT.mc_id=tmg_share_tw

Fuchs Michael H. and Buckley David (2007), “Pursuing the Global Common Good.” in *Pursuing the Global Common Good*, edited by Sally Steenland, Peter Rundlet, Michael H. Fuchs, and David Buckley, Washington, DC: Center for American Progress, 5-16.

Gartzke Erik (2013), ‘The Myth of Cyberwar’, *International Security*, 38:2, 41-73

HM Government (2015), *National Security Strategy and Strategic Defence and Security Review,* https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 November.

HM Treasury (2015), 'Chancellor's Speech to GCHQ on Cyber Security', (17 November), https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

Hehir Bryan (2007), 'The Just War Ethic: Protecting the Global Common Good', in *Pursuing the Global Common Good*, edited by Sally Steenland, Peter Rundlet, Michael H. Fuchs, and David Buckley, (Washington, DC: Center for American Progress,.

Henschke A & Lin P (2014), 'Cyberwarfare Ethics, or How Facebook Could Accidently Make Its Engineers into Targets'. *Bulletin of Atomic Scientists*. 25 August.

Hirschfeld Davis Julie (2015), 'Hacking of Government Computers Exposed 21.5 Million People', *The New York Times* (29 July) http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0

ICS-CERT (2016), *Cyber Attack Against Ukrainian Critical Infrastructure*, (25th February), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Ignatieff Michael (2000), *Virtual War*, New York: Metropolitan Books.

Iasiello E (2014), 'Is Cyber Deterrence an Illusory Course of Action'. *Journal of Strategic Security*. 7:1, 54-67.

International Committee of the Red Cross (1949, 1977), *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), (8 June 1977).* https://www.icrc.org/applic/ihl/ihl.nsf/9ac284404d38ed2bc1256311002afd89/50fb5579fb098faac12563cd0051dd7c

Jackson Nicolas (2011), 'United Nations Declares Internet Access A Basic Human Right', *The Atlantic* (3rd June).

Jenkins Ryan (2016), 'Cyberwarfare as Ideal War', in Allhof, et al, *Binary Bullets: The Ethics of Cyberwarfare*, Oxford: Oxford University Press.

Kaplan Fred (2016), *Dark Territory: The Secret History of Cyber War*, New York: Simon Schuster.

Kello Lucas (2013), 'The meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security,* 38:2, 7-40.

Lasiello L. V. (2004), 'Jus Post Bellum: The Moral Responsibilities of Victors in War' *Naval College Review* 57:3/4, 33–52.

Leach Adam (2014), 'Cyber Espionage: Understanding Energetic Bear', *Power-Technology.com,* (October), http://www.power-technology.com/features/featurecyber-espionage-understanding-energetic-bear-4414662/

Libicki Martin C. (1999), 'The Emerging Primacy of Information', in Colin S. Gray and Geoffrey Sloan (eds), *Geopolitics, Geography and Strategy*, London: Frank Cass.

Libicki Martin C. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica: RAND.

Libreria Editri Vaticana (1994). *Catechism of the Catholic Church*, (Vatican City: Libreria Editrice Vaticana.

Lin Patrick, Rowe Neil, and Allhoff Fritz (2012), 'Is it Possible to Wage a Just Cyberwar?', *The Atlantic* 5th June.

Lindsay Jon R. (2013), 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22:3 365-404.

Lindsay Jon R. (2015a), 'Introduction: China and Cybersecurity: Controversy and Context', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds), *China and*

Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford: Oxford University Press.

Lindsay Jon R. (2015b), 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyber Attack.' *Journal of Cyber Security*. 1:1, 53-67.

Lonsdale David J. (2004), *The Nature of War in the Information Age: Clausewitzian Future*, London: Frank Cass.

Lonsdale David J. (2016), 'Britain's Emerging Cyber Strategy', *RUSI Journal*, 161:4, 52-62.

Lonsdale David J. (2017) 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy and Technology*, available online at https://doi.org/10.1007/s13347-017-0252-8

Lucas George R. (2016), 'Emerging Norms for Cyberwarfare', in Allhof, et al, *Binary Bullets: The Ethics of Cyberwarfare*, Oxford: Oxford University Press, 2016.

Lucas George R. (2017), *Ethics and Cyber Warfare: Law and Order for a Lawless Frontier*, Oxford: Oxford University Press.

Mahnken Thomas G. (2011), 'Cyber War and Cyber Warfare', in Kristin M. Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age, Volume II*, Washington, DC., Center for a New American Security.

Nakashima Ellene and Ryan Missy (2016), 'US Military Has Launched a New Digital War Against the Islamic State', *Washington Post*, July.

Nicholson Peter P. (1990), *The Political Philosophy of the British Idealists: Selected Studies*, Cambridge: Cambridge University Press.

Office of the Secretary of Defense (2018), *Nuclear Posture Review*, available at https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

Ohlin Jens David, Govern Kevin, and Finkelstein Claire (2015), *Cyberwar: Law and Ethics for Virtual Conflicts,* Oxford: Oxford University Press.

Orend Brian (2007), 'Jus Post Bellum: The Perspective of a Just-War Theorist', *Leiden Journal of International Law* 20:3, 571–591.

Orend Brian (2016), 'Postcyber: Dealing with the Aftermath of Cyberattacks', in Allhoff, et al, *Binary Bullets: The Ethics of Cyberwarfare*, Oxford: Oxford University Press.

Pagliery Jose (2015), ‘The Inside Story of the Biggest Hack in History’, *CNN Money* (5 August) http://money.cnn.com/2015/08/05/technology/aramco-hack/

Payne Keith B. (1996), *Deterrence in the Second Nuclear Age*, Kentucky: University of Kentucky Press.

Pontifical Council for Justice and Peace (2004), *Compendium of the Social Doctrine of the Church*. Vatican City: Libreria Editrice Vaticana.

Rid Thomas (2012), ‘Cyber War Will Not Take Place’, *Journal of Strategic Studies*, 35:1, 5-32.

Rid Thomas & Buchanan B (2014), ‘Attributing Cyber Attacks’. *Journal of Strategic Studies*. 1:2, 4-37

Rosenquist M (2015), ‘Offensive Cyber Security Changes the Industry’. *Cyber Security Intelligence*. https://www.cybersecurityintelligence.com/blog/offensive-cyber-security-changes-the-industry-455.html

Rowe N. C. (2007), ‘Ethics of Cyberwar Attack’. In Colaril, A. & Janczewski, L. (eds) *Cyber War and Cyber Terrorism*, Hershey, PA: The Idea Group.

Schmitt Michael N. (ed) (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

Schmitt Michael N. and Vihul Liis (2016), ‘The Emergence of International Legal Norms for Cyberconflict’, in Allhoff, et al, *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press.

Schmitt Michael N. and Vihul Liis (eds) (2016), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

Sheldon Robert and McReynolds Joe (2015), ‘ Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias’, in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* Oxford: Oxford University Press, 188-224.

Singer P. W. (2015), ‘How the US Can Win the Cyberwar of the Future: Cold War Deterrence Theory Won’t Cut it Anymore’, *Foreign Policy*, (18th December).

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

Solon Olivia (2016), ‘Yahoo Confirms State-Sponsored Hackers Stole Personal Data From 500m Accounts, *The Guardian* (23 September).

https://www.theguardian.com/technology/2016/sep/22/yahoo-hack-data-state-sponsored

Stoltenberg General Jens (2016), *NATO Press Conference*, (14th June), http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en

Taddeo Mariarosaria (2012), 'An Analysis for a Just Cyber Warfare', in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), *4th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications, 209-218.

Taddeo Mariarosaria (2014), 'What Ethics Has To Do With the Regulation of Cyberwarfare', *Ethics and Armed Forces* 2.

Tsagourias Nicholas (2013), 'Cyber Attacks, Self-Defence and the Problem of Attribution', *Journal of Conflict & Security Law,* 17.

Tyler Colin (2006), "Contesting the Common Good: T. H. Green and Contemporary Republicanism". In *T. H. Green: Ethics, Metaphysics, and Political Philosophy*, edited by Maria Dimova-Cookson and William J. Mander, Oxford: Clarendon, 262-291.

Tyler Colin (2012), *Civil Society, Capitalism and the State*, Exeter: Imprint Academic.

United Nations Office for Disarmament Affairs, *GGE Information Security: Developments in the Field of Information and Telecommunications in the Context of International Security*
http://www.un.org/disarmament/topics/informationsecurity/

Valeriano Brandon and Maness Ryan C. (2015), *Cyber War Versus Cyber Realities*, Oxford: Oxford University Press.

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

The White House (2016), *Fact Sheet: CyberSecurity National Action Plan*, (February 9th) https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Williams R. E. and Caldwell D. (2006), 'Jus Post Bellum: Just War Theory and the Principles ofJust Peace', *International Studies Perspectives* 7:4, 309–320.

Deputy Secretary of Defense Work Robert O. (2015), *Opening Statement Before the Senate Armed Services Committee*, September 29.

Zetter Kim (2014) , *Countdown to Zero Day*, New York: Broadway Books.

Zetter Kim (2015), ‘The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks’, *Wired* (10 February).

Zetter Kim (2016), ‘Everything We Know About Ukraine’s Power Plant Hack’, *Wired*, (20 January), https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/