Philos. Technol.
DOI 10.1007/s13347-017-0252-8

RESEARCH ARTICLE

Warfighting for Cyber Deterrence: a Strategic and Moral Imperative

David J. Lonsdale[1]

Received: 4 July 2016 / Accepted: 13 January 2017

Abstract Theories of cyber deterrence are developing rapidly. However, the literature is missing an important ingredient—warfighting for deterrence. This controversial idea, most commonly associated with nuclear strategy during the later stages of the Cold War, affords a number of advantages. It provides enhanced credibility for deterrence, offers means to deal with deterrence failure (including intrawar deterrence and damage limitation), improves compliance with the requirements of just war and ultimately ensures that strategy continues to function in the post-deterrence environment. This paper assesses whether a warfighting for deterrence approach is suitable for the cyber domain. In doing so, it challenges the notion that warfighting concepts are unsuitable for operations in cyberspace. To do this, the work constructs a conceptual framework that is then applied to cyber deterrence. It is found that all of the advantages of taking a warfighting stance apply to cyber operations. The paper concludes by constructing a warfighting model for cyber deterrence. This model includes passive and active defences and cross-domain offensive capabilities. The central message of the paper is that a theory of victory (strategy) must guide the development of cyber deterrence.

Keywords Cyber · Deterrence · Warfighting · Strategy · Cyberwar · Ethics

1 Introduction

Cyberspace has been officially designated a domain of warfare (Kaplan 2016, 6). At the same time, deterrence has become embedded in the cyber policies of major states (Department of Defense 2015; HM Treasury 2015). This has been reflected in some excellent work discussing the difficulties of operating a successful deterrence posture in

✉ David J. Lonsdale
d.lonsdale@hull.ac.uk

[1] School of Law and Politics, University of Hull, Cottingham Road, Hull HU6 7RX, UK

Published online: 02 February 2017

the cyber domain (Singer 2015; Denning 2015; Libicki 2009; Lindsay, 2015a; Iasiello 2014; Geers 2011; Harknett et al. 2010). However, discussion of cyber deterrence rarely goes beyond the point of failure—the point at which conflict ensues. 'Warfighting for cyber deterrence' is missing in action. Yet, deterrence cannot be viewed in isolation. It must be considered as part of a unified strategy, including what happens in the post-deterrence environment. In this respect, warfighting cannot safely be disassociated from deterrence. For one thing, the efficacy of the latter is dependent upon the former.

During the Cold War, nuclear warfighting theorists convincingly argued that deterrence required far more than a basic threat of retaliation. Beginning with Albert Wohlstetter's (1959) RAND study, which identified vulnerabilities in Strategic Air Command's retaliatory capability, nuclear strategy became ever more detailed, moving beyond existential deterrence and Mutually Assured Destruction (MAD).

For warfighting theorists, MAD could never be considered effective strategy. It lacked credibility, especially when faced with extended deterrence commitments. Moreover, it failed to address a critical strategic question in a satisfactory manner: what happens if deterrence fails? In essence, the warfighting theorists were urging the defence and policy communities to think more rationally, more strategically about deterrence and post-deterrence options (Gray & Payne 1980, 14). More controversially, the warfighting literature raised the issue of victory in nuclear war.

This paper introduces warfighting into cyber discourse and in doing so takes the cyber deterrence literature beyond the confines of the denial/punishment framework. In order to provide an intellectually robust analysis, the work begins with a conceptual exploration of warfighting for deterrence. Specifically, the work will explore five key rationales that motivate warfighting for deterrence, before identifying the main challenges to this approach. Once a general conceptual understanding of warfighting has been established, the paper will assess the utility of this framework for cyber deterrence. Finally, in the third section of the paper, we will construct an outline of what warfighting for cyber deterrence actually looks like.

For the most part, the work uses the literature and theory of nuclear warfighting for deterrence as its conceptual foundation. It is accepted that this analogy has some limitations, and these are noted where appropriate within the text. However, this methodological approach is justified on the grounds that warfighting for deterrence is most developed in its nuclear form. Moreover, although nuclear and cyber forms of power are clearly distinct, the principles of deterrence and its relationship to warfighting are arguably universal. It should be noted that conventional deterrence is also referred to within this paper, although the literature in this area is considerably more limited (Gerson 2009).

Whether we are discussing nuclear, conventional or cyber forms of power, strategy cannot stop at deterrence; it cannot be solely concerned with the prevention of war. Strategy, and therefore deterrence, is ultimately about battle, whether physical or virtual. As defence professionals grappling with the challenges of cyber deterrence, we must give respect to Clausewitz's comment that 'it is inherent in the very concept of war that everything that occurs *must originally derive from combat*' [emphasis in the original] (Clausewitz 1978, 87). As we go forward with the analysis, it is worth keeping in mind the Duke of Wellington's forthright reply when asked what were his campaign objectives for 1815: 'Why, to beat the French.' (Gray 1984, 9).

2 Warfighting for Deterrence: a Conceptual Approach

The ideas behind warfighting for deterrence developed as a result of intellectual engagement with the challenges of nuclear strategy. Throughout the Cold War, the defence community of the USA sought to shore up the credibility of its nuclear deterrence. Put simply, the USA had to convince the Soviet Union, and itself, that it would launch devastating nuclear attacks in response to communist gains. From the relatively unsophisticated beginnings of punishment through Massive Retaliation, over time, the USA developed a more flexible, mature capability. This included Limited Nuclear Options (LNOs), offensive counterforce capabilities—aimed at Soviet nuclear forces, limited defensive measures, and a developing understanding of the strategic culture of the Soviet Union. As a result, although it never abandoned MAD, the USA was able to explore countervailing and prevailing strategies. The former sought to prevent the Soviets from achieving their objectives (deterrence by denial). Prevailing went further, and sought to provide the wherewithal for the USA to achieve victory in nuclear war.

There are five primary motivations for adopting a warfighting deterrence posture: to enhance credibility, to deal with deterrence failure, damage limitation, to provide a theory of victory and to adhere to the moral obligations of the Just War tradition. The paper will discuss each one of these in turn, and in doing so will construct a strong argument for warfighting for deterrence. It is important to note that warfighting for deterrence is not just about having the right capabilities; it is just as much about having the will and the right mind-set to approach war avoidance from the perspective of battle.

2.1 Enhanced Credibility

Any deterrence threat must be credible. The enemy must believe that there is a reasonable chance that your threats will be fulfilled. In the Cold War, the challenge was to persuade another state that you were prepared to initiate and/or risk nuclear holocaust, even in response to limited provocations. Credibility, though, is not just an issue for nuclear deterrence. It is a requirement for all forms of deterrence, including the cyber variant. As will be discussed in greater detail below, for punishment forms of cyber deterrence to work, states that rely upon the free flow of information across networks must persuade each other that they are willing to unleash harmful malware into cyberspace.

When we discuss the credibility of deterrence, we cannot restrict our musings to the abstract. Context is everything. This is a central theme of the ‘fourth wave’ of deterrence theory (Knopf 2010), which has developed in the post-Cold War period, but is also evidenced in work of a more classical vintage. As Herman Kahn (1960) warns, deterrence has to work in an infinite number of possible scenarios. In this sense, deterrence must be flexible. It must be credible enough when dealing with various issues and various actors. In this way, Lawrence Freedman (2004, 40–42) describes deterrence operating in a general and immediate sense. The former operates in the background of a security relationship, deterring provocative actions without the expressed intention of doing so, whereas immediate deterrence deals with an existential crisis with the deliberate intent to deter. Another way of approaching this issue is

'tailored deterrence', whereby deterrence posture is cued to the specific actor and situation at hand (Knopf 2010, 8).

Warfighting enhances credibility by making it more likely that the threat will be enacted and objectives fulfilled. This is one of the strengths of conventional forms of deterrence (Stone 2012). By default, conventional forces are procured with combat in mind. In contrast, nuclear weapons are hampered by their initial association with war avoidance (Brodie 1946). Without extant capabilities and plans to wage war (physical or virtual), the unleashing of military action risks much without any sense of order or purpose. Casualties may be inflicted and escalation is risked without control or an understanding of how the war will progress and be terminated. Such a deterrence threat would look empty, merely a desire rather than a committed intent. In contrast, a threat supported by the means to fulfil it looks, and indeed is, more tangible. It is not just the enemy that would be impressed. The state making the threat could do so with more confidence that should hostilities ensue, the conflict could be controlled and objectives pursued.

Warfighting is also important when dealing with context. A broad, existential deterrent threat, which may operate successfully as a general deterrent, may be unsuitable in certain contexts, at times of crisis (Kahn 1960). This is most evident in extended deterrence. The general threat to respond massively to a Soviet attack on the continental USA seemed plausible. However, that same threat, which would involve the almost certain destruction of the USA, lacked credibility when seeking to deter limited Soviet gains in Europe or Asia. For these other security interests, the USA needed a more detailed deterrence story to sell to the Soviets and their allies. Specifically, the USA had to show that it could fight a controlled limited form of nuclear war. Being seen to have the capabilities and will for limited nuclear war made resort to the ultimate weapon more probable. In this way, warfighting enhanced credibility. Escalation remained important though. By this mechanism, LNOs made the deterrent threat more likely, but it was the prospect of global Armageddon that underwrote the deterrence posture.

2.2 What if Deterrence Fails?

Strategy must go beyond deterrence (Gray & Payne 1980, 19). Even if the overwhelming objective is to avoid conflict (Brodie 1946, 76), the strategist must plan for a post-deterrence world. To do otherwise would be an act of strategic negligence. Once war begins, for whatever reason, it must be prosecuted in a controlled manner in the pursuit of policy objectives. Moreover, having the ability to wage controlled forms of war ensures that intrawar deterrence is able to function.

Deterrence may fail for a range of reasons (Payne 2001, Wolf 1991 & Wieseltier 1985). The enemy may be beyond deterrence. His policy objectives may be of such import that he will accept any costs in their pursuit. Alternatively, his rational decision-making may be constrained by organisational, psychological or intelligence reasons (Morgan 1977). The aggressor may perceive vulnerability in the military posture of the victim state. He may identify a technological or operational opportunity that he is willing to exploit. This is an apparent weakness of conventional deterrence postures (Stone 2012). Perhaps more worryingly from a rational actor perspective, war may begin by accident.

This point jars against the Clausewitzian position that war is always a rational tool of policy (Clausewitz 1978). However, the military technological situation in the Cold War was such that accidental nuclear war was a danger (Blair 1993). This point is not just of historical interest. Accidental cyber conflict is not beyond the realms of possibility. The unpredictability of cyber attack, allied to the complexity of global information networks, makes accidental cyber conflict plausible. Deterrence may also fail due to miscalculation. The Falklands War and the Iraqi invasion of Kuwait are just two examples of a failure of general deterrence. In both cases, the aggressor state miscalculated the will of the dominant power.

The possibility of deterrence failure is of particular interest to current cyber studies. This is because at present cyber strategy is underdeveloped (Harknett et al. 2010, 1; Mahnken 2011, 57). None of the main cyber powers observably have a comprehensive cyber strategy that could cope with deterrence failure. *The DoD Cyber Strategy* (2015) is reasonably strong on cyber security and deterrence. However, it is noticeably light on offensive operations. A similar picture can be seen in the UK. Although Britain has publically discussed a retaliatory offensive capability (HM Treasury, 2015), details are light. As in the USA, UK cyber strategy is focused primarily on defence and deterrence, with the latter constructed primarily from denial and a norms-based approach (Lonsdale 2016). If cyber strategy is to advance, it must look beyond deterrence and fully develop a warfighting component. Not only will this strengthen the credibility of cyber deterrence, as noted above, it will enable the state to cope with deterrence failure and use cyber assets for the rational and controlled pursuit of policy.

2.3 Damage Limitation

One of the main objectives for warfighting has to be damage limitation should deterrence fail. Should conflict occur, the state has an obligation and interest in limiting harm to the nation-state. Damage can be curtailed either by defensive measures or by going after the offensive capabilities of the enemy. During the Cold War, this meant the development of advanced counterforce capabilities (to attack enemy nuclear forces), including Multiple Independently Targetable Re-entry Vehicles (MIRV) for increased penetration. More controversially, it also included discussion of ballistic missile defences. Rather obviously, depleting the enemy's offensive forces reduces their ability to inflict harm on the state. Active and passive defences achieve the same end. Indeed, the most potent nuclear warfighting stance merges these two approaches (Gray 1984). Depleted Soviet nuclear forces would have been an easier proposition for active and passive US defences.

Damage limitation is not merely designed to ensure a better conflict outcome. It further enhances the potency of deterrence. If the enemy's offensive capability is reduced, he may perceive that his objectives are unobtainable. This is countervailing strategy and deterrence by denial working in harmony. Moreover, threats to his military power from advanced offensive forces may also deter via the threat of punishment. This is especially the case if his military forces and command and control infrastructure are central elements of his political power. Furthermore, since military assets are often co-located with civilian and industrial assets (countervalue targets), punishment against his socio-economic infrastructure is also likely.

2.4 Theory of Victory

The discussion of victory in nuclear war is problematic to some (Howard 1983, 142–144). It seems fanciful, perhaps obscene, to seek positive outcomes amongst the desolation of a nuclear holocaust. Nonetheless, even though victory is likely to be pyrrhic in a large nuclear conflict, still it must guide strategy (Gray & Payne 1980). Without a theory of victory the prosecution of war has no direction, no purpose. Thus, forces corralled for deterrence must be primed to execute war-winning missions should deterrence fail. Merely having offensive forces is not enough. These forces need a strategy that works in the context of the nature of the enemy and sought after policy objectives. This is what we mean by a theory of victory: the ability to pursue policy objectives in the face of the enemy.

This raises an interesting question over whether large-scale war, especially nuclear war, can serve rational policy objectives. Some (Freedman 1989) regard nuclear weapons as astrategic. That is, without rational policy utility. From this perspective, discussion of victory is nonsensical. This is not just because nuclear weapons are unimaginably destructive. It is also argued that nuclear conflict cannot be controlled adequately to serve rational policy goals. It may be that cyber attack suffers a similar, albeit much less catastrophic, fate. And yet, regardless of the destructive potential and/or uncontrollable nature of war, strategy must be enforced even in the most inauspicious of circumstances. To do otherwise is simply to condemn oneself to mindless violence. Thus, here again, we have the need for warfighting. However, we have now gone beyond countervailing. We are now in the realms of prevailing, which may further strengthen deterrence if the enemy adopts a conservative stance to prevent a conflict that would lead to our victory.

2.5 Just War

Just War is prohibitive in nature (Dipert 2010, 394). It seeks to restrain the violent tendencies of war. At the same time, moral concerns demand a warfighting posture. Indeed, one could argue that the moral legitimacy of deterrence (avoiding war) extends to warfighting for deterrence because the primary intention to deter requires a secondary intention to use. And, as Gray (1984, 17) reminds us, the Just War tradition requires that war be fought for a better future, with reasonable prospects for success, using discrimination and proportionality to minimise harm to non-combatants. All four of these moral requirements call for warfighting. In the nuclear context, the alternative to warfighting-based deterrence would have breached all four of these requirements on a massive scale. In the absence of workable, flexible war plans, nuclear deterrence (and hence nuclear attack should deterrence fail) could only be based on massive countervalue punishment strikes against urban areas with no understanding of how victory or war termination could be achieved. Contrastingly, a warfighting approach is characterised by counterforce strikes to degrade enemy forces and their command and control. These attacks would be undertaken in a bid ‘to compel our enemy to do our will’ (Clausewitz 1978, 75), namely, to achieve victory.

Of course, warfighting for deterrence raises certain ethical concerns. Threatening and preparing for war in such an advanced manner may make war more likely. This is especially troublesome in a tense nuclear standoff, when, for technical and operational reasons, forces are on a high state of alert. Deploying advanced counterforce capabilities could make the enemy nervous about the survivability of his retaliatory capabilities. More philosophically, one could argue that the moral relationship between deterrence and warfighting is not as close as argued above. Michael Novak (1983, 37 and 97) argues that once deterrence fails it is not deterrence that is under ethical scrutiny. Rather, a new stage has been initiated, in which the use of force must be assessed on its own merits and not given moral leeway for underpinning the threat to avoid conflict. In response, one could argue that to disassociate the threat of force from its use in the pursuit of moral judgement completely ignores the strategic basis upon which deterrence functions. There can be no effective deterrent without the real threat of force in use. Moreover, the threat of force has moral consequences that cannot be ignored. The wrongful intentions criteria suggest that moral judgements applied to the enactment of the threat must also be applied to the latent threat. This latter position is rejected by Gregory Kavka (1987, 82), who argues that 'the Wrongful Intentions Principle fails when applied to a conditional intention adopted solely to prevent the occurrence of the circumstances in which the intention would be acted upon'.

2.6 Problems with Warfighting for Deterrence

A strong case has been made for the necessity of warfighting for deterrence. Not only is the credibility of deterrence enhanced, robust warfighting capabilities ensure that strategy continues to function in a post-deterrence environment. Despite the apparent need for warfighting, it does not automatically follow that it will work. An obvious problem for nuclear warfighting, and one that seems potentially as problematic in the cyber domain, is the co-location of targets. The advantages of warfighting are largely premised on the idea that it offers a more controlled, discriminatory and rational approach to deterrence and post-deterrence operations. However, this vision begins to break down somewhat if counterforce and countervalue targets cannot be adequately separated.

A related problem is that of escalation. For many reasons the rational control of war could be undermined. This is true in a general sense, as Clausewitz makes clear in his writings on friction and the fog of war (Clausewitz 1978). However, it is arguably more acute within the chaos of a nuclear conflict, and perhaps also in the cyber domain. The overlap between public and private networks, and the mutual dependency this creates, produces greater levels of uncertainty and nonlinearity within the complex architecture of cyberspace. Within such a setting the escalatory dynamics of war could have a field day.

Once deterrence fails, warfighting-based threats must succeed in the crucible of conflict. The operationalisation of pre-conflict plans and threats is fraught with difficulties. Thus, the many positive reasons for adopting a warfighting deterrence posture may not come to pass, or may do so at significantly higher costs. Friction is an ever-present thorn in the side of operational efficacy. Moreover, the enemy may be far more resilient and wily than assumed. In addition, key targets, regarded as essential for damage limitation and victory, may be beyond reach. This is just a snapshot of the

numerous obstacles to warfighting success. Strategy is a difficult beast to master (Lonsdale 2007; Gray 1999; Luttwak 1987; Jablonsky 2004) Thus, we must be conscious of the fact that warfighting for deterrence can fail in its primary goal of avoiding conflict. Additionally, it may fail in its secondary objectives of delivering damage limitation and victory.

Finally, we must return to the security dilemma. As indicated above, one of the major concerns regarding warfighting for deterrence is that it undermines the very thing it is designed to achieve. Perhaps, the most important watchword in Cold War nuclear strategy was 'stability'. Despite the obvious problems with MAD—not least that it threatened global Armageddon with no real means of defence—it was embraced by many as the surest way to maintain stability. Indeed, the stability offered by MAD was enshrined in the SALT and ABM treaties. These treaties exemplify an arms control regime that included an almost complete prohibition on missile defences and severely limited the deployment of counterforce weapons. This suggests that robust warfighting capabilities may threaten stability and precipitate conflict. However, this narrative only works if we accept the technological approach to stability, and ignore the political dimension. (Gray 1992) If war is a continuation of political intercourse, then it stands to reason that the causes of war are to be found in politics, not technological balances. That being said, force development and deployment can signal political motivations, and thereby can have an effect on political relations.

3 Warfighting for Cyber Deterrence

Having established the credentials for warfighting for deterrence, this paper will now assess whether such an approach is suitable for cyber deterrence. In the first instance, we must deal with the issue of whether warfighting language makes any sense in the cyber domain. Martin Libicki (2009, 328-330, 2012) bemoans the use of military metaphors for operations in the cyber domain. He argues that so-called cyber warriors do not fight. Rather, they reverse engineer. Consequently, he thinks it more appropriate to talk in engineering, architecture and administrative terms. In contrast, General Shaw, then UK Assistant Chief of Defence Staff, discusses offensive operations in terms of manoeuvre. He calls for full integration of cyber operations into the joint environment, noting that emphasis should be placed on the effect, not the means of delivery: '[cyber] is merely the latest medium though which to achieve effect.' (House of Commons Defence Committee 2012). Additionally, in their critique of cyber deterrence, Harknett, Callaghan and Kauffman (2010) call for a warfighting approach to cyber strategy, placing emphasis on the offence-defence dynamic.

In conceptual terms, much of the existing discourse on warfighting somewhat misses the mark. Warfighting is not restricted to tactical and operational details. Although both are required to fight in cyberspace, warfighting is really about strategy. It is about threatening and using force in a controlled manner in the pursuit of rational policy objectives. To reiterate, it is an approach to deterrence that rejects the emptiness of existential forms. Instead, it provides a deterrence posture with purpose, both in terms of credibility and the post-deterrence environment.

Let us now take the key issues raised earlier, and establish their suitability for the cyber domain.

3.1 Enhancing Cyber Deterrence Credibility

Without a clear understanding of how the threat will be operationalised, deterrence lacks credibility. Does this apply in cyberspace? Following strategic logic, the answer must be yes. Having the forces, plans, and command and control arrangements in place must enhance the credibility of a threat. The problem for cyber deterrence is communicating this to the enemy. Credible deterrence requires ownership of the capabilities to fulfil the threat, and the will to do just that. These two components must then be clearly communicated to the enemy. As Stone (2012, 117) notes, in sociological terms this is referred to as technology's 'interpretative flexibility', whereby the effects produced by a form of technology are constructed in a social context.

In the physical domain, forces can be displayed during parades or on military exercises. Additionally, military prowess and commitment may be evidenced from conflicts in the recent past. At first glance, these forms of communication appear not to fit with the virtual domain. After all, a May Day parade of malware is unlikely to attract the crowds or global media. And yet, cyber warfighting capability can be displayed. The establishment of Cyber Command in the USA and the UK's Defence Cyber Operations Group (DCOG) and the Joint Cyber Unit are evidence of increased cyber competence. On the defensive front, enemy probes of networks will reveal the strength of cyber defences. In addition, cyber exercises, such as Cyber Storm in the USA, which are designed to test the potency of cyber security, are an excellent means to communicate the strength of cyber defence, and in this way contribute to the potency of deterrence by denial.

Communicating the potency of cyber offensive capability brings its own challenges and solutions. Some cyber attacks use one-shot weapons that exploit zero-day vulnerabilities (Soloman 2011, 19). This means they are non-repeatable, because once altered the enemy can patch the vulnerability. In these circumstances, it is difficult to communicate a substantial ongoing threat. In which case, the punishment component of warfighting is more challenging in cyber attack. (Lindsay, 2015a, 54) Nonetheless, the scale of the cyber threat is well understood. As a means of offence, malware is an incredibly adaptive and relatively inexpensive form of weapon. A virus may contain as little as 125 lines of code. In contrast, security software uses over 10 million lines of code (Singer and Friedman 2014, 154). Add to that the fact that malware is often designed to evolve as it spreads, and we get a significant asymmetry in the offence defence relationship. (Geers 2011, 118; Harknett et al. 2010) Moreover, some attacks, especially Denial of Service (DoS), do not require fixable vulnerabilities. Rather, they rely upon the basic functions of the target system. None of this is designed to suggest that offence has an overwhelming advantage in cyberspace. Indeed, some analysts (Libicki 2009) argue the opposite. Rather, it is to suggest that the competitive dynamic will function in the cyber domain (Luttwak 1987). In which case, we can conclude that the offensive potential of cyber attack for warfighting deterrence is reasonably well established.

In some ways, it might be easier to signal capability and will in cyber attack. For obvious reasons, physical weapons cannot actually be used against the enemy without causing the conflict the deterrent threat is designed to prevent. Not so for cyber weapons. Malware can be inserted into a system to display capability and intent, without actually causing any harm. At present, it is not clear whether this would breach

state sovereignty or constitute an armed attack under international humanitarian law (Schmitt 2013; Waxman 2011).

Finally, it can be argued that offensive cyber warfighting capability is a more credible form of deterrence than many physical expressions of power—especially nuclear weapons. Although generally non-violent, cyber attack could lead to civilian casualties. It is certainly the case that widespread disruptive attack (WDA) would lead to negative effects on the standard of living. Moreover, in the cyber age, we must consider the moral value of informational objects and the potential for cyberharm (Dipert 2010; Taddeo 2014; Miller, 2016). Nonetheless, and despite melodramatic predictions from the likes of Richard Clark and Mike McConnell, who predict social breakdown and nuclear conflict levels of effects (The Economist 2010), it is likely that cyber attack would produce significantly less death and destruction than physical expressions of power. (Geers 2011, 118) In which case, a state is more likely to prosecute its deterrent threat (Libicki 2009, 72), and thereby the credibility of deterrence is enhanced. This is not a universally accepted position. Some commentators (Lindsay, 2015a, 57) argue that the possibility of civilian casualties and blowback from cyber attack will create self-deterrence, making policy makers wary of using the cyber instrument. As a result, denial is a more effective form of deterrence than punishment in the cyber domain (Denning 2015, 12). As will be argued in the third section of this paper, the most effective warfighting for deterrence posture would use both forms of deterrence.

The flipside of this argument is that if little damage were caused by cyber attack, then why would the enemy be deterred? A similar concern is evident in conventional deterrence. Relative to the guaranteed levels of destruction in nuclear retaliation, the ability of conventional response to inflict sufficient damage is open to question (Gerson 2009, 43). Doubts are even greater in the cyber domain. In this respect, there is a serious question mark hanging over the strategic efficacy of cyber attack. The most significant cyber attacks to date: Stuxnet, Wiper, Shamoon and Bronze Soldier, although technically and tactically impressive, did not produce lasting strategic impact (Valeriano & Maness 2015). This particular challenge to the deterrence efficacy of cyber attack can be countered, to some degree, by the same means identified earlier in relation to nuclear strategy. The limited effects of cyber attack make the threat more plausible, but the potency of the threat comes from the possibility of escalation to physical forms of conflict.

3.2 Damage Limitation

It has already been established that damage limitation is a moral and strategic responsibility for the state. Those in charge of strategy must plan for the possibility of deterrence failure. At the same time, an effective damage limitation capability enhances cyber deterrence, both through denial and by making resort to force more likely. As in the ideal form of nuclear warfighting, cyber damage limitation is best achieved with active and passive defences alongside offensive capabilities. However, in the cyber variant, defences are given priority.

Much of what follows should be read as an addition to the discussion above concerning the advantages and limitations of cyber attack. For the most part, then, the bulk of the effort for cyber damage limitation falls on defensive measures, although

there are some limited offensive counterforce options available. 'Search and destroy' and 'offensive security' are emerging capabilities, whereby attackers are identified, tracked and then neutralised with DoS attacks or malware (Informationweek 2013). More complete offensive options are also appearing: 'Such capabilities may operate in a number of valuable ways, including conducting reconnaissance and surveillance, intercepting communications, denying resources and access, compromising systems, undermining integrity, disabling or destroying assets, and manipulating, impeding, or demoralising an opponent.' (Rosenquist 2015) These offensive damage limitation approaches are controversial, primarily because those who benefit from to the free flow of information would have to restrict it in certain circumstances. Yet, they do offer the possibility of disabling enemy offensive capabilities that could cause harm to the state.

An important general concern raised about offensive cyber capabilities is whether they can cause enough predictable harm to the enemy to act as an effective deterrent (Libicki 2009, 53) and/or an instrument of damage limitation. One possible response is cross-domain action. In this way, we should not regard cyber capabilities as stand-alone tools. Rather, they are but one option within a range of possible responses. This is certainly the option taken by the US (Department of Defense 2015). Physical attack options could be used to eliminate the sources of enemy cyber attacks. Of course, as with so many issues in cyber security, we run into the problem of attribution. However, this particular problem may have been oversold somewhat. Cyber intelligence capabilities are improving (Rid & Buchanan 2014) and the anonymity of large-scale attacks is difficult to maintain (Lindsay, 2015a, b, 56).

When discussing deterrence in general terms (although not perhaps for nuclear strategy), defensive measures are often preferred over offensive punishment actions. This is because, as Freedman (2004, 39) notes, denial is more reliable because it is subject to greater levels of control. Whether or not the enemy is deterred by threats of punishment is largely his decision. Whereas, one has a degree of control over how effective defensive options are – with the caveat that the enemy may develop a clever counter. The same principle can be applied to cyber deterrence warfighting capabilities (Singer and Friedman, 2014; Lindsay, 2015a, 54). Therefore, cyber damage limitation relies primarily on the elements of good cyber security. These include efforts at the individual or business level, such as educational programmes to improve cyber hygiene, in addition to state-level actions to provide fight through resiliency and redundancy for the economy and critical infrastructures (Soloman 2011, 21).

3.3 Theory of Victory

What does victory look like in a cyber conflict? How should it be pursued? The answers to these questions are largely dependent upon context. Strategy should always be conducted with the policy objectives and the nature of the enemy clearly in mind. Only when these two factors are understood can a legitimate theory of victory be identified. Context is everything. If the object of war is to impose our will on the enemy, then we must seek to understand what the enemy values, where is his centre of gravity? Once this is understood, the campaign can be planned and targets chosen. During the Cold War, US targeting policies increasingly focused on the Communist Party's instruments of political control, which included decision-making centres and

their military and security services (Gray 1984). As previously noted, these more nuanced forms of posture have increasingly come to the fore in tailored deterrence.

In the contemporary cyber security environment China poses the most prominent threat to the US and its allies. It has an active cyber espionage programme for industrial and military advantage, regards cyber attack as a means to deter the US from interference in its affairs, has a doctrine of first strike (Pollpeter 2015, 139–153), but suffers from a degree of chaos in its cyber security efforts (Lindsay 2015b, 8). On this evidence, it would seem that a warfighting approach would serve the interests of the US well. Bearing in mind the nature of the Chinese state, the US would be well placed to focus its efforts on information control. In contrast to the West, which values the free flow of information, the Chinese government seeks to control information flow in order to prevent challenges to its authority (Lindsay 2015b, 10).

This sounds like a sensible approach. And yet, in terms of a theory of victory it is difficult to gauge the strategic impact of information manipulation. Despite claims of a long and distinguished history, accurately identifying direct policy casual effect from information manipulation is difficult (Barnett and Lord 1989). The information environment is dynamic and extremely competitive, and the target (in this case the political culture of a state) is ethereal. Thus, the results of a campaign are uncertain, and cannot be relied upon to provide direct attainment of most policy objectives.

The same cautious conclusion can be made with regards to more aggressive forms of cyber attack against critical infrastructure and specific targets. As has already been noted, the largest attacks to date have not proven especially effective in the pursuit of policy. To add a little detail to support the analysis, the attack on the Iranian nuclear programme, Stuxnet, provides a case in point. Strategically, the results of Stuxnet were somewhat muted. According to Sanger, Stuxnet destroyed 984 centrifuges (11.5% of the capacity at the facility). That sounds impressive, until you learn that the IAEA estimates normal failure rate at 10%. The IAEA also reports that the slack was taken-up elsewhere in the system, thereby minimising impact on the Iranian nuclear programme (Valeriano and Maness 2015, 153–154). Stuxnet was not cheap either. Reportedly, it cost approximately $300 million to develop (Valeriano and Maness 2015, 151). This is significant, especially when one learns that it was ‘quickly and effectively disarmed.’ (Farwell and Rohozinski 2011, 27).

The unavoidable conclusion from this analysis is that effective theories of victory are difficult to clearly identify in cyber attack. Yet, theories of victory must be developed. They enhance credibility and provide a legitimate strategic focus if deterrence fails. It is to be remembered that victory was unlikely in nuclear war. However, a theory of victory was essential, otherwise strategy would cease to function just when you need it most: when the fighting has begun. Moreover, we should note that victory can take many different forms. It may be that the primary policy objective, as in the case of UK cyber security strategy, is to defend British cyber activity, making ‘the UK one of the most secure places in the world to do business in cyberspace’ and ‘to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace’. (Cabinet Office 2011) Alternatively, cyber victory may entail making an effective contribution to a joint campaign. This was evident, for example, in the 2007 Israeli attack on the Syrian nuclear facility at Kibar. Prior to the air assault the Syrian air defence network was hacked, leaving Israeli jets a free run to their targets (Singer and Friedman 2014, 127).

3.4 The Failure of Cyber Deterrence?

The potency of cyber deterrence is difficult to judge. This is partly because there exists no consensus on what constitutes an act of sufficient cyber aggression. Therefore, it is not entirely clear what is to be deterred. Where exactly the threshold for response should be will be discussed in section three of this paper. For now, we can state that low-level nuisance attacks are a daily occurrence. For example, U.S. military networks are probed and scanned millions of times each day (Work 2015, 1). Similarly, acts of cyber espionage are reasonably common. However, what is also evident is the lack of major cyber attacks. For a while, Stuxnet, Wiper, Shamoon and Bronze Soldier appeared to signal the rise of cyber attack as a potent new instrument of policy. However, medium to large-scale attacks have essentially dried-up. Indeed, reflecting the empirical evidence, and marking a shift in tone, in his September 2015 testimony to the Senate Armed Services Committee, Director of National Intelligence, James Clapper, talked down the possibility of an 'electronic Pearl Harbor'. Instead, he focused on ongoing 'low-to-moderate' level threats (Clapper 2015, 2).

What does this all tell us? Is deterrence working? If one considers low-to-moderate threats as deterrable, then the answer would seem to be no. From this perspective, and according to some policy makers, deterrence is already failing. In a 2015 Senate Armed Services Committee Hearing, Chairman John McCain was scathing in his assessment: 'Our adversaries view our response ... as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequence of continued cyber attacks against us outweigh the benefit.' (Takala 2015) However, if we take the view that cyber deterrence should really concern itself only with large-scale attacks, the picture is more positive. Indeed, Valeriano and Maness (2015) have identified considerable levels of restraint in state cyber behaviour. This could be due to a lack of confidence in the strategic utility of cyber attack. It may also reflect the development of norms against aggressive forms of cyber behaviour and the efficacy of deterrence. Indeed, norms increasingly form part of 'complex deterrence', within which military and non-military elements operate together. In cyberspace, although a settled understanding of universal rules of behaviour is still lacking, norms appear to be crystalising around acceptable forms of intrusion rather than a blanket non-use position (Stevens 2012, 25). This may explain the continuance of low-level probes whilst large attacks have trailed off.

Overall, it is reasonable to conclude that despite the absence of large-scale cyber attacks, offensive cyber operations are too prevalent. This is especially the case in relation to espionage incidents. Senator McCain may be right; deterrence is failing at some level. This is perhaps because the US does not observably have an adequate post-deterrence posture in place. Although elements of it can be identified, a comprehensive cyber strategy is still missing in action. One glaring omission from that strategy is an effective cyber warfighting capability.

3.5 Just War Cyber Ethics

It has been established that warfighting for deterrence has a strong moral component. By providing the means for a controlled rational use of force in a post-deterrence environment, warfighting offers the possibility of doing more good than harm (relative

to the use of force devoid of plans); fighting a campaign characterised by discrimination and proportionality; and with a greater chance of success. The question we must address in this section is whether warfighting for cyber deterrence possesses these qualities. The answer to this question is complex because cyber warfare demands a new ethical framework, fashioned by merging traditional Just War with Information Ethics (Taddeo 2012). From an ethical perspective cyber deterrence is paradoxical (Arquilla 2016, viii). It appears to offer bloodless means and threats to pursue policy, and therefore has enhanced credibility (Dipert 2016, 64) and less impact on the physical and psychological wellbeing of those involved. On the other hand, it may lack discrimination, produce novel forms of harm, and produce a more expansive form of conflict, leading to more instances of fighting amongst states and other actors. In line with the warfighting framework presented earlier, this section will now discuss warfighting for cyber deterrence in relation to three issues: providing a better outcome; discrimination and violence; and proportionality. Whether cyber war promotes the possibility of success has already been discussed.

War always produces pain and suffering. The Just War tradition recognises this, and therefore demands that the post-conflict outcome be superior to that had the conflict not been fought. One means to achieve this is to minimise destruction in war. Warfighting for cyber deterrence appears to offer a preferable means to maximise post-conflict social wellbeing should deterrence fail. By offering a rational controlled use of cyber power in the event of war, cyber warfighting offers a form of attack that is largely non-destructive and often immediately reversible in its effects (Dipert 2010, 392). With these characteristics it may be possible for critical infrastructure to survive a conflict intact. Once the fighting stops, society and the economy can quickly return to pre-conflict conditions. Moreover, a strong cyber defence (including resilience), which must be an integral part of a warfighting strategy, further shores-up the continued functioning of critical infrastructure.

The above presents an ideal vision of cyber conflict. However, it is important to note the areas were cyber attack could cause harm to social wellbeing. First, the idea that cyber attack is controlled and limited is open to question. The mechanisms by which cyber weapons operate are not well understood (Barrett 2013, 10). Once malware is released, it often spreads beyond the initial target. Thus, the effects on critical infrastructure, and therefore social wellbeing, are uncertain. Indeed, one can go further and note that coercive forms of cyber attack are often aimed against infrastructure 'and can inflict serious damage to contemporary information societies' (Taddeo 2014, 37). Attacks against infrastructure are the means by which the public will is targeted and pressure put on decision makers. Finally, we have to consider the issue of cyberharm. It is no longer sufficient to assess suffering purely on a physical basis. Increasingly, the virtual domain and its objects are afforded moral value (Taddeo 2014). The Internet is essential for modern life (Canetti et al. 2016, 165), and thus a sustained, or even a temporary (Barrett 2013, 6), interruption of that service must be included in calculations of harm.

With its propensity for non-violence, cyber conflict has been described as an ideal form of war (Jenkins, 2016, 89). It takes the protection of non-combatants to another level. This positive tendency is magnified by the possibility of extreme discrimination in targeting. As George Lucas notes, Stuxnet is illustrative of this: 'Unless you happen to be running a large array of exactly 984 Siemens centrifuges simultaneously, you

have nothing to fear from this worm.' (Singer & Friedman 2014, 119). It is because of non-violence and discrimination that Stuxnet, as a harbinger of things to come, has been described as the 'first purely ethical weapon' (Lucas 2016, 28). We see here a massive shift from nuclear deterrence. In the event of nuclear deterrence failure, a warfighting approach will seek to control and limit damage, but would still likely result in millions of casualties. In contrast, warfighting for cyber deterrence promises zero casualties in the event of deterrence failure.

This rosy outlook is once again tempered if we consider that cyber attack can produce casualties, potentially on a large-scale. Disrupting power supplies could affect vulnerable members of society (the elderly and those in hospital, for example). Attacking nuclear power plants or air traffic control would have obvious consequences for the civilian population. Moreover, as already indicated, the difficulty of controlling certain forms of cyber attack could lead to serious breaches of the discrimination criteria (Rowe 2007). A cyber campaign could also create new targets for physical reprisal. IT workers, who are often civilians contracted to the military, could become legitimate targets if they directly participate in hostilities (Henschke & Lin 2014; Dunlap 2012), even if those hostilities are themselves non-violent. Moreover, we should not overlook cyberharm and its effects on the population, or indeed the psychological harm that results from social dislocation (Canetti et al. 2016, 158).

To be just, the use of force has to be proportionate to the issue at hand and military requirements. For this to occur, force must be driven by a rational and controlled process. Warfighting for cyber deterrence promises just that by placing limits on the use of force and its consequences. Virtual incursions, although open to some discussion regarding their legal status, are not on the same scale as physical breaches of state sovereignty. The less-invasive character of cyber actions (Lucas 2016, 13), added to the reversibility of effect, suggests that political fallout will be more limited, as will the dangers of conflict escalation. The generally non-violent nature of cyber conflict adds further to this positive effect, and means cyber deterrence threats are less drastic.

And yet, the potential for unpredictability in cyber attack suggests a degree of caution is required. Furthermore, one of the greatest dangers of action in the cyber domain is that it could lower the threshold of conflict (Jenkins 2016, 108). The cyber variants of crime, espionage, sabotage and war share such similarities at the tactical and operational levels, that the distinctions amongst them are blurred. Thus, there exists the danger of rising tensions in international politics and greater propensity for conflict, with the danger of escalation to the physical realm. In this way, limited cyber actions could have wildly disproportionate results. This danger is exacerbated by the fact that cyber attack undermines neutrality and trust (Rowe 2007; Schmitt 2013). The attribution problem, alongside the practice of routing attacks through numerous states, risks spreading suspicion and tensions throughout the international system (Barrett 2013, 9). These features also complicate the application of international law. Moreover, if cyber attack is considered a casus belli, states may find themselves increasingly at war with a range of non-state actors who operate in and through cyberspace (Eberle 2013, 60).

We can conclude from an ethics perspective that warfighting for cyber deterrence is somewhat of a mixed bag. It offers the promise of non-violent, proportionate and discriminating threats and use of force. However, this promise may be undone by the unpredictability of cyber attack, new forms of harm, and the fact that it potentially lowers the threshold of conflict. And yet, once again we must conclude that this is still

preferable to not having a developed warfighting capability. In the absence of the latter, a failure of deterrence is likely to lead to even greater levels of unpredictability and harm.

4 Warfighting for Cyber Deterrence: a Model

It has been established that warfighting for deterrence can function in the cyber domain. Despite challenges and shortcomings, it is evident that a warfighting stance is required for enhanced credibility and to cope with the post-deterrence environment. But what does warfighting for cyber deterrence actually look like? We can look once again to nuclear warfighting for an appropriate analogy. As Gray (1984, 21) argues, warfighting demands a balanced approach containing both offensive and defensive components. Specifically, nuclear warfighting required precision offensive forces, civil (passive) defence, and ballistic missile defences (active defence) (Gray & Payne 1980, 25). Translated into cyber deterrence, we can envisage the following balance of capabilities: a cross-domain offensive retaliatory capability (including non-military response, such as sanctions); active defences comprised of offensive security measures, firewalls, password security etc.; and passive defences including resiliency and redundancy. As a unified approach this would provide the ability to fight a cyber war by defending critical infrastructure, networks and information; maintaining socio-economic functions; and inflicting harm on the enemy to achieve policy objectives (victory). The paper will now explore this model of cyber warfighting in more detail. Prior to that, we must just deal with the question of thresholds.

4.1 Thresholds

What actions would cause the failure of cyber deterrence? At what point would a retaliatory response be triggered? This issue is complicated by differing perceptions of harm in cyberspace. The USA and China, for example, have very different ideas about the importance of 'content', and whether or not the flow of information can cause harm to the state (Iasiello 2014, 57). When we talk about response, we are clearly discussing offensive retaliatory actions, since non-aggressive defensive measures will be in play by default. Deterrence by denial can function with no reference to thresholds.

The Director of National Intelligence, James Clapper, describes the current environment as permissive in reference to thresholds. He bemoans the lack of response from victims, arguing that this encourages the continuation of low-level attacks (Lindsay, 2015a, 63). Whilst this may be true, the regularity and number of cyber probes and intrusions suggests that a zero tolerance approach to the threshold issue is a non-starter (Libicki 2009, 65). A degree of cyber infringement must be tolerated. Indeed, being overly enthusiastic in one's response could prove counterproductive. Jon Lindsay (2015a, 63) argues that tolerance of low-level intrusions may be necessary in order to enhance the credibility of response to attacks against critical targets. Having the intention to respond to every minor attack or intrusion runs the risk of devaluing retaliatory response. The attribution issue magnifies this problem. Small incursions may remain anonymous or be tracked to enemies with little to retaliate against. When a retaliatory threat is made, but not fulfilled, one's overall deterrence credibility is reduced.

Jonathan Soloman (2011, 12) suggests one solution: a threshold that mirrors the current legal definitions of 'armed attack'. However, such an approach ignores the notion of cyberharm, and probably sets the threshold too high, leading to the danger of being virtually nibbled to death. It is clear, then, that a cyber-dependent state cannot threaten to retaliate to every pernicious action in the cyber domain. And yet, warfighting for deterrence demands some form of offensive response. Moreover, what appear to be relatively low-level incursions could be the prelude to something more threatening. Espionage incidents, for example, although relatively harmless individually, cumulatively could have a substantial impact, and indeed could be preparation for a larger attack (Beard (2016), 153).

The answer to these dilemmas may lie in a cross-domain version of flexible response. A state should arm itself, in terms of capability and will, with the ability to respond across the spectrum, ranging from political and economic sanctions to physical military retaliation. To ensure proportionality and credibility, this would include various cyber retaliatory responses shaped to the nature of particular enemies. Within this flexible response posture, it is advisable to have thresholds of differing solidity. At lower levels of attack, thresholds could be more adaptive. A greater degree of ambiguity at these lower levels would allow the state to measure the nature and cumulative effects of attacks, and then harden the response as required. At the same time, it should be made clear that attacks against critical infrastructure and valuable assets will not be tolerated. A unified warfighting approach provides the wherewithal to operate in this flexible manner.

4.2 The Model

Due to the challenges of retaliatory actions in the cyber domain, which include attribution and the limited efficacy of cyber attack, denial should be given priority in our warfighting for cyber deterrence model. There is some empirical basis for this conclusion. As Goodman (2010, 111) notes, Estonia was able to resist the cyber attack it suffered in 2007 – meaning that it refused to move the bronze statue of the Soviet soldier – via defensive measures rather than resorting to punishment forms of retaliation. The latter was off the table for two main reasons. First, although Russian involvement was strongly suspected, it could not be verified. Second, even had Estonia wished to retaliate against Russia, the latter's cross-domain escalation dominance—superiority in all forms of military power—ruled out that course of action. Importantly, because denial is predominately defensive in nature, it does not rely upon attribution. That does not mean that denial is inert. It must be committed to as part of an overall warfighting for deterrence approach. A certain amount of work is required to keep active cyber defences current and to provide the required resiliency and redundancy needed for passive defence.

Despite the priority given to defensive capabilities, denial is not enough (Gray 1984, 10). As deterrence fails and the higher thresholds are breached, offensive options are required for damage limitation, enhanced intrawar deterrence and the pursuit of victory. Of course, denial continues to function for intrawar deterrence and as part of damage limitation. However, offensive actions now join the fight to degrade enemy capability (damage limitation), for intrawar deterrence through the infliction of punishment, and to pursue any policy objectives amenable to compellent offensive actions. These

offensive actions must be cross-domain. What we are discussing here is a flexible comprehensive strategic approach to enhance deterrence against cyber attack, but one that also enables a rational and flexible pursuit of policy in the event of deterrence failure. In this way, cyber warfighting operations join their kinetic cousins in utilising the 'power to hurt' (Schelling 1966) for both intrawar deterrence and compellence should conflict occur.

An important element in this picture, and another one that harks back to Cold War deterrence, is escalation dominance. Although it does not use the exact term, the DoD aspires to escalation dominance when it discusses the desire to 'control conflict escalation' (Department of Defense 2015, 8). Escalation dominance is an essential component of both pre-conflict and intrawar deterrence. Having escalation dominance facilitates a greater degree of control over dynamic conflict relationships (Kahn 1965). Put simply, if one is dominant at the next level of conflict escalation, the enemy is less likely to go there and deterrence is more likely to hold.

5 Conclusion

This paper has introduced the concept of warfighting to the cyber deterrence discourse. Thus far, discussions on cyber deterrence have rarely looked beyond the point of failure, nor do they convincingly link post-deterrence capabilities with the credibility of pre-conflict deterrence. This is largely because deterrence is often regarded as a self-contained strategy, whereas in fact, deterrence must be seen as one component of grand strategy, seamlessly integrated with other strategies in the pursuit of policy objectives and relevant to both conflict and peace. In order to introduce warfighting into the debate in a rational manner, this paper used nuclear warfighting theory, with additional references to conventional deterrence, to provide a structured conceptual framework.

The analysis of nuclear warfighting deterrence identified five rationales: enhanced credibility, dealing with deterrence failure, damage limitation, providing a theory of victory and adherence to moral obligations from the Just War tradition. These were then applied to cyber deterrence to discover whether or not the latter required and could accommodate a warfighting dimension. It was found that warfighting is imperative for effective cyber deterrence. Not only would it enhance credibility, it would also increase the chances for cyber power to act as a rational tool of policy in the event of conflict.

On this basis, a model was developed outlining what warfighting for cyber deterrence should look like. Thresholds should operate on an adaptive basis. To cope with the proliferation of intrusions, thresholds should be somewhat ambiguous at lower levels of threat, with the ability to harden as risks develop. Greater threats against high value targets demand a clearer threshold of response. Responses should be cross-domain and based on a flexible spectrum of options, ranging from political and economic sanctions to physical military action if required. The nature of cyber threats suggests that defensive denial measures would take the lead. However, for enhanced deterrence, intrawar deterrence, damage limitation, and in the cause of victory, offensive cross-domain options are essential.

Cyber deterrence is evolving in a positive direction. What is required now is a greater focus on strategy, understood to mean the use of instruments in the pursuit of policy. To achieve positive strategic effect cyber deterrence must be guided by the Duke

of Wellington's straightforward rationale—defeating the enemy. Thereby, the credibility of cyber deterrence will be enhanced, as will the ability to prosper, or at least minimise harm, in the post-deterrence environment.

Compliance with Ethical Standards

Funded Research This research was funded by the Economic and Social Research Council, as part of the Partnership for Conflict, Crime and Security Research: Ethics and Rights in a Security Context. The project title is *Common Good: Ethics and Rights in Cyber Security.*

References

Arquilla, J. (2016). Foreword: ethics for the coming epoch of conflict. In F. Allhoff, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of Cyberwarfare* (pp. vii–xii). Oxford: Oxford University Press.

Barnett, F. R., & Lord, C. (Eds.). (1989). *Political warfare and psychological operations*. Washington, DC: National Defense University Press.

Barrett, E. T. (2013). Warfare in a new domain: the ethics of military cyber-operations. *Journal of Military Ethics., 12*(1), 4–17.

Beard, M. (2016). Beyond Tallinn: the code of the cyberwarrior. In F. Allhoff, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of cyberwarfare* (pp. 139–156). Oxford: Oxford University Press.

Blair, B. (1993). *The logic of accidental nuclear war*. Washington, DC: The Brookings Institution.

Brodie, B. (1946). *The absolute weapon*. New York: Harcourt Brace.

Cabinet Office (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Canetti, D., Gross, M. L., & Waismel-Manor, I. (2016). Immune from Cyberfire? The psychological and physiological effects of cyberwarfare. In F. Allhoff, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of cyberwarfare* (pp. 157–176). Oxford: Oxford University Press.

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

Clausewitz, C. (1978). *On War*. Princeton, NJ: Princeton University Press.

Denning, D. (2015). Rethinking the cyber domain and deterrence. *Joint Force Quarterly, 77*, 8–15.

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.

Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics., 9*(4), 384–410.

Dipert, R. R. (2016). Distinctive ethical issues of Cyberwarfare. In F. Allhoff, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of Cyberwarfare* (pp. 56–72). Oxford: Oxford University Press.

Dunlap, C. J. (2012). The intersection of law and ethics in cyberwar: some reflections. *Air and Space Journal, 24*, 1–17.

Eberle, C. J. (2013). Just war and cyberwar. *Journal of Military Ethics., 12*(1), 54–67.

Farwell, J. P. & Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', *Survival*, 53(1).

Freedman, L. (1989). *The evolution of nuclear strategy*. London: The Macmillan Press.

Freedman, L. (2004). *Deterrence*. Cambridge: Polity Press.

Geers, K. (2011). *Strategic cyber security*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Gerson, M. S. (2009). 'Conventional Deterrence in the Second Nuclear Age'. Parameters. Autumn. 32–48.

Goodman, W. (2010). Cyber deterrence: tougher in theory than in practice? *Strategic Studies Quarterly, 4*(3), 102–135.

Gray, C. S. (1984). War-fighting for deterrence. *Journal of Strategic Studies., 7*(1), 5–28.

Gray, C. S. (1992). *House of cards: why arms control must fail*. Ithaca: Cornell University Press.

Gray, C. S. (1999). *Modern Strategy*. Oxford: Oxford University Press.

Gray, C. S., & Payne, K. B. (1980). Victory is possible. *Foreign Policy, 39*, 14–27.
Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving deterrence behind: war-fighting and national cybersecurity. *Journal of Homeland Security and Emergency Management, 7*(1), 1–24.
Henschke, A. & Lin, P. (2014). 'Cyberwarfare Ethics, or How Facebook Could Accidently Make Its Engineers into Targets'. *Bulletin of Atomic Scientists*. 25 August.
HM Treasury. (2015). 'Chancellor's Speech to GCHQ on Cyber Security', 17 November 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.
House of Commons Defence Committee (2012). *Defence and Cyber Security, Sixth Report of Session 2012–13*, December 2012, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf.
Howard, M. (1983). *The causes of war and other essays*. Cambridge, MA: Harvard University Press.
Iasiello, E. (2014). Is cyber deterrence an illusory course of action. *Journal of Strategic Security., 7*(1), 54–67.
InformationWeek (2013). 'Offensive Cybersecurity: Theory and Reality'. *InformationWeek*. 21 January.
Jablonsky, D., (2004). 'Why is Strategy Difficult?', in J. B. Bartholomees (ed), *U.S. Army War College Guide to National Security Policy and Strategy*. http://www.au.af.mil/au/awc/awcgate/army-usawc/strategy2004/00376.pdf pp. 69–78.
Jenkins, R. (2016). Cyberwarfare as ideal war. In F. Allhoff, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of cyberwarfare* (pp. 89–114). Oxford: Oxford University Press.
Kahn, H. (1960). *On thermonuclear war*. Princeton, NJ: Princeton University Press.
Kahn, H. (1965). *On escalation: metaphors and scenarios*. London: Pall Mall Press.
Kaplan, F. (2016). *Dark territory: the secret history of cyber war*. New York: Simon & Schuster.
Kavka, G. S. (1987). *Moral paradoxes of nuclear deterrence*. Cambridge: Cambridge University Press.
Knopf, J. W. (2010). The fourth wave in deterrence research. *Contemporary Security Policy., 31*(1), 1–33.
Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica: RAND.
Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *I/S Journal., 8*(2), 321–336.
Lindsay, J. R. (2015a). Tipping the scales: the attribution problem and the feasibility of deterrence against cyber attack. *Journal of Cyber Security., 1*(1), 53–67.
Lindsay, J. R. (2015b). Introduction: China and cybersecurity: controversy and context. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cybersecurity: espionage, strategy, and politics in the digital domain* (pp. 1–26). Oxford: Oxford University Press.
Lonsdale, D. J. (2007). Strategy: the challenge of complexity. *Defence Studies, 7*(1), 42–64.
Lonsdale, D. J. (2016). Britain's emerging cyber strategy. *The RUSI Journal., 161*(4), 52–62.
Lucas, G. R. (2016). Emerging norms for cyberwarfare. In F. Allhof, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of cyberwarfare* (p. 28). Oxford: Oxford University Press.
Luttwak, E. N. (1987). *Strategy: the logic of war and peace*. Cambridge, MA: Belknap Press.
Mahnken, T. G. (2011). Cyber war and cyber warfare. In K. M. Lord & T. Sharp (Eds.), *America's cyber future: security and prosperity in the information age, volume II*. Washington, DC: Center for a New American Security.
Miller, S. (2016). Cyberattacks and dirty hands: cyberwar, cybercrime, or covert political action. In F. Allhoff, A. Henschke, & B. J. Strawser (Eds.), *Binary bullets: the ethics of cyberwarfare* (pp. 228–250). Oxford: Oxford University Press.
Morgan, P. M. (1977). *Deterrence: a conceptual analysis*. London: Sage.
Novak, M. (1983). *Moral clarity in the nuclear age*. Nashville: Thomas Nelson.
Payne, K. B. (2001). *The fallacies of cold war deterrence and a new direction*. Lexington, KT: University of Kentucky Press.
Pollpeter, K. (2015). Chinese writings on cyberwarfare and coercion. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cybersecurity: espionage, strategy, and politics in the digital domain* (pp. 138–162). Oxford: Oxford University Press.
Rid, T., & 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 A. Colaril & L. Janczewski (Eds.), *Cyber war and cyber terrorism*. Hershey, PA: The Idea Group.
Schelling, T. C. (1966). *Arms and influence*. New Haven: Yale University Press.
Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.
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*. December 18.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: Oxford University Press.
Soloman, J. (2011). 'Cyber Deterrence Between Nation-States: Plausible Strategy or a Pipe-Dream'. *Strategic Studies Quarterly*. 1–25.
Stevens, T. (2012). A Cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy., 33*(1), 148–170.
Stone, J. (2012). Conventional deterrence and the challenge of credibility. *Contemporary Security Policy., 33*(1), 108–123.
Taddeo, M. (2012) 'An Analysis for a Just Cyber Warfare'. In C. Czosseck, R. Ottis, K. Ziolkowski (Eds.). *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications. 209–218.
Taddeo, M. (2014). What ethics has to do with the regulation of cyberwarfare. *Ethics and Armed Forces., 2014*(2), 36–40.
Takala, R. (2015). 'Forget China—Russia the Real Cyber Threat, Says Admiral', *Washington Examiner*, 29th September. http://www.washingtonexaminer.com/forget-china-russia-the-real-cyber-threat-admiral-says/article/2573047.
The Economist (2010). 'War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?', *The Economist*, July 1st 2010, http://www.economist.com/node/16478792.
Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: cyber conflict in the international system*. Oxford: Oxford University Press.
Waxman, M. C. (2011). 'Cyber Attacks as Force Under UN Charter Article 2(4)'. *In* Pedrozo & Wollschleager (Eds.). *International Law and the Changing Character of War*. (pp. 43–57) Newport: Naval War College.
Wieseltier, L. (1985). 'When Deterrence Fails'. *Foreign Affairs*. Spring 1985.
Wohlstetter, A. J. (1959). The delicate balance of terror. *Foreign Affairs, 37*, 211–234.
Wolf, B. (1991). *When the weak attack the strong: failures of deterrence*. Santa Monica: RAND.
Work, R. O. (2015) *Opening Statement Before the Senate Armed Services Committee*, September 29.