Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?

Craig B. Greathouse

Abstract Warfare in the future will be different from warfare in the past, but are the classic theorists still viable capable of providing insight into the nature of war, conflict, and policy within the realm of cyber war? While a significant amount of work has been directed towards the possibility of cyber war and explaining what it might look like, there is a limited focus on strategic options which states might select in this emerging field. The chapter first offers a typology to view issues of cyber conflict. Second it offers an examination of possible strategic choices for policy makers based on classic strategic thought. The ideas of Clausewitz, Sun Tzu, Jomini, along with more modern theorists such as Douhet and Warden are applied to the ideas of cyber war. The possible ramifications of the application of these strategic options in the cyber realm are then discussed. Classic strategic theorists can provide options for policy makers but significant work still remains to be done.

C. B. Greathouse (✉)
University of North Georgia, Dahlonega, GA, USA
e-mail: craig.greathouse@ung.edu

J.-F. Kremer and B. Müller (eds.), *Cyberspace and International Relations*,
DOI: 10.1007/978-3-642-37481-4_2,

1 Introduction

The impact of the information age on warfare has been a major issue over the last two decades as policy makers, soldiers, strategists, and non-state actors consider how best to use and protect themselves from the threat of cyber war. Unlike weapons of the past, the technology necessary for waging cyber war are not restricted to particular actors within the system. The capacity to assault important systems exists both in state and non-state actors and could possibly cripple whole societies that have become reliant on information. Over the last several years the world has seen examples of cyber war. Attacks include the 2007 cyber attack on Estonia, the 2008 attack on the state of Georgia, the Stuxnet virus from 2009 which attacked the Iranian nuclear program, and the actions by the hacker group "Anonymous" against companies such as Visa, MasterCard, PayPal, and Amazon over the Wikileaks scandal. Each attack illustrates the potential destructiveness of cyber war. "Because cyber warfare is unconventional and asymmetric warfare, nations weak in conventional military power are also likely to invest in it as a way to offset conventional disadvantages" (Geers 2011). Going forward policy makers will be required to develop strategies which address the issues of cyber war. The difficulties of developing effective strategies will be compounded by a multitude of issues including; what qualifies as cyber war, should responses be the same as from attacks by state or non-state actors, does the state respond the same if elements of its civilian sector are attacked rather than the public sector, and whether an offensive or defense stance is necessary? This chapter argues that policy makers do not have to start from scratch in their search for effective strategies. Examining traditional strategic thought will yield possible solutions to the issues of cyber war and state policy.

While a great deal has been written on the topic, there needs to be a stronger examination of how the combination of cyber weapons with traditional strategic approaches might impact strategic choices related to cyber war. Do the past approaches to warfare fit with the evolving world of cyber war or must a new generation of strategists be developed to specifically address the ideas of cyber war within the system? Examining the possible applicability of classic ideas of warfare to cyber war must include possible policy ramifications based on potential outcomes. While "bombs" may not be going off with cyber war, the impact of this type of conflict may in fact be more devastating in terms of disrupting societies. "The more electronically dependent an actor is, the more vulnerable it is" (Liaropoulos 2011, p. 4). In several cases traditional strategies of action will create an impact above and beyond the damage done if that strategy were implemented using conventional weapons.

This chapter is broken up into several parts to logically approach the puzzle raised. First there is a need to address the terms and concepts that exist within the field. As in any developing field there is not a common vocabulary for describing the ideas at use. Second a typology of different types of cyber war will be presented which will show the different levels of action within the cyber realm which

are possible and it will briefly discuss the possible weapons of cyber war which can be harnessed within each level. The typology allows for distinctions to be made between cyber war and other forms of action. Not all actions on the internet can or should be considered within the realm of cyber war. The next section examines classic military thinkers and their preferential strategies as applied to cyber war and possible ramifications from their usage. While the weapons of cyber war did not exist when Jomini, Clausewitz, and Sun Tzu put forth their thoughts, their ideas do address conflict between actors and should provide some viable ideas/approaches for how to engage in cyber war. The ramifications of applying these ideas will be addressed. The final section will examine some of the general policy implications of using classic strategic approaches within a new arena of warfare. This section will illuminate areas in which more policy work will need to be done regarding these new capabilities.

2 What is Cyber War?

As with any emerging area of study there no commonality within the field about the correct terms which should be used. Authors can and do create language which they feel best describes the phenomena they are trying to address. However because of the diversity of descriptions offered, the field has quickly become overrun with competing ideas and terms. Concepts such as the revolution in military affairs (RMA), fourth generation warfare, electronic warfare, information warfare, network centric warfare, and cyber war have all been offered to explain the emerging area of conflict. The focus on understanding this new type of conflict matters. Unlike nuclear explosion where millions would die the disruption created within a society or for a group by a major cyber attack or war may be just as serious. As Cetron and Davies observe "major concern is no longer weapons of mass destruction, but weapons of mass disruption" (Cetron and Davies 2009, p. 47). So to understand what these approaches are and how they may work is an important step in developing effective policy. A small sample of definitions is provided to give a taste of the approaches and ideas that have been articulated.

> The Shanghai Cooperation Organization has defined "information war" in part as a "confrontation between two or more states in the information space aimed at… undermining political, economic, and social systems [or] mass psychologic [*sic*] brainwashing to destabilize society and state." (Gjelten 2010, p. 36).

> A cyber attack is "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives." (U.S. Army Training & Doctrine Command 2006).

> Cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain (Nye 2010, pp. 3–4).

> The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state (Schaap 2009, p. 127).

The Schaap definition works well to describe a range of cyber weapons within the system however there are problems for the definition. It focuses on "of another state" and this assumption/usage fails to take into account the fact that cyber war could be launched against an international organization, supranational actor, non-government organization, or a multinational corporation. The actor which launches the attack may not be a state. Given the low barrier to entrance into this realm of capability, it could be some type of non-state actor. The transformed definition used for this study is that cyber war is the use of network based capabilities of a state or non-state actor to disrupt, deny, degrade, manipulate, or destroy information resident in computers or computer networks or the computers or networks themselves of another actor.

The literature and occurrences in the system show that non-state actors are significantly involved in conducting cyber war (Klimburg 2011 and Manson 2011). The actions of "hacktivists" including the group Anonymous or "patriotic hackers" and actions taken during the 2007 cyber attack on Estonia or the actions of Chinese or Taiwanese hackers (Nye 2010, p. 6) all point to the ease of non-state actors engaging in this form of conflict. The reason for the inclusion of more actors within this emerging realm is that information and the use of information is growing across the globe. But as the use of information grows there is also an increased threat to the control of civilization (Alford 2001). This threat could come in the form of targeting systems which are dependent on software for their operation; Alford (2001) illustrates this point by pointing out aircraft and their move from hardware control to fly by wire/software control. The Stuxnet virus is another example, its focus on disabling safety systems to damage equipment being used in the Iranian nuclear program. Threats to information or the ability to manipulate information could be catastrophic as the world becomes more information reliant.

3 Typology of Cyber Operations

As with traditional forms of war there are different levels of "intensity" of cyber war. Not all of these types of attacks are going to be directed towards destruction of resources or misdirection during an attack. Some will engage in criminal activities while others will engage in intelligence gathering. Due to the nature of the of this evolving realm of conflict they would all fall within cyber operations but an effective typology must be constructed to provide guidance to policy makers and strategic thinkers about how to address certain types of attacks.

Saad et al. (2011) provided a general typology of attacks used between Israel and Hezbollah which provides a starting point for developing a more generalized typology of cyber operations. They argue that there are three dimensions; attacks that focus on strategic objectives, attacks that focus on technical objective, and attacks of a political nature (Saad et al. 2011, p. 1). Attacks with a strategic focus those on include information systems, communications, and civil security; technical targets include weapons control and military communications; while political assaults look to alter the power balance within diplomatic relations (Saad et al.

2011, p. 1). Cyber weapons include viruses, malware, denial of service, spying, along with jamming and blocking (Saad et al. 2011, p. 4). While this typology provides a starting point basing it on objectives limits its usefulness. Following the Clauswitizian definition of war as a political activity all actions will be ultimately directed towards shaping the power relationships between the actors involved (Clausewitz 1984). In addition the separation between strategy and technical objectives does not provide an effective continuum through which cyber war can be analyzed. Nye argues "one should distinguish simple attacks which use inexpensive tool kits which anyone can download from the internet from advanced attacks which identify new vulnerabilities that have not yet been patched, new viruses, and involved "zero day attacks" (first time use)" (Nye 2010, p. 11).

Schmitt's (1999) six criteria could be used to evaluate cyber attacks; these include severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy (Schmitt 1999, pp. 18–19). These criteria however are focused on international law issues, which while important must be a secondary consideration when building a typology of cyber operations. Liaropoulos (2011) proposes a broad typology including cyber espionage, web vandalism, denial of service, and attacks on critical infrastructure. This provided a more practical approach to defining types of cyber operations but needs to be more fully fleshed out in that denial of service may actually be targeted at critical infrastructure.

3.1 Cyber Espionage and Cyber Crime

Creating a typology of cyber operations is difficult; distinguishing meaningful and separate categories which don't bleed from one area to another may prove to be impossible given the nature of the technology. The typology advocated here attempts to provide distinctive cut points which will then allow for strategy and policy differences based on the severity and intensity of any cyber attack. At the low end of the spectrum exists cyber vandalism, this type of activity is not designed to cause damage but rather to be an annoyance. For example this type of action may entail changing a website to insert text or some other statement which has not been approved by the owners of that site. Within the context articulated here, this would be political statements rather than a singular hacker entertaining themselves. Moving up the spectrum would be cyber espionage, the use of electronic capabilities to gather information from a target. This step in the continuum is an extension of the activities that actors within the system engage in everyday. It simply uses a new means to access different types of data which had previously not been available. The reason cyber espionage is placed so low on the spectrum is that it is an accepted and understood activity within the international system. The next level of the typology is cyber crime. This activity while it may not directly be focused towards a particular state can be targeted towards both public and private actors within the system. The definition of cyber crime used is the use of electronic capabilities to engage in criminal activities by an

actor for profit, what distinguishes cyber crime from other cyber activities is the profit motive. The means for many of the previous three elements will be the use of viruses or malware, which are easily created or written to open up vulnerabilities to networks or individual users (Chabinsky 2010). Viruses which have been propagated across the internet have both criminal and espionage motives as they create weaknesses in defenses and allow for information to be transferred outside of the user's control.

3.2 Denial of Service

Within the typology those elements up to and including cyber crime would not fall into the category of cyber war. However beyond cyber crime these categories of the typology could elements of cyber war. While malware may be used to gain information it can also be used to create another effect within the cyberworld, a denial of service attack. Denial of service is the next step up on the spectrum of cyber operations. While denial of service may not be "destructive" it has the potential to prevent actions by the target and cover other types of activity by the attacker. A denial of service attack overwhelms a particular website or network through the use of data overload. This type of attack is designed to crash the system of the targeted actor. Some of the most effective denial of service attacks uses botnets, infected computer networks which are then directed to overloading the targeted site. Recent examples of this type of attack include the assaults on Estonia and Georgia which have been traced to Russia (Klimburg 2011). In both of these instances the denial of service attack was designed to limit the target government's means to communicate and react due to the nature of the attack. In the case of Estonia the attack was limited to creating chaos within the country (Crosston 2011), however in regards to Georgia the attack was meant to assist the actions of Russian troops as they moved into parts of Georgia which had been under dispute (Korns and Kastenberg 2008). The military application of denial of service attacks is visible from these two examples. Anonymous' reaction to the Wikileaks scandal points to the potential of non-state actors using this tactic more in the future. Denial of service does not need the resources of a state within the system. While Anonymous did not completely take down the PayPal, Visa, or MasterCard sites it did cause disruption (BBC December 9, 2010). A more focused and drawn out denial of service attack would have significant potential to disrupt economic activities within an information dependent economy.

3.3 Focused Cyber Attack

The final two categories within the typology are similar but differ in scope. The fifth category in the typology is an attack to destroy or completely disrupt an

element of critical infrastructure within the actor. This type of attack would be designed to either destroy the data, software, or hardware which controls a particularly important part of an actor's infrastructure. This might include an electrical grid, water distribution system, banking system data, or any multitude of other systems. These systems need not be government controlled, in the realm of the information society many critical systems are controlled by the private sector. A systematic attack on the New York Stock Exchange or NASDAQ would have significant economic fallout given how connected elements are both within the U.S. and across the globe. A recent example of this type of attack is the Stuxnet worm, designed to attack vital components of the Iranian nuclear program (Farwell and Rohozinski 2011). While the Stuxnet worm was disabled fairly quickly once discovered (Farwell and Rohozinski 2011) the capacity to use the weapons of cyber war to destroy or disable a particular element of infrastructure raises the stakes significantly. Retaliation or escalation due to an attack of this nature may in fact occur. Depending on the critical infrastructure element attacked this could have far reaching consequences for the targeted actor.

3.4 Massive Cyber Assault

The last category in the typology is that of a massive cyber attack designed to destroy network and data systems across the entirety of an actor. What distinguishes this type of attack from the previous one is the scale. Going after one piece of infrastructure could have a negative impact on a society; however at this level of attack the intent is to completely cripple an actor. This attack would not be limited to just military or government assets but would also be directed at civilian networks and assets. The goal would be to destroy or completely degrade the information capabilities of the target and limit their ability to operate. This type of attack would be overwhelming and crippling for actors dependent on information. For example a massive attack across numerous sectors in the United States might have the ability to cripple both the electrical and banking sectors. This type of attack could create a mass disruption scenario within the United States which could provide the attacker with a significant edge in future actions. The question raised by some authors is whether this would in fact be equivalent to an armed attack? (Waxman 2011) One of the weapons which would be at the heart of the final two categories would be the "logic bomb". The logic bomb is a type of program designed to be inserted into a network and when activated destroy data or cause other changes which would cripple the network in question (Klimburg 2011). One example might be attacking the communications points of network within a target which would limit the ability to communicate during times of crisis. In combining a logic bomb with other sorts of cyber attacks like denial of service could possibly create electronic and information mayhem. This type of attack could be further exacerbated with a complimentary physical attack on critical communication nodes. An attack on the Telx facility in Atlanta, GA could cripple the ability of the Southeastern United States to connect to the internet. While cyber

war is normally thought of as not directed at physical targets, the operation of the internet and other networks is dependent on power and a physical infrastructure.

Given the possible nature of cyber warfare which has and is emerging there is a significant need for policy makers and military leaders to develop strategies for dealing with these threats and for using the new options that exist. However rather than creating brand new approaches, this study argues that some of the classic and modern military theorists have already provided the basis which can be used and manipulated to address the topic of cyber war. By expanding on the existing ideas strategists can focus on implementation actions rather than spending time on rebuilding a literature.

4 Strategists and Strategies for Cyber War

Historic thinkers in military strategy continue to form the basis for examining how warfare might occur within the international system. The inclusion of forms of cyber war will not stop the applicability of these ideas to how future conflicts may be fought. However the application of these classic ideas to the weapons of cyber war may have ramifications above and beyond the scope they would have in terms of physical conflict. Therefore when examining the baseline strategic suggestions of these thinkers it is imperative to also examine the possible consequences over and above the directed action.

4.1 Jomini

Jomini's strategic ideas were shaped by the Napoleonic period. His main goal within *The Art of War* was to distill for future generals important maxims about war which would hold across time which could then be put to use within any particular situation. At the heart of his argument is that "the art of war consists in bringing into action upon the decisive point of the theater of operations the greatest possible force" (Jomini 2008, p. 85). For Jomini the application of overwhelming force at the most decisive point in the battlefield was a recipe for victory. Decisive points were defined as

1. The features on the ground
2. The relation of the features to the ultimate strategic aim
3. The positions occupied by the respective forces (Jomini 2008, p. 65–66).

Applying this approach to cyber war, one would expect to see attacks such as denial of service or similar actions against particular sensitive elements within a state. The attacks would be designed to cause the target the greatest destruction/confusion and the resulting outcome would limit the ability of the target to respond. This type of cyber attack would not be a limited operation, rather there would be significant resources focused on one point to cause its incapacitation or

destruction after a determination was made about the most decisive point a cyber attack could be made. For information dependent societies the vulnerability of being attacked at a decisive point could be crippling. However, a decisive point may not be a military target; it may in fact be civilian with significant ramifications for the entire population.

Using Jomini's approach within the cyber realm is predicated on finding a decisive point within the target's information network on which to launch the assault. If the entirety of the strength of the attacker is directed to destroying one point, a point needs to exist which would cripple the target's ability to react. The diffuse nature of many information networks may mitigate against this approach. However if information nodes or convergence points exist through which the majority of traffic passes, the targeting of this element could be very successful, especially if privately operated. For example in the United States, Telx is a company (telx.com) which provides interconnection between networks. Taking down several of these sites would significantly degrade information transfer in key areas. Any focused attack, as advocated by Jomini, would not be concealed, therefore the knowledge of who launched the cyber attack would be clear to parties within the conflict and those outside of it. This would limit one of the unique features of the current generation of cyber weapons that of being able to disguise who the attackers actually are (Cornish et al. 2010). While the ideas advocated by Jomini may work towards a limited network with one important element, against a more diverse network this approach may not be as effective.

4.2 Clausewitz

Of mid-ninetieth century military theorists there is one name which stands above the rest, Clausewitz. Given the amount of material written about *On War* and some of his baseline ideas of war it is unnecessary to fully delve into those ideas. In examining some of the strategic options proposed by Von Clausewitz the ideas of the center of gravity, the trinity, friction, fog of war, and whether war can be limited come to the fore. One of the biggest misconceptions about Clausewitz is that *On War* advocates total/absolute war. Within Book 1, Clausewitz[1] clearly argues that absolute war can only exist in the world of theory (Clausewitz 1984 Book 1, Chap. 1 pt 6. And pt 10) therefore any cyber war would be of "limited" impact rather than an absolute approach. The nature of any cyber conflict would be "limited" with the other elements becoming more important.

The trinity is "composed of primordial violence, hatred, and enmity…of chance and probability…and its subordination as an instrument of policy" (Clausewitz 1984, p. 89). These three elements balance each other and are elements which must be considered when discussing war. When examining the trinity in the context of

[1] All citations for Von Clausewitz are taken from Michael Howard and Peter Paret Indexed Edition of On War released in 1984.

cyber war some of the ideas of Clausewitz may be limited. The virtual nature of cyber war may limit the impact of violence, hatred, and enmity. By removing some of the physical interaction and issues which can be translated to the people, the nature of war may fundamentally change. In terms of the other elements of the trinity, that of chance and probability and as an instrument of policy there is no doubt both of these elements clearly remain in play. The context of chance and probability and friction due to fog of war could be significantly altered within the context of cyber war. One of the problems Clausewitz articulated was a lack of information is going to limit the ability of commanders and politicians to effectively act. The amount of information that may be gained about how an actor may act due to compromising their protected files may in fact lift the fog of war to a significant extent. However, just as the fog of war may be lifted, the capabilities provided within cyber conflict can actually increase exponentially the ability to increase fog of war.

The cyber attacks on the state of Estonia in 2007 and Georgia during the 2008 conflict with Russia illustrate the capacity of actors that attempt to increase the fog of war by attacking information nodes and important websites to disrupt communications (Ashmore 2009). Clausewitz spent a great deal of time talking about the impact of the fog of war on operations and how it creates friction on the battlefield. The more technologically reliant an actor is, whether at home or abroad, the more susceptible they will be to an effective attack on their information systems. Actors that become reliant on advanced technology may become more vulnerable to issues of friction and fog of war than ever before due to the actions of an enemy using the tactics of cyber war. These issues would not just be related to governments, any cyber operation most likely target civilian networks as well. This will further complicate any actor's capacity to respond and may in fact create more significant problems. Some civilian networks may not be as protected nor have the redundancies built into allow them to be quickly restored. The longer an information based society is limited, the great the damage and confusion will be.

Center of gravity is one of the most debated ideas that come from Clausewitz. Echevarria (2007) shows numerous interpretations about what center of gravity represents. Center of gravity can best be described as a linkage whose loss will have devastating effect on an enemies' capacity to wage war (Echevarria 2007, Chap. 8). By undermining a center of gravity, the ability of an enemy to wage war will be limited or completely impaired. Clausewitz talks about the center of gravity providing unity (Clausewitz 1984, pp. 485–486), which in the information age provides a very different application than Clausewitz's original expectations Echevarria shows that Clausewitz applied the concept of center of gravity to wars where decisions are sought (Echevarria 2007, p. 184) and that the concept does not effectively apply to more limited wars (Echevarria 2007, pp. 183–184). Cyber war can create the ability to target and destroy the connectivity between the operations in the field and the political control. The application of center of gravity taken in the context of cyber war changes the original interpretation of Clausewitz, but the concept still matters. If the center of gravity provides for unity within an actor, destroying or degrading unity will limit or in extreme cases destroy that actor's capacity to engage in effective action within the system.

The previous overview of Clausewitz's ideas show that his theoretical approach to understanding war still holds relevance when examining cyber war. The issues of center of gravity, if understood as unity, and fog of war are incredibly powerful ideas that can be exploited by actors using the tactics of cyber war. The ability to blind information dependent actors through the use of electronic noise, as was attempted in both the situations in Estonia and Georgia, or to neutralize their information unity puts those targets at significant risk. Actors looking to engage in information warfare need to seriously consider creating the ability to blind/jam the information flow within a target to (1) create a fog of war which creates friction for their ability to operate and (2) to effectively break the ability of a targeted actor to act at all. The nature of Clausewitz's work can be applied to cyber war. Fog of war can be seen as coming to play with every denial of service attack that has been launched. In addition specific attacks on communication nodes would be of critical importance in the Clausewitz strategic guide to cyber war.

4.3 Sun Tzu

In contrast to the heft of Clausewitz, the Chinese theorist Sun Tzu provided a series of maxims to shape and guide future military leaders and thinkers. Given the nature of his writings, one of the important advantages is his distillation of fundamental ideas about how to approach conflict. It is easier to apply Sun Tzu to cyber war and in some ways the applicability of Sun Tzu to cyber war is much more effective.

He argues that "all warfare is based on deception" (Tzu 2006, p. 7) and "when able to attack we must seem unable, when using our forces we must seem inactive…" (Tzu 2006, p. 7). These ideas fit perfectly within cyber war. Engaging an enemy through the use of cyber weapons can limit the defender's knowledge of who attacked them and will benefit the attacker. Targets that are attacked without their knowing it will be unable to effective repel the assault and significant damage may be inflicted on them. For example, the Stuxnet virus that was found within the international system in 2009 and 2010 seems to have been designed specifically to cripple elements of Iran's nuclear weapons program (Farwell and Rohozinski 2011; Williams 2011; Broad et al. 2011). This virus would be a clear application of Sun Tzu by attacking an enemy without being visible. The hidden nature of who launched the cyber attacks on Estonia in 2007 (Klimburg 2011) again shows the ability of actors to effectively use these maxims of Sun Tzu to great effect.

Another of Sun Tzu's maxims is "know the enemy and know yourself, you need not fear the result of a hundred battles" (Tzu 2006, p. 15). Through the ability to hack into files, obtain information, and then make use of that information a target is put at risk even prior to their taking action if the instigator is effective in using cyber capabilities to effectively find information about their adversary. Geers (2011) argued that the ability to seize data, attack or defend networks, and shape the digital battlefield are essential elements of information. The Wikileaks case shows the potential vulnerability of actors in the information age. The amount

of information obtained could expose critical information and secrets of an actor. This maxim has been has been pursued relentlessly by states in the system during war, most spectacularly during World War II, with the breaking of Ultra by the British and the Japanese JN-25 code by the Americans. This action put the Germans and the Japanese at a significant disadvantage due to their enemies knowing a great deal about their plans. In the modern information age the damage that could be done may be exponentially greater.

"So in war the way is to avoid what is strong and to strike at what is weak" (Tzu 2006, p. 34). Again this element guides potential activity within the course of cyber war. "If he sends reinforcements everywhere, he will everywhere be weak" (Tzu 2006, p. 33) the ability to fully defend all important elements within an information society does not exist. While certain systems may be shielded, other systems may not be so protected, and that vulnerability can be exploited by an effective strike.

Examining Sun Tzu it is clear that the ideas advocated by him matter today as much or more than they did when the ideas were posited. The focus on knowledge is a critical element of the information age. Those actors which can exploit the information aspects of cyber war provide themselves with a much stronger position of power. The use of deception within cyber war is also another critical element that applies; it can exploit knowledge or can be used to prevent the targeted actor from responding to an attack. During the 2007 cyber attack on Estonia it was not clear who the attacker was, (Ashmore 2009). This ability to deceive limits the ability of the targeted state to launch a counter attack. While there was evidence about where the attacks originated there were enough questions to prevent absolute proof from being offered (Ashmore 2009). Lastly Sun Tzu's argument about trying to protect everything will create vulnerabilities in all systems has merit. Actors, especially those that are more dependent on information, will have to pick which systems to most heavily protect; many of those elements will be beyond the scope of state protection and have to be left to civilian means of defense which may not be fully secure. For example is the Telx center at 56 Marietta Street in Atlanta, GA completely secure against a targeted attack? Given the nature of Sun Tzu, his arguments would be an effective guide for action across the entire cyber war spectrum.

4.4 Airpower Theorists

While the aforementioned theorists have a great deal to say about ideas which may be incorporated into the strategic development of cyber war, another set of theorists may be better positioned to draw lessons from are the airpower theorists, who created doctrine for employing the "new" weapons system of the twentieth century, the airplane. Many of the ideas of airpower theory can be directly translated to cyber war in that they contain issues predicated on technology and also the idea of movement that is not limited by geography which is a critical difference between classical military theorists and the issues related to cyber war.

4.4.1 Douhet

The first airpower theorist to be addressed is Guilio Douhet, an Italian artillery officer who wrote during the inter-war period. In *Command of the Air* he articulated his most important ideas related to the use of aircraft in war (Meilinger 2001). One of the core ideas for Douhet was the ability of airpower to attack vital centers for the enemy (Douhet 1983). This idea while on its face similar to those offered by Clausewitz and Jomini was not just directed against armies. Rather a vital center was "the key industries and structures that allowed a state to function" (Meilinger 2001, p. 104). The expansion of war beyond just the armies and/or navies to the civilian sector is an important idea which was enabled by the development of new technology (Douhet 1983, pp. 9–10 and MacIsaac 1986) synthesized Douhet's most important ideas.

1. Modern warfare allows no distinction between combatants and noncombatants
2. Successful offensives by surface forces are not longer possible
3. The advantages of speed and elevation in the three dimensional arena of aerial warfare have made it impossible to take defensive measures against an offensive aerial strategy
4. A nation must be prepared at the outset to launch massive bombing attacks against the enemy centers of population, government and industry—hit first and hit hard to shatter enemy civilian morale leaving the enemy government no option but to sue for peace (MacIsaac 1986, p. 630).

While there are some elements from Douhet which obviously have not proven correct including offensives by surface forces will be limited and that there are limited effective defenses against an offensive aerial attack (Douhet 1983, pp. 15–19) by taking the remaining ideas to the cyber realm a very aggressive approach is developed. The most controversial but also one of the most critical assumptions made by Douhet is that there are no distinctions between combatants and non-combatants (Douhet 1983, p. 20). Within the cyber realm this argument has significant implications. For the United States more than 98 % of government information flows along civilian means of communication (Jensen 2010, p. 1534). The interdependence that has been generated between in the realm of information makes separating government and civilian components almost impossible (Jensen 2010). Just as government and society are inexorably linked together within information societies, targeting for cyber war will be both civilian and military/government oriented. Attacking just government servers/systems will in fact not prevent the target from reacting; only by engaging systems across the entire information spectrum can a fully successful cyber attack occur. This raises the question of what is the state's role in defending private interests and vice versa. While this issue is not the focus of this study, it is an important implication that emerges and must be addressed.

Another element that Douhet (1983) raises is speed of attack. Cyber attacks that can be launched to overwhelm existing defenses quickly will be the most

successful attack. Combining this with a broad based attack across both military and civilian sectors could ensure that the target of the attacks be incapacitated. Speed within the information world has always been a hallmark whether processing speed of CPUs, how fast information flows across the internet. To effectively destroy defenses an attacker is going to have to quickly and effectively overwhelm the defenses of those systems to achieve a positive outcome.

The idea of shattering civilian morale has been one of the most criticized elements that Douhet argued (Meilinger 2001). While a massive attack on the information system of a country may not break civilian morale it could in fact bring a country to a halt. Using the ideas advocated by Douhet systems from communication, electric, water, banking, transportation, and other critical elements could all be overwhelmed in the initial attacks. For technologically advanced states this could completely disrupt the way they live and work. For example if a massive cyber attack were to cripple electrical and banking systems, this would create widespread panic within a state. The loss of power would cripple a society like the United States, which would have a massive effect on communication as well; in addition an attack on the banking sector would limit economic markets and basic transactions for a significant amount of time. Disruption of society and the ability to effectively wage war was one of the reasons that Douhet argued for attacking vital centers. This process actually becomes easier to do within the context of cyber war. Disruption may be further exacerbated by the issues of private and public coordination. With neither sector being in control of this realm, an effective response may be limited. Cornish et al. (2010) argued that a major weakness between the private and public is their reluctance to share information. This is further exacerbated by the loyalties of many corporations in the west not to their countries but to their shareholders (Cornish et al. 2010, p. 22).

4.4.2 Mitchell and Trenchard

Following on the heels of Douhet is William "Billy" Mitchell and Sir Hugh Trenchard who both took some of the basic ideas of Douhet and advocated similar but more nuanced strategic approaches. Both agreed that control of the air was a vital component in winning any war, however they did not go to the lengths of Douhet to win (Chun 2001 and Meilinger 2001). One of the important differences between these two and Douhet was their unwillingness to attack civilians directly. Both advocated that airpower should be directed against infrastructure and industrial targets to limit the ability of the target to effectively fight in the war (Chun 2001).

In contrast to Douhet, this differentiation of targeting is morally acceptable but when looking at the application of ideas to the cyber world, this position becomes difficult to address (Swanson 2010). The overlap between information systems and their interconnectedness is a major issue in any technologically advanced country. Therefore being able to only target specific information systems is much more difficult and requires a much more focused approach. Attacking specific systems

to disrupt the ability of that target to act can produce the outcome sought by the attacker without imposing a significant cost on the general population. This type of targeted attack could be represented by the Stuxnet virus which was specifically created to target a very specific type of structure in the state of Iran (Williams 2011 and Broad et al. 2011). However the cost of creating a virus or cyber weapon to target each particular type of machine might be beyond an actor's resources. Thus a more general attack to disrupt systems across the country may be a more effective outcome as compared to a focused approach.

4.4.3 Warden

Col. John Warden, whose ideas have been used by the United States Air Force during Operational Iraqi Storm (Chun 2001), brought together some of the strategic threads posited by the classical theorists, earlier airpower thinkers, and combined them with an understanding of modern technological innovation. Warden is a proponent of strategic war, "in strategic war, a clash may well take place, but it is not always necessary, should normally be avoided, and is almost always a means to an end and not an end in itself" (Warden 1995). He argued that any actor must be viewed as a system, and within that larger system there are five subsystems that can be targeted, he phrases his approach as a five ring model. The five subsystems or rings include leadership, organic essentials, infrastructure, population, and fighting mechanism (Warden 1995). These rings should be attacked from inside out with the leadership at the core and then working out to each subsequent ring. At the core of each actor are numerous centers of gravity, these can be located using the five ring model which will then illustrate circles of vulnerability. Targeting the circles of vulnerability from inside out, conflicts can be more effectively ended faster. By destroying the actor's leadership or the ability of the leadership to communicate compromises the ability of the entire system to effectively respond. Likewise the targeting of organic essentials "leads to the collapse of the system" (Warden 1995) and makes it difficult for the actor to engage in action.

An additional element that Warden claims is important in effectively attacking the enemy system is to use the parallel attack. "States have a small number of vital targets at the strategic level…These targets tend to be small, very expensive, have few backups and are hard to repair. If a significant percentage is struck in parallel the damage becomes insuperable" (Warden 1995). The ability to hit multiple strategic targets at once prevents the target from bringing those elements back into good order and respond effectively to future attacks. "The greater the percentage of targets hit in a single blow, the more nearly impossible his response" (Warden 1995).

Bringing together disparate threads Warden generated an approach which proved to have a significant impact on how conventional wars were approached. However the ideas of Warden would be even more devastating if used within the context of a cyber war. The targeting advocated by Warden across the entire system starting at the leadership and then moving to forces in the field would generate a significant number of targets. Using the ring model, communications systems

would be the foremost element of any attack. The ability to cut the leadership level from the rest according to the model would create almost catastrophic impact; this would not even include attacks on infrastructure and organic essentials which would only increase the impact. Combining this strategic targeting scheme with parallel attacks through cyber war, a technologically dependent actor could be crippled more quickly than Iraq. If an attacker had the capacity of using parallel attacks, they would strike to bring down whole systems including communications, electrical, and financial to prevent the target from being able to effectively respond due to the massive impact of the initial assault.

5 Cyber Defense

Up to this point strategic approaches which point to offensive types of operations have been examined. The question becomes can defense and deterrence be a viable policy stance for states? Defense is the ability to actively resist if an attack is launched against an actor. Fixed defenses are the classic representation of this type of approach. From castles, forts, coastal and harbor defenses, to the Maginot Line each of these was designed to defend a specific objective from assault. The problem historically is that none of these defensive structures has ever been able to survive changes in technology. Castles became vulnerable to the emergence of gun powder based weapons, air power, or attack based on movement. Some of the strongest defensive positions have fallen as new weapons and tactics have moved the advantage, in some respects, to the offensive side of the ledger. Fixed positions have become vulnerable to the destructive power of precision weapons and the ability to attack the fortification from multiple directions.

If one were to apply only the strategy of defense in the realm of cyber war, this choice is defective from the start. Defending computers and networks has created a massive sector which develops and maintains security, the capacity of this approach is always being threatened. First and foremost the defensive aspects of cyber war are at a disadvantage due to the 'offensive dominance' which has been shown to this point (Cornish et al. 2010). Second these defenses are never going to be perfect either due to programming issues, the need for the system to be connected to the larger internet, or human error. The only way to completely protect a system from external threats would be to full segregate the system from external connection, but even by doing this the system still could be threatened by the human element either intentional or not (Brechbuhl et al. 2010 and Ashmore 2009). However, given the need for interconnectiveness, segregating most systems from the ability to communicate defeats the purpose of connectivity. Some defenses that can be put into place include encryption, firewalls, and automated detection. But as with most defenses these are as good at the updates and operators, and even then can still be penetrated.

Another issue in developing a defensive posture for an actor in the cyber world is what to defend. If a state were only to defend its networks, that may be feasible

but that then leaves whole segments of infrastructure which are operated by the private sector open to assault which could have a debilitating impact on society. Even though the private sector does build in defenses against types of cyber threats, an intentional attack is very likely to disrupt their business. Operation "Payback" launched by the hacker group Anonymous against Visa, MasterCard, PayPal, and Amazon.com over their treatment of Wikileaks is but one example. Of those four only Amazon was able to effectively resist the denial of service attack due to the capacity that Amazon has built into its system (BBC 2010). Just taking this simple example and extending it, if three out of four companies could not effectively protect themselves or their capacity the impact by sustained cyber attacks would be devastating to the domestic economic structure of a state. There are arguments that governments are required to help defend private networks and sites due to inter-connectiveness (Brechbuhl et al. 2010 and Jensen 2010). However, in attempting to defend a whole array of elements beyond that of their own sites and capacity would potentially leave the government vulnerable. In many western states, especially within the United States, private industries are essential in protecting important systems from a cyber attack (Klimburg 2011).

6 Cyber Deterrence

A deterrent stance provides another option, but only with a clearly articulated and known capacity to back up the threat of retaliation should any cyber attack be launched. Only with capability and willingness to retaliate can deterrence be achieved (Cornish et al. 2010). In a cyber war situation, deterrence means that a state would have to have an offensive capability which could cause disproportionate harm if it were attacked. Given the problems of finding who is launching an attack, the ability to deter is limited. Deterrence is only effective if the attacker could be clearly identified and punished. In the Estonian cyber attack there was not clear evidence at the time of the attack who was responsible. The state of Georgia also suffered a significant cyber attack, however it appears that this attack was launched via non-state nationalist groups (Ashmore 2009), whether at the behest of the state is still unclear. If a cyber attack's origin can be hidden then the threat of deterrence is lessened. Blank (2001) put forth a compelling argument that deterrence in information war (IW) may not be effective given the nature of the "weapons" at work.

> IW cannot be deterred by another IW force since both sides can easily deceive or cripple their opponent's ability to make the kind of evaluations that deterrence depends on. Pre-emptive IW becomes a viable, almost a necessary, option here. Since everyone has access or will have access to forms of IW and can use commercially available satellites, cell phones, PCs and the like to launch delayed attacks, hack systems, etc., *IW deterrence must be ubiquitous and universal to be effective*. Otherwise the temptation to strike first can be overwhelming. This trend towards defending everything can be seen in the US' accelerated efforts to set up homeland and anti-terrorist defense organizations. But evidence to date suggests that despite our technological superiority we cannot accurately deter or predict what enemy forces will do, especially when they can target our insight

> into their thought processes or vice versa. Nor is it clear that we can deter our adversaries if our strategy focuses on destroying their ability to command troops, govern their country, and control their WMD (Blank 2001, p. 133).

7 Policy Ramifications/Conclusion

In looking at strategic choices that are available to states and other actors in the international system to address the issue of cyber war and cyber attacks the need to have clearly articulated policy stances in place is necessary. Without having defined policy stances before a cyber attack occurs, the actor's ability to respond to that attack will be limited and disjointed at best. However in trying to build an effective policy for cyber conflict, states will continually have to reassess the issue given the technological developments that are always occurring and the capacity which actors may be developing. There are three important areas that all actors must clearly lay out in terms of cyber policy; first what are viable targets, second how to deal with non-state actors, finally what offensive/defensive balance will be pursued. The issue of defense capacity is more difficult due to the inclusion of the private sector in the policy discussion and the necessary coordination which must be developed. In examining the issues surrounding the cyber world the situation becomes more complex than threats from physical attacks. "In a networked world, there are no real safe harbors—if you are on the network, you are available to everyone else on the network. A key consequence is that security is not the concern of someone else" (Brechbule et.al. 2010, p. 84).

Through the development of an effective cyber war typology states and other actors may be able to effectively match actions to events in the system. Using the proposed typology of cyber operations and relying on previously developed strategic models would allow states to build strategies and policies to provide a basis for action in this area. The typology also helps to define elements of cyber deterrence given the need for an escalation threat to make deterrence viable. However even with this typology of cyber operations strategic development is still in its infancy. The classical theorists provide a basis but given the nature of cyber war their ideas need to be nuanced into the cyber world.

There are divergent strategy choices that are being put before actors on which they will have to make decisions in the near future. If an actor ignores the evolution of cyber issues it will put them at a significant disadvantage going forward. Ashmore (2009) contends that there needs to be defense in depth created across the society within both the civilian and military networks. The problem of this approach is that in a country like the United States the number of possible actors is massive. Combine this with the need to develop commonality of action across the public and private sectors and the complexity and cost potential for this approach would grow exponentially. Given the speed of advances in cyber capabilities there is no guarantee that complete safety or anything even close would emerge.

Another possible option to explore as the debate occurs is to assess how much of a response to develop within an actor. Does the actor need to develop a counter

cyberspace policy or should it focus on offensive action? "Counter cyberspace: a function consisting of operations to attain and maintain a desired degree of cyberspace superiority by the destruction, degradation, or disruption of an enemy's capabilities to use cyberspace" (Trias and Bell 2010, p. 96). But in either developing a counter response or just focusing on offensive cyber war capability an issue will be raised that will require significant thought. "Attacks through cyberspace against cyber assets can also result in cascading collateral damage. The fear of such common side effects had kept American leadership from pulling the trigger of cyber weaponry" (Trias and Bell 2010, p. 97). Given the degree of disruption that could possibly be raised through creating a counter attack or offensive cyber capability policy makers need to very clearly address this issue.

There needs to be significant work done at all levels of the emerging field of cyber war. There is a need for both strategic thought but also tactical innovation but at the same time these two levels must be able and willing to talk to each other. Further complicating this issue going forward will be the need for actors to develop a grand strategic approach to cyber war which will provide the direction necessary for strategic and tactical development. All the while technology will continue to grow and evolve which mean the thinking necessary cannot be static in nature, it must continue to evolve to address new developments both in terms of technical capabilities but strategic situations.

References

Alford, L. D. (2001). Cyber warfare: A new doctrine and taxonomy. *Crosstalk: Journal of Defense Software Engineering, 14*(4), 27–30.

Ashmore, W. C. (2009). Impact of alleged Russian cyber attacks. *Baltic Security & Defence Review, 11*(1), 4–40.

BBC. (2010). Pro-Wikileaks activists abandon Amazon cyber attack. Retrieved December 9, 2010, from http://www.bbc.co.uk/news/technology-11957367.

Blank, S. (2001). Can information warfare be deterred? *Defense Analysis, 17*(2), 121–138.

Brechbühl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development, 16*(1), 83–91.

Broad, W., Markoff, J., & Sanger, D. E. (2011, January 15). Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*. Retrieved October 8, 2011, from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2.

Cetron, M. J., & Davies, O. (2009). Ten critical trends for cyber security. *The Futurist*, 43(5), 40–49.

Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. *Journal of National Security Law and Policy, 4*(1), 27–40.

Chun, C. K. S. (2001). Aerospace power in the twenty-first century: A basic primer. USAF Academy in Cooperation with Air University Press: Colorado Springs, CO. Retrieved October 30, 2012, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA421723.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010) On cyber war. Chatham House. Retrieved October 3, 2012, from http://www.chathamhouse.org/publications/papers/view/109508.

Crosston, M. D. (2011). World cyberMAD: How "mutually assured debilitation" is the best hope for cyber deterrence. *Strategic Studies Quarterly, 5*(1), 100–116.

De Jomini, B. (2008). *The art of war* (G. H. Mendell & W. P. Craighill, Tans.). Radford: Wilder Publications.
Douhet, G. (1983). *The command of the air*. Washington, D.C.: Office of Air Force History.
Echevarria, A. J. (2007). *Clausewitz and Contemporary War*. Oxford: Oxford University Press.
Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23–40.
Geers, K. (2011). Sun Tzu and cyber war. Cooperative Cyber Defence Centre of Excellence. Retrieved March 20, 2012, from http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf.
Gjelten, T. (2010, November/December). Shadow wars: Debating cyber disarmament. *World Affairs*, *173*(4), 33–42.
Jensen, E. T. (2010). Cyber warfare and precautions against the effects of attacks. *Texas Law Review, 88*, 1533–1569.
Klimburg, A. (2011). Mobilising cyber power. *Survival, 53*(1), 41–60.
Korns, S. W., & Kastenberg. J.E. (2008). Georgia's cyber left hook. *Parameters*, 38, 60–76. Retrieved March 22, 2012, from http://www.carlisle.army.mil/usawc/parameters/Articles/08winter/kokor.pdf. (Last accessed March 22, 2012).
Liaropoulos, A. (2011). Cyber-Security and the law of war: The Legal and Ethical Aspects of Cyber-Conflict. GPSC Working Paper # 7. Retrieved March 22, 2012, from http://www.gpsg.org.uk/docs/GPSG_Working_Paper_07.pdf.
MacIsaac, D. (1986). Voices from the Central Blue: The air power theorists'. In P. Paret (Ed.), *Makers of modern strategy.* Princeton: Princeton University Press.
Manson, G. P, I. I. I. (2011). Cyberwar: The United States and China prepare for the next generation of conflict. *Comparative Strategy, 30*(2), 121–133.
Meilinger, P. S. (2001). *Airmen and air theory: A review of the sources*. Maxwell Air Force Base: Air University Press.
NYE, J. S. (2010). *Cyber Power*. Harvard Kennedy School, Belfer Center. Retrieved March 22, 2012, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA522626.
Saad, S., Bazan, S., & Varin, C. (2011). *Asymmetric cyber-warfare between Israel and Hezbollah*: *The web as a new strategic battlefield.* Proceedings of the ACM WebSci'11, June 14–17 2011, Koblenz, Germany. Retrieved March 22, 2012, from http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf.
Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law, 37*, 885–937.
Schaap, A. J. (2009). Cyber warfare operations: Development and use under international law. *Air Force Law Review, 64*, 121–174.
Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loyola of Los Angeles International & Comparative Law Review, 32*(2), 303–333.
Trias, E. D., & Bell B. M. (2010). Cyber this, cyber that… so what?. *Air & Space Power Journal*, *24*(1), 90–100.
Tzu, S. (2006). The art of war. London: Filiquarian Publishing LLC.
U.S. Army Training & Doctrine Command. (2006). DCSINT Handbood No. 1.02, Critical Infrastructure Threats and Terrorism. Retrieved October 30, 2012, from http://www.fas.org/irp/threat/terrorism/sup2.pdf.
Von Clausewitz, C. (1984). *On War*: *Indexed Edition* (M. Howard & P. Paret, Ed. and Trans.). Princeton: Princeton University Press.
Warden, J. A. (1995). The enemy as a system. *Airpower Journal*, 9, 40–55. Retrieved October 8, 2012, from http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.
Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2(4). *The Yale Journal of International Law, 36*, 420–459.
Williams, C. (2011, January 21). Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel'. The Telegraph. Retrieved October 8, 2011, from http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html.

Springer

http://www.springer.com/978-3-642-37480-7

Cyberspace and International Relations
Theory, Prospects and Challenges
Kremer, J.-F.; Müller, B. (Eds.)
2014, XXIV, 284 p. 2 illus., Hardcover
ISBN: 978-3-642-37480-7