DIIS WORKING PAPER

WORKING PAPER

The cyberwar mirage and the utility of cyberattacks in war
How to make real use of Clausewitz in the age of cyberspace

Jeppe Teglskov Jacobsen

DIIS Working Paper 2014:06

JEPPE TEGLSKOV JACOBSEN
Research Assistant
jetj@diis.dk

DIIS · Danish Institute for International Studies
Østbanegade 117, DK-1401 Copenhagen, Denmark
Ph: +45 32 69 87 87
E-mail: diis@diis.dk
www.diis.dk
Layout: Ellen-Marie Bentsen
Printed in Denmark by Vesterkopi AS
ISBN:
978-87-7605-679-7 (print)
978-87-7605-680-3 (pdf)
Price: DKK 25.00 (VAT included)
DIIS's publications can be downloaded free of charge at www.diis.dk

CONTENTS

ABSTRACT

Cyberwar is everywhere – in the media, in the military, among politicians and in academia. It is the new weapon of mass discussion. But there is no such thing as cyberwar. This observation, however, does not render cyberattacks unimportant. The article revisits the debate on Carl von Clausewitz's On War (1832), and examines the utility of cyberattacks as a tool in future war. In doing so, the article not only targets the misunderstandings and exaggerations prevalent in the literature, but demonstrates that Clausewitz's On War, albeit being two centuries old, is a valuable analytical lens in making sense of the relationship between cyberattacks and war. Drawing on the Clauzewitzian trinity, the article finds that cyberattacks can be useful tools in warfare, particularly in the initial stages of war. They are easily deployable and have already proven capable of causing physical damage. However, the article argues that cyberattacks remain inferior to conventional military weaponry, ultimately rendering cyberwar – understood as a war fought primarily through cyberspace – unlikely.

INTRODUCTION

Two decades ago the term was discussed only sporadically within American military-academic scholarship (Arquilla & Ronfeldt 1993), but with the cyberattacks in Estonia in 2007, the concept of cyberwar has gone mainstream (Lesk 2007). The Estonian cyberattacks took place over the duration of a month during which websites were disrupted and bank-services momentarily shut down (Lander & Mankoff 2007). Later in the same year, the term *cyberwarfare* was used to describe a cyberattack that neutralised a Syrian radar-system prior to the Israeli bombing of a nuclear construction site in Dayr ez-Zor (Fulghun et. al. 2007). Since then, the term *cyberwar* has increased in popularity as a number of businesses, governments and private individuals have been targeted through cyberspace. To date, the incident that has attracted the most attention was Stuxnet, a computer worm, which in 2010 managed to destroy centrifuges at an Iranian nuclear facility (Sanger 2012; Foltz 2012; Farwell & Rohozinski 2011).

These events constitute the backdrop against which the scholarly debates on cyberwar are played out. Despite similar empirical starting points, the debate as to whether cyberwar is here, whether cyberwar is impending or whether cyberwar is merely a discursive term used to describe a threat which, at best, is greatly exaggerated and at worst, is non-existent, rages (cf. Langø 2013). What both scholars who argue that *cyberwar is coming* (Adams 1998; Clarke & Knake 2010; McConnell 2010; Farwell & Rohozinski 2012; Arquilla 2012) and the critical scholars who deny these findings as exaggerated claims based on dooms-day scenarios with little or no empirical validity (Samaan 2010; Lawson 2011; 2012; Rid 2011; 2012; Gartzke 2013), lack, is proper theoretical grounding.

Carl von Clausewitz's monumental book *On War* (2007 [1832]) is widely acknowledged to be the most influential book on war (Gray 2005; Heuser 2002). Within the cyberwar literature however, only few scholars claim to draw inspiration from Clausewitz, and do so in a rather selective manner, cherry-picking quotes and misusing concepts (cf. Arquilla & Ronfeldt 1997; Cornish et al. 2010; Rid 2011; 2012; Farwell & Rohozinski 2012). These scholars reject Clausewitz's framework as inapplicable to cyberwar, either because *On War* is considered out-dated (Cornish et al. 2010: 32) or because the 'war' in cyberwar does not respect the Clausewitzian criteria of war (Rid 2011; 2012). But drawing out selective theoretical concept and testing them against empirical events goes against the very idea of the Clausewitzian framework. *On War* is "the prism through which we […] look at war" (Strachan & Herberg-Rothe 2005: 1), and it is a way of thinking about war. *On War*, when thought of as a prism and not a "checklist", is still relevant when discussing and understanding cyberwar.

Motivated by the urge to show that the use of Clausewitz within the cyberwar-debate thus far has been both limited and based on misinterpretations, *this article uses* On War *as a lens through which to analyse the relationship between cyberattack and war*, and finds that, while cyber-weapons are becoming the new "weapons of mass discussion", the threat from, and opportunities of, cyberattacks are greatly exaggerated.

The article argues i) that despite the fact that cyberwar cannot be rejected on the basis of past cyber-incidents, the number of scholars and politicians predicting *cyberwar is coming* exaggerate the efficacy of cyberattacks in causing physical damage relative to conventional weaponry, hence *cyberwar will not come*, and ii) that cyberattacks, while providing some tactical opportunities in the initial phase of war, are not the new and decisive tool for governments' in controlling the outcome of future

wars. In making these arguments, the article draws inspirations from Clausewitz's insistence on the political, tactical and physical nature of war; on war as reciprocal interactions, and on the inevitable role of his trinity of passion, creativity and reason. In doing so, the article also shows that *On War* – far from becoming redundant within the cyberwar-debate – is more relevant than ever!

The article is in four parts: first, the relevant insights from *On War* are introduced; second, three oft-cited cyber-incidents are revisited with reference to the political, tactical and physical nature of war; third, the reciprocal character of cyberattacks is discussed to determine whether cyberwar, understood as a war primarily fought with cyber means, is a likely future scenario. And fourth, the utility of cyberattacks in conventional wars is discussed through the Clausewitzian trinity.

ON WAR REVISITED IN THE AGE OF CYBERSPACE

Clausewitz's insights from *On War* are not wholly ignored within the cyberwar-literature, but a thorough introduction to its relevant concepts is often missing.[1] These omissions may stem from a general belief that the thoughts presented in *On War* are so widely appreciated that no further introduction is necessary. However, the number of misinterpretation and misapplications of its central concepts, suggest an introduction is not out of place. Hence, the following section briefly places central Clausewitzian concepts in the context of the cyberwar-debate to show how these, when properly used, can further our understanding of the cyberattacks and war.

Most introductions to *On War* invariably begin with the well-known dictum: "war is simply a continuation of political intercourse, with the addition of other means" (Clausewitz 2007: 252). Within the cyberwar-literature, some scholars have rephrased the dictum by claiming that cyberwarfare should be characterised by "the insignificance of political intercourse caused by the availability of digital means" (Cornish et al. 2010: 32). Cornish et al. (2010) motivate this modification by claiming that cyberspace is a space to achieve not only political goals but also economic, cultural and religious goals; that cyberspace out-dates Clausewitz's state-centric and government-centred framework, and that cyberwarfare cannot be politically controlled. There are a number of problems with these observations.

First, claiming that warfare is economic and religious activities that harbour no politico-territorial claims is not a rejection of Clausewitz so much as it is a decision to broaden the definition of warfare to include all types of crime and violence. Second, contrary to common belief, Clausewitz is not state-centrist. The German word *Politik* is used throughout *On War* to refer both to *policy,* which is the decision or will of state or groups to pursue a goals, political or otherwise, and to *politics*, defined as the interactions or struggle between individuals and groups hoping to achieve power over something or someone. Hence the term *Politik* is not bounded by state affairs (Echevarria 1995/96). And third Clausewitz does not claim that war is *controlled* by politics but argues instead that the war carry within it its own grammar and must be analysed through its unique nature (Clausewitz 2007: 28). Thus, it is vital not to analyse war solely through *Politik*.

1 Notable exceptions are David Lonsdale (2004) and Manabrata Guha (2011).

Clausewitz starts *On War* by stating, "war is nothing but a duel on a larger scale [and] an act of force to compel our enemy to do our will", and that physical force constitutes the means to "render the enemy powerless" (ibid.: 13). Clausewitz distinguishes between the *absolute ideal of war*, where war is *not* controlled by politics, knows no limits to the use of force, contains eternal fear of subjugation and always leads to ever-increasing military efforts (2007: 15-16), and the *limited war* or war in reality, which modifies the absolute ideal of war with reference to the fact that war in reality is never an isolated, wholly unexpected and definitive act (ibid.: 17-19).

In the limited war, *Politik* moderates the extent to which war is fought. It defines and limits the objective of war, and tries to determine, but can never be directly translated into, the tactical, short-term goals during the war (ibid.: 74). Thus the limited war is not necessarily a question of rendering the enemy powerless. Fighting can cease if peace-agreements are reached or if one side changes its behaviour in accordance with the will of the other. I.e. war, in reality, does not necessarily imply the total destruction of the enemy. Furthermore when war is fought, it always contains *reciprocal interactions* based on anticipations, threats and acts of force. *On War* is littered with reference to force as something that physically and morally destroys the enemy (ibid.: 31-44), thus a 'war' that consists of neither runs counter to the Clausewitzian nature of war (Heuser 2007: xxvi).

Thus, in understanding the extent to which (cyber)-conflict can be informed by the Clausewitzian concepts of war, three elements are particularly relevant: the strategic or *political objective* (der Zweck), which constitutes the purpose of war, motivates the coercive attempts in war, and, when achieved, ends the war, the *tactical aims* (das Ziel), which are always to defeat of the enemy in battle, and the physical *means* (das Mittel), defined as reciprocal threats, and the use – or attempted use – of force. Examining the extent to which cyberattacks harbour these characteristics of war provides the natural starting points in any analysis.

Selectively choosing a few concepts in *On War* and testing them against individual cyberattacks, as Thomas Rid (2011) has done, runs counter to the logic of the book. *On War* was not written as a checklist for determining whether an attack is a war or not (Heuser 2002). When discussing contemporary conflicts in which cyberattacks have played a part, *On War* should rather be used as a companion in the attempt to understand the characteristics of cyberattacks. The narrow emphasis on either proving or disproving that cyberattacks are acts of war furthermore precludes the cyberwar-debate from examining how cyberattacks might play a role in future war – a discussion for which Clausewitz also provides a very appropriate theoretical framework yet largely unexplored in the cyberwar-literature.

Relevant here is Clausewitz's trinity of war, which acts as guiding principle in considering the utility of cyberattacks. The trinity makes up the vital parts in any war (Herberg-Rothe & Honig 2007: 142; Lonsdale 2004) and is "composed of primordial violence, hatred, and enmity, which are regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone" (Clausewitz 2007: 30). Primordial violence, hatred and enmity are defined by Clausewitz as expressions of *passion*, and are illustrated throughout *On War* by the *people*; the play of chance and probability are seen as *creativity* and are illustrated by the *army*, and the subordination of war to policy is seen as *reason*, illustrated by the *government*. Overlooking the fact that Clausewitz

merely draws on the *people*, the *army* and the *government* as analytical illustrations of how the three primary concepts of passion, creativity and reason are present and interact in war, some scholars mistakenly suggest that Clausewitz's framework is only applicable to inter-state-wars (van Creveld 1991: 36-37; Keegan 1993).

What the trinity does is to illustrate the dynamic and interconnected nature of war. Hence, a government with a clear, well-defined and realistic political objective is not necessarily guaranteed success. Success in war, whether in cyberspace or beyond, also depends, first, on the talent of the army, and its tactical superiority in dealing with the enemy and the unpredictability of battle, and second, on the people and their support for the government's fight against the enemy. Discounting the *passion of the people*, dismissing the importance of a *creative army*, or entering a war without a clear and *rational political objective*, can lead to wars going horribly wrong (Gray 2007: 27).

Scholars optimistic about the information revolution have heralded the coming of advanced technologies that have enabled the emergence of anonymous, precise, pre-planned cyberattacks, as a development which allows the president to "give an order […], hang up the telephone and let organization execute the plan" (Davis 1997: 92) – hence technology has enabled war to be controlled by the reasonable government alone. This view however runs counter to Clausewitz's trinity. Clausewitz invented the term *friction*, to describe the events that inevitably distinguish real war from war on paper (2007: 66). Friction covers any number of unforeseen occurrences, including bad weather, human mistakes and poor intelligence. Clausewitz considered the information collected in war, not as a form of controllable asset as Arquilla & Ronfeldt have claimed it to be (1997: 10), but as a friction – or fog – which should not be trusted (Clausewitz 2007: 89). The good general and government must accept friction and be able to overcome it whenever possible (ibid.: 66).[2]

A final important Clausewitzian concept of war, which has been erroneously challenged with the emergence of cyberattacks, is the *offensive-defensive nexus*. Clausewitz gave the advantage to the offence only in the initial phase of war. When war drags out, the defender, fighting on home soil has the advantage in relation to *the terrain*, the benefit of the *fortresses* and *people in arms* (ibid.: 160-166). However, Farwell & Rohozinski (2012) view offensive cyberattacks as intrinsically stronger than defensive cyber-security, thus reversing Clausewitz's offensive-defensive nexus. Malware, they claim, is less complex, cheaper and faster to create and execute (Ibid.: 114). While these claims hold some truth, the two scholars overlook, that using cyberattacks as tactical and targeted attacks in war, is likely to demand more complex and thoroughly pre-planned malware – especially if even a minimum of cyber-security is implemented. Thus, in investigating the utility of cyberattacks in future wars, a discussion on *the cyber-terrain*, *the cyber-fortress* and *people in cyber-arms* is not obsolete.

The following analyses demonstrate how insights from *On War* might inform our understanding of cyberattacks and the interaction between cyberattacks and war. With Clausewitz's distinction between the political, tactical and physical nature of war as the guiding principle, the next section takes a closer look at three of the most discussed cases in which cyberattacks have played a role. Re-assessing these cases through a Clausewitzian prism, a

2 Clausewitz tends to be overly pessimistic about intelligence in war. Intelligence and gathering of information has become vital parts in any war – and especially in enabling cyberattacks.

number of interesting questions concerning the ability and utility of cyberattacks in war emerge. In answering these, the reciprocal nature of war, as well as the trinity, friction and the offensive-defensive nexus helps to provide a deeper understanding of the relationship between cyberattacks and war.

EXAMINING THE EMPIRICS THROUGH CLAUSEWITZIAN LENSES

Whether recent cyber*attacks* should be characterised as cyber*wars* remains a topic of debate. The disagreements derive from a lack of consensus in defining the terms *cyberwar* and *cyberattack*.[3] Hence, debating whether cyberattacks are acts of war serves a purpose only for those scholars interested in war as a discursive concept (Cavelty 2008; 2012; Hansen & Nissenbaum 2009; Brito & Watkins 2011; Lawson 2011; 2012) or those scholars concerned with how uncritical references to war, dilutes the concept to a metaphor like 'war on obesity'.

A proponent of the latter critique is the prominent cyberwar critic, Thomas Rid (2011; 2012; 2013). Rid uses concepts from *On War* to create a Clausewitzian definition of war that is useful when evaluating whether recent cyberattacks were acts of war or not. Investigating a number of cyberattacks he finds that none have contained the necessary components to constitute an act of war. But Rid, in his desire to rebut cyberwar and to place cyberattacks into well-known categories of subversion, espionage and sabotage, weakens his own conclusion – that cyberwar will not take place. Not only does he wrongly equate Clausewitzian physical force with lethality and argues that the technical anonymity of cyberattacks renders them incompatible with political objectives (Stone 2013: 105-106). He also uses Clausewitz to *test* whether each individual attack 'fulfilled' Clausewitz's criteria of war. *On War*, however, is not written as a set of criteria for determining whether individual attacks are acts war. Instead it provides a lens, which helps the analyst in guiding his analysis towards a better understanding of the world of wars and warfare and thus also the relationship between cyberattacks and future wars.

Revisiting three of the most-discussed cyberattacks, Estonia 2007, Syria 2007 and Iran 2010, based on the Clausewitzian political, tactical and physical nature of war, provides a better understanding of the character of cyberattacks.

The Political Objectives of Cyberattacks

Clausewitz argued that wars always pursue a political objective (2007: 28, 252). *Politik* constitutes the purpose of war and motivates the coercive attempts in war. Following the Estonian government's decision to remove a Soviet World War II-memorial in Tallinn, street riots arose in April 2007. These protests were followed by three weeks of cyberattacks overloading governmental and business servers, the so-called Distributed Denial of Service attacks (DDoS), and led to the defacement of governmental websites and a brief breakdown of bank-services (Geers 2011: 84-85; Schreier 2012: 109-110). The incident was thus a response to a political decision concerning a war memorial. When assessing the event through

3 'Cyberattack' is in this article distinguished from 'cybered attack', which include drone strikes and electromagnetic pulse attacks (Moss 2013), and refer instead to the "actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and the networks themselves" (JCS 2006). By using this definition cyber-espionage and low-level cyber-fraud are excluded from the definition.

its historical context, it appears to relate to a much broader objective, namely maintaining Russian influence in Estonia. However unsuccessful in coercing the Estonian government to change its decision, the alleged Russian hackers, whether acting on order from Kremlin or not, were thus pursuing a political objective.

The Israeli bombing three months later of a nuclear facility in Dayr ez-Zor in Syria, which was preceded by a cyberattack on a Syrian radar-system (Geers 2009: 4; Rid 2011: 16-17; Clarke & Knake 2010: 1-8), can also be traced back to a political objective. Since the 1948 creation of Israel, survival of the Jewish state, enabled by regional military superiority, has been the overarching political objective (Shlaim 2000). Thus, destroying what is considered an existential threat, by thwarting Syria's alleged ambitions to build a nuclear weapon, also follows a clear political objective.

Equally as politically motivated was the pre-programmed Stuxnet, which managed to cause about a thousand nuclear centrifuges at the Iranian facility in Natanz to malfunction, while avoiding detection (McGraw 2013; Langner 2011). Even before investigative journalist David Sanger (2012) provided solid evidence that Stuxnet was part of a comprehensive military U.S.-Israeli operation called *Olympic Games*, fingers had been pointed at Israel and the United States, due to the two countries' technical capabilities and their well-known political efforts to put an end to the Iranian nuclear programme. Israel had a clear political objective in limiting the military power of a regional competitor. On numerous occasions, the United States have voiced concern about an emerging nuclear arms race, and expressed their ideological aversion towards an Islamic theocracy.

Tactical Aims as Instruments in Achieving a Political Objective

Cyberattacks can be politically motivated, but Clausewitz also argued that war is characterised by a logical connection between the tactical aims and the political objective, i.e. tactical aims must ultimately be instrumental in achieving the political objective (2007: 74-75).

Most of the cyberattacks targeting Estonia appeared uncoordinated and random. But assuming that the alleged Russian 'hacker-gangs' were fighting with the means available to them against the *de-Russification* of Estonia, the decision to jam banks and electronic services, these services being vital societal functions, could be seen as instrumental, albeit unsuccessful, in undermining the authority of the pro-European Estonian government.

In their tactical aims, the Estonian attacks differ from the Syrian incident. Israel, a country with superior cyber- and conventional capabilities, decided to bomb neighbouring Syria, whose intentions, Israel considered threatening. Proving capable and willing to destroy physical infrastructure sent a clear message about how serious Israel was in its attempt at coercing Syria to stop its nuclear aspirations. Tactically, the destruction of the nuclear site is instrumental to the Israeli political objective. However, it would be wrong to assert that the cyberattack neutralising a radar-system was *causal* in reaching the political objective. Israel conducted a similar bombing on an Iraqi nuclear reactor at Osirak in 1981, absent the preceding cyberattack (D'Amato 1983). Thus the Syrian incident is illustrative as a case that underlines the convenience of cyberattacks as force multipliers.

At first glance, the U.S.-Israeli decision to target the nuclear facility in Natanz is instrumental as well. However, on closer inspection, there is little connection between the attack, and coercing the Iranian government into ending their nuclear enrichment programme.

Olympic Games was initiated according to President Bush, as a *third* option to either permitting Iran to get the bomb or *go to war*, thus it was an attack that aimed at preventing war. Furthermore, the attacks remained for some times unknown, and only by mistake did Stuxnet spread through the Internet and became publicly known (Sanger 2012: 204-205). Sanger's interviews with U.S. government staff revealed an explicit request from President Obama that the attack was kept invisible to Iranian scientists working at the site (Ibid.: 202). Destroying centrifuges without Iran knowing, may serve a tactical aim, but it seems illogical and short-sighted if the political objective is to coerce Iran into stopping its nuclear aspirations. Intuitively, not knowing that you are under attack inevitably makes it more difficult to act in accordance with the will of the attacker.

Cyberattacks Causing Physical Damage

Cyberattacks *can* be used instrumentally towards a political objective, but *On War* is also rich with references to war as physical fighting and destruction (2007: 41, 73). This does not mean that the only important part in war is the exchange of brute force. E.g. the passionate people in Clausewitz's trinity can be turned against their government, or de-moralised soldiers can turn against the inexperienced military commander (ibid.: 53, 141). However, a conflict, whether in cyberspace or not, 'fought' without exchanges of physical threats or mutual attempts at causing physical destruction, runs counter to *On War*. Throughout the book war is seen as the continuous interaction of opposites with physical force as the primary means of combat (ibid. 37-38; 84).

Consider for a moment the Estonian incident. None of the cyberattacks caused, or threatened to cause any direct or indirect physical damage. Even though the attacks challenged Estonian sovereignty, the lack of destruction rendered an invocation of the NATO *one-for-all, all-for-one* article 5 impossible (Roscini 2010: 129). Instead the Estonian Government made the incidents a matter for national and international criminal investigation (Shackelford 2009: 208). Although the attacks did not cause physical damage, they have proven capable of cutting off flow of information and denying access to vital services, which could prove useful in war either operationally or in undermining the trust in government.[4]

Israel's bombing of an alleged nuclear construction site in Syria was indeed an act of physical force, but the cyberattack preceding the bombing caused only a Syrian radar-system to overlook the incoming Israeli airplanes. Logic bombs or backdoors[5] are likely to have been slipped into the lines of code in the radar-systems software, but the incident became physical only through the bombing. Syria did not officially threaten Israel prior to the attack, and they did not respond with attempts to cause physical damage. However there is little doubt that Israel saw the construction of a nuclear facility as an act of war and thus considered their attack as a pre-emptive act of self-defence (Patrick 2013).

Stuxnet is different. It managed, as the only confirmed cyberattack to date,[6] to cause direct

4 Considering the cyberattacks in Estonia in combination with the similar attacks in Georgia during the South Ossetian conflict in August 2008 (Tikk et al. 2008), cyberattacks have yet to have operational effect or impact the people's trust in government.

5 Logic bombs are hidden software installed in computer system set to trigger a malicious function under given circumstances (Krepinevich 2012: 84). Backdoors are hidden lines of code enabling remote access without normal authentication (Schreier 2012: 52)

6 Scholars have pointed to a still unconfirmed incident in Siberia in 1982 where a logic bomb allegedly caused a Russian gas pipeline to explode (Andres 2012: 89; Rid 2011: 10-11).

physical damage to an underground nuclear facility, which conventional military strikes may have had difficulty in doing. In doing so, Stuxnet is the most complex malware yet detected. It targeted the specific Siemens Industrial Control System used at the facility, it took advantage of four yet unknown vulnerabilities in the operating systems, it used stolen verification certificates to circumvent the anti-virus software, and it exploited default passwords, all the while bridging the *air-gap* between the open Internet and the facility's 'offline' IT-infrastructure (Nachenberg 2012). Whether complex or not, Stuxnet has proved that causing physical damage from a cyberattack *is* possible.

***

The above exercise has avoided merely testing concepts from *On War* against the empirical events. Instead the analysis has used Clausewitz's idea of the political, tactical and physical nature of war to investigate the character of cyberattacks, based on the knowledge gained from the events in Estonia, Syria and Iran. The important lesson from the above is that cyberattacks *can* be politically motivated *can* cause physical damage, and *can* have an independent tactical purpose, instrumental towards reaching a political objective. Based solely on an empirical analysis on the cyber-events so far, it is impossible to reject that cyberwar will take place (Rid 2011). Clausewitz claimed that "war consists of a continuous interaction of opposites" (2007: 84), thus to further the understanding of the relationship between cyberattacks and war, it becomes relevant to investigate, whether cyberattacks are likely to be the primary attacks used in the interaction between opposites in war.

IS CYBERWAR REALLY COMING?

It is impossible to predict if a cyberattack will cause the outbreak of a war sometimes in the future. Throughout history wars have started in countless ways, but claiming that a cyberwar is coming is different. *A cyberwar must necessarily require that cyber-tools are the primary weapons used in fighting the battles.* A war, initiated with a cyberattack, but in which the battle subsequently moves into the sphere of conventional attacks cannot logically be characterised as a cyberwar.

It has already been shown that cyberattacks can be politically motivated, used to pursue tactical aims, and cause physical damage. While these characteristics are important requisites for a war fought with cyber-means, Clausewitz further introduces war as a series of reciprocal interactions between two adversaries (2007: 84). War is never a single, short and decisive blow (2007: 16-19). It is therefore natural, when analysing whether cyberwar is coming, to investigate whether retaliations are likely to take place and whether war is to be fought primarily with cyber-means.

So far, all cyberattacks have been weapons used only for the initial attack. None of the attacks detected so far have caused serious counteracts. Some scholars have pointed to anonymity as the obstacle to the interaction between adversaries, because retaliation, so it is claimed, requires attribution (Libicki 2009a: 39-44; Clarke & Landau 2011). Indeed the origin of a cyberattack can be impossible to verify as adversaries can route cyberattacks through compromised computers all over the world (Owens et al. 2009: 139-141). But it is misleading to argue that anonymity renders retaliation, and thus the reciprocity of a Clausewitzian war, unlikely. Turning instead to the relationship between strong and weak actors in contemporary international relations and the technical character of cyber-attack, the fol-

lowing shows that while retaliation is possible, cyber-means remain inferior to conventional weaponry and are therefore not likely to be the primary weapon in future wars.

Retaliatory Interactions between the Strong and the Weak

On War does not deal much with anonymity. Only when writing about the people in arms, did Clausewitz suggest that defensive uprisings "should be nebulous and elusive [and] never materialize as a concrete body" (2007: 187). But how does one deal with anonymity and how does one know where to strike back? For Clausewitz, this is not difficult, as the territory as well as context of the fighting give away *the people in arms*. Indeed the exact perpetrator may be able to stay hidden, but this does not stop the target from retaliating. The context also plays a key role when dealing with anonymous cyberattacks. Based on the geo-political situation and technical capabilities, anonymous cyberattacks have been ascribed to both states and non-state actors. Russia, whether Kremlin or Russian hackers, had an interest in the memorial in Tallinn as a symbolic artefact tying Russia to one of the former Soviet republics, Israel had expressed their concern about the Syrian nuclear reactor in Dayr ez-Zor, and the United States and Israel had both the will and capacity to bring the Iranian nuclear aspiration to an end.

With this in mind, it is unlikely that the absence of retaliatory attacks in cyberspace can be blamed on technical inability to attribute cyberattacks. In the three incidents examined above, the cyberattacks, when assessing the context, appeared to originate from within strong military states, and have targeted what, in military and technology terms, might accurately be described as weaker states.

Whether possible for weaker states to exploit the weak protection of much IT-infrastructures of stronger states or not (McGraw & Fick 2011; McGraw 2013), the significance of strong and weak states should not be overlooked. Consider the Syrian or Iranian incident in reverse – a cyberattack destroying a nuclear or military facility in Israel or the United States. It requires little knowledge of Israeli and American history, politics, or identity to know that retaliation would be inevitable in order to satisfy domestic political demands, but also to maintain the impression of military superiority. This conventional logic of power politics, rather than anonymity is likely to prevent weaker states – if capable – from launching cyberattacks in an attempt to cause physical damage in revenge for cyberattacks committed on their soil.

State actors, preparing a cyberattack with the ability to cause serious damage to an opponent's infrastructure, are aware of the fact that the attack, if executed, is likely to give the targeted state a sense of legitimate right to retaliate. If the targeted state is relatively strong it is likely to go through with a retaliatory attack. If the state, on the other hand, is relatively weaker, it will fear an escalation of war, as the superior opponent can cause the most damage.

Even if non-state actors, who do not necessarily fear retaliation, are to deploy a cyberattack, which causes serious physical damage to unprotected infrastructures in stronger states, retaliation is likely. For the sake of argument, let us consider a scenario in which the alleged Iranian sponsored hacker groups, *Cutting Sword of Justice*, who took credit for the virus targeting Saudi Aramco in 2012, disrupting operations for two weeks due to a random deletion of data on 30.000 company computers (Bronk & Tikk-Ringas 2013; Mount 2012), managed to cause serious destruction in the United States. In this scenario, it seems non-controversial to suggest that the United States would demand from Iran an investigation, followed by prosecution and extradition of the attackers. Regardless of whether the Iranian Govern-

ment was behind the attack, or merely refused to investigate citizens on their soil, if the Islamic Republic was to be as non-corporative as the Taliban, it does not seem far-fetched to assume that the American public would demand retaliation. Thus, retaliation does not depend on any conclusive link. The Iraq and Afghanistan invasions support this observation.

In sum, recent events may suggest that anonymity has rendered retaliation and the reciprocal war unlikely (cf. Libicki 2009a). However, a cyberwar – fought primarily with cyber-means – cannot be rejected on the basis of anonymity. As long as the current international system is dominated by militarily strong states such as Russia, the United States and Israel, who continue to perceive themselves as states, that cannot tolerate military weaknesses politically or globally, retaliation is likely to follow from a serious cyberattack initiated by relatively weaker states or non-state actors. While some weaker state may be deterred from initiating a cyberattacks or serious retaliatory acts against stronger states, it is impossible to deny, based on the above, that cyberattacks causing physical damage and reciprocal interactions of force will not take place in the future. But if such reciprocal exchanges of force are to turn into cyberwars where cyber-tools are the primary weapon, retaliation needs to be by cyber-means.

Cyberattack as Inferior Weapons

Cyberattacks are characterised by their lightning speed, their large range, their low cost, the easy accessibility and their anonymity (Betz & Stevens 2011: 82-88; Krepinevich 2012). This has made some cyberwar-scholars see offensive cyberattacks as the primary weapons in future wars, with the alleged ability to cause physical damage similar to or more serious than conventional weapons (Clemmons & Brown 1999; Sharma 2009; Sheldon 2011). Empirically however, cyberattacks have yet to show this capacity (Samaan 2010; Gartzke 2013), and scrutinizing the technical character of cyberattacks casts doubt on the assertion that cyberattacks should be preferred to conventional military weaponry in launching future retaliatory attacks.

From a technical perspective, cyberattacks can be categorised into two types, *low-potential*, DDoS-attacks which only temporarily slow down, or shut down IT-systems without causing damage, and *high-potential* cyberattacks aimed at causing damage to specific targets (Rid & McBurney 2012). Low-potential attacks, like the one in Estonia, can cause annoyance, but have little impact and are easy to defend oneself against. E.g. cyber-security experts McGraw and Fick (2011: 44) have pointed to the fact that the cyberattacks against Estonia would "fail utterly launched against popular U.S. e-commerce websites such as Amazon or Google, possibly to a point of not even being noticed", because of the high security at these commercial websites. At the other end of the spectrum, high-potential cyberattacks have the ability, as Stuxnet proved, to cause physical damage.

At least initially, this form of cyberattack always targets the code of another IT-system; it always relies on human mistakes that have been made in the process of programming software or installing new computers; and depends on the ability of the attacker to exploit these mistakes (Libicki 2009a). This impacts the ability of cyberattacks as weapons in battle in a number of ways. First, it implies that targeting any object, such as a specific function at a nuclear facility is dependent on the attacker's ability to seek out vulnerabilities in, and gain access to, the computer software.

Second, the cyberattacker may cause a computer to dysfunction by disrupting the code in the industrial control system (ICS). However, it is rarely the computer, but rather the processes, which the ICS controls, that are impor-

tant to the attacker. Destroying a computer may temporarily halt the process, but computers in power grid, communication networks or nuclear power plants invariably break down sometimes anyway. Fixing or replacing computers are not rare, fairly easily accomplished practices, and the cost is comparatively modest.

Third, cyberspace is complex. The complexity has reached an extent where no individual has the full understanding of the technical side and social effects of cyberspace. Power grid and communication networks are sometimes linked across international borders (Krepinevich 2012: 65), and servers and it-infrastructures are interconnected across public and private networks. As a result, the potential second-order effects are almost impossible to fully predict.

Fourth, cyberattacks are complicated by the relationship between code and the targeted process. The source code consists only of raw data that reveals a minimum of information about what process the different strings and queries in the code controls. Thus, targeting the actual process, be it the process that regulates the dispensing of sugar onto doughnuts at a doughnut factory or the process that regulates the chlorine content at the water plant, demands not only programming skills to alter the code but also technical knowledge of the processes and machineries at the factory. Furthermore, most vital infrastructures, which are controlled by ICS, have safety systems. These prevent the unexpected from causing serious damage. If the chlorine content in the water plant is too high or the centrifuges at a nuclear facility spin too fast, the processes are programmed to stop. Hence, in a cyberattack that causes physical destruction to an object, such as Stuxnet did, the attacker needs to acquire a thorough knowledge of the IT-infrastructure, technical know-how about the nuclear-processes and time necessary to plan and test the cyberattack (Langner 2011; Sanger 2012).

Lastly, following an attack, the knowledge of the cyber-weapon has an impact on the ability to use the same weapon again. Not only the targeted actor, but also all other actors relying on the software that has been exploited by the attacker can fix those vulnerabilities, which made the attack possible in the first place. Thus when cyberattacks are used, the attacker is likely to lose the ability to use the same attack again. This renders cyberattacks *use and lose capabilities* (Gartzke 2013).

In sum, the efficacy of a cyberattack, compared to conventional bombing of a nuclear facility, the establishment of a no-fly zone or boots on the ground, is limited by the fact that cyberattacks take time to prepare and depend on a number of unknown factors such as the ability to discover and exploit vulnerabilities in the enemy's IT-infrastructure. Cyberattacks may cause convenient and somewhat discreet disturbances to an enemy state, but when states' feel justified in escalating the conflict militarily, damaging physical hardware remains more difficult to undertake through cyberspace than through conventional military strikes (Peterson 2013; Rid 2013). Thus, cyberattacks are neither likely to be the only nor the preferred form of attack, where a strong state decides to retaliate against an attack carried out on their soil.

***

On War's emphasises the reciprocal interactions of force as a key characteristic of war (Clausewitz 2007: 13-19). Taking this as a starting point, this section asked whether cyber*wars* are a likely future scenario, by analysing whether cyberattacks are to cause retaliation, and whether the reciprocal interactions of war will stay within the remit of cyberspace. It was argued that cyberattacks could result in retaliation if the attacks are serious enough and if they target powerful states. However, the in-

ferior ability of cyberattacks to cause physical damage compared with conventional weaponry renders it unlikely that strong military states will stay bounded by the limits of cyberspace. Thus a cyberwar, fought entirely or primarily within the boundaries of cyberspace, is an unlikely future scenario.

The following takes yet a step further and asks: if cyberwar is unlikely to take place, then what role is cyberattacks likely to play within future conventional wars? Some have claimed that offensive cyberattacks are new and unique tools applicable in future war, and have argued that the nature of these tools challenge *On War* (Arquilla & Ronfeldt 1997; Farwell & Rohozinski 2012; Mirenda 2011). The following discussion questions these claims. By introducing Clausewitz's trinity to the cyberwar debate, it aims at shedding light on the limits and opportunities of cyberattacks in war.

THE UTILITY OF CYBERATTACKS IN WAR

At first glance, cyberspace as a technological invention of the late 20th century seems far removed from a book on war published in 1832, which allocated only few lines to the role of technology in war. When considering technology as something that resides in all part of Clausewitz's trinity of the *passion of the people*, *creativity of the army* and *reason of government*, it becomes possible to assess the significance of new technologies in current and future wars (Echevarria 1995/96).

A number of scholars, optimistic about computer and information technologies, see offensive cyber-capabilities, see as intrinsically stronger than defensive cyber-capabilities and especially useful for the government, not only when pre-planning or calculating the effect of an attack, but also in mitigating the risks and uncertainties on the physical battlefield (Berkowiz 1997; Farwell & Rohozinski 2012). A war, which can be pre-planned and executed without the risk of friction, is an attractive offensive tool for a government, in its attempt to control the outcome of war. However, the idea runs counter to Clausewitz's idea of war as a dynamic relationship between the irrational and passionate people, the non-rational and creative army and the rational government.

In investigating the utility of cyberattack in future wars, the following shows that cyber-technology does *not* render insignificant the creativity as represented by the army and passion as represented by the people. These elements *still* limit the ability of the rational government to control the war. This is not only a theoretically discussion, but it also provides insights into the relative strength of offence and defence and the role friction, when cyberattacks are used in war.

Trinitarian Cyberattacks in the Offensive-Defensive Nexus

In the sixth book of *On War*, Clausewitz claimed, "the defensive form of warfare is intrinsically stronger than the offensive" (2007: 160). The defence, fought on home soil, has the advantage in relation to *the terrain*, the benefit of the *fortresses* and *public support*. On the other hand, Clausewitz acknowledged that the offence had the initiative and the element of surprise (ibid.: 162-166).

In cyberspace there are, on an average day, thousands of vulnerabilities not yet made public (McGraw 2013: 110). This enables the attacker to gain much knowledge of the defender's IT-infrastructure and probably even more knowledge of the vulnerabilities of the specific IT-system than the defender. In a Clausewitzian terminology, the enemy's IT-infrastructures could be understood as *the terrain*, and the specific IT-system as *the fortress*. And due to the non-physical and instantaneous nature of cyberspace, the attacker does not need to

move amongst the people, but is likely to strike quickly and anonymously from afar. This has created a sense among politicians that cyberattacks are a politically controlled offensive, "collateral free" alternative to conventional war, as the cyber-soldier and politicians can sit together behind a screen achieving instant and preplanned effect simply by the press of a button (Gray 2005: 314; cf. Sanger 2012: 191). And when the average malware contains only 125 lines of code, while defensive systems have millions (Kenyon 2011), offensive cyberattacks appear, compared to defensive cyber-security, a cheap and attractive capability (Nye 2009: 125).

Although cyber-offence may appear stronger than cyber-defence, this does not contradict Clausewitz's offensive-defensive nexus. The current perceptions that the nexus is reversed (Farwell & Rohozinski 2012: 114) stem from a misunderstanding of Clausewitz as well as an overestimation of the power of cyberattacks. Today, defensive cyber-measures have been given a considerably lower priority in comparison with offensive cyber-tools. *On War* contains no suggestions as to whether to prioritise defence or offence, and it is clearly not within a Clausewitzian mind-set *not* to prioritise defences at all. To declare that the offence is intrinsically superior to defence, creates a self-fulfilling prophecy, as states ignore defensive security measures.

One important characteristic, which weakens a cyberattack, is its dependence on vulnerabilities, either those yet unknown by the enemy or those not yet fixed. Cyberattacks are *use and lose capabilities* with the ability to cause direct damage or work as a force multiplier. As soon as a cyberattack is recognised, the defending countries can correct the liability and thereby neutralise the attack. Thus, the ability to keep using cyberattacks in war demands that the *creative army* continues to discover new vulnerabilities. If the offence targets a specific military facility within enemy territory, the attacker needs to be aware of the enemy's potential cyber-capability, and needs to collect intelligence on the targeted facility's IT-systems, discover and exploit known and unknown vulnerabilities and successfully plan, test and execute the cyberattack. This takes time. In light of cyberattacks' inferior ability to cause direct damage, it is understandable that the United States and NATO decided to use conventional military air-bombings in Libya during the Arab Spring in 2011, and not cyberattacks (Maurer 2011; Rid & McBurney 2012).

The lack of defensive efforts in fixing the *known* vulnerabilities in cyberspace and in creating software security standards are two of the main reasons for the continued opportunity for offensive cyberattacks. Stuxnet is illustrative in this regard. Indeed the attack on the Iranian nuclear facility was sophisticated, but dissecting the malware reveals that while relying on four at the time unknown vulnerabilities, most of the components used, such as default passwords were well-known to IT-security firms (Nachenberg 2012). Hence, the most sophisticated cyberattack ever conducted, relied on *known* vulnerabilities, which could have been fixed. Thus cyber-security, such as encryptions and continuously installing security updates, would make it considerably more difficult to execute a successful cyberattack. It is thus discomforting that the Snowden leaks have shown that the NSA is deliberately weakening IT-security standards in commercial software to be able to spy on ordinary citizens (Schneier 2013).

With this limit in mind, the utility of offensive cyberattacks hinges on the important role of the *creative army*. As Clausewitz argued, the offence only has an advantage when it maintains the initiative. In cyberspace, the advantage shifts to the defence, when the known vulnerabilities in cyberspace are exhausted. When an offence depends on a continuous dis-

covery and exploitation of new vulnerabilities to maintain the offence initiative in war, the success in war not only depends on the rational government, but also on the non-rational, *creative* part of the trinity, which is often associated with the army.

The advantage of offensive cyberattacks is further complicated, just as Clausewitz predicted, by the third part of the trinity, *the passionate people*. Clausewitz gave the advantage to the defence partly due to the fact that the offence needed to fight its way through an enemy territory where people might have taken up arms. Cyberattacks indeed avoid physical enemy territory, but cyberspace also creates a space for the people to *take up arms*. Cyberspace enables people to become familiar with cyber-tools and communicate with likeminded online. This creates opportunities for radicalisation, mobilisation and possibly resistance (Arquilla & Ronfeldt 1996; Denning 2001). Well-known 'hacktivist' groups, such as Anonymous, have proven that taking the law into their own hands is possible in cyberspace.

Although it is significantly harder for non-state actors to cause physical damage to specific vital infrastructures through the Internet, there is little doubt, with the cyberattacks in Estonia in mind, that individuals or groups can wield the power to undermine trust in government. It is far from improbable that future cyberattacks, conducted by individuals, could cause random physical damage to badly protected infrastructures or disruption to communication networks. Cyberspace is, therefore, just as *the terrain,* a space in which the *passionate people* can roam.

In short, armies' neglect of defensive cybersecurity-measures, the low barrier to entry and the ability to communicate with and mobilise likeminded individuals through cyberspace provide excellent *opportunities* for the non-rational and irrational parts of the trinity to use cyber offensive capabilities, and *limits* the rational government ability predict and preplanned effects of a cyberattack. As a weapon in war, cyberattacks are *use and lose capabilities*, which means that these forms of attack are likely "to be most effective as an opening salvo" in war (Liff 2012: 417).

The utility of cyberattacks can be developed further through the trinity by investigating cyberattacks ability to deal with *friction*.

Friction as Limits to the Rational Use of Cyberattacks

On paper, cyberattacks, especially when priority is given to the offence and not the defence, are useful tools for both the military and the rational government that aims to control the war.

Clausewitz, however, remained sceptical about war on paper and pointed to friction, as the term, which described the inevitable unpredictability in war (2007: 66). Clausewitz exemplified friction by pointing to the gun that does not go off or rain delaying a battalion march. Friction is something the good general must be able to overcome, and something, which the government cannot control through reason.

That friction also applies in cyberspace can be illustrated by the operation *Olympic Games* in Iran. President Obama was specific about not wanting Stuxnet to be 'unattributable' (Sanger 2012: 202). But attribution did happen.[7] When analysing the way Stuxnet became publicly known, it is friction that springs to mind. The worm was designed to release itself only if detected by the computer controllers connected to the centrifuges at the Iranian nuclear facility, but Stuxnet started to spread throughout the Internet. The cause remains unknown but the event points to a well-known problem

7 Langner (2013) speculates that the uncovering stuxnet was part of the plan, as it "showed the world what cyber-weapons could do in hands of a superpower".

for every software manufacturer: poor testing (ibid.: 204). In practice computer code always does what it is programmed to do, but only rarely exactly as intended. *Friction* is a reminder that things do not always go as planned.

Friction is also embedded in the extreme complexity of cyberspace. The unique setup of computer infrastructures within private networks and their interrelationship with large public networks or with the Internet as a whole makes it difficult to foretell the potential consequences of cyberattacks. This is underscored by the U.S. army's attempt to shut down a website that was used by extremists. When dismantling the website, more than 300 servers in Saudi Arabia, Germany and Texas were inadvertently disrupted (Cornish et al., 2010: 23).

Another important component that nurtures friction is the use of intelligence or the uncertainty of all information, known as the *fog of war* (Clausewitz 2007: 64-66, 88-89). Clausewitz claimed that that knowledge gathered about the enemy is often contradictory and flawed. This in turn, makes it hard to determine how well an offence is going, ascertain when victory can be assured, or judge how reliable the information gathered is. The two post-9/11 wars in Afghanistan and Iraq spring to mind. The information gathered on WMD's in Iraq all turned out to be false, and measuring the progress made during the counterinsurgencies against the Taliban proved extremely difficult. In cyberspace, it is furthermore extremely difficult to ascertain whether an opponent happens to be exploiting vulnerabilities in one's own vital IT-infrastructures. Thus, cyberattacks are always launched in an uncertain environment with friction and fog inevitably present.

However, an offensive attacker could nevertheless attempt to achieve a *frictional imbalance* between itself and the enemy. Here cyberattacks are especially useful. Hackers can, after having successfully managed to access email or other means of online communication, quite easily alter the content of electronic messages used by the enemy when communicating internally (Libicki 2009b). U.S. Department of Defence's exercise, *Eligible Receiver* from 1997 proves the impact of this in a potential situation of war. The simulated North Korean hackers were so successful that "the Navy's human command-and-control-system was paralysed by mistrust, and nobody from the president on down, could believe anything" (Geers 2011: 26).

Thus, cyberattacks provide both limits and opportunities in war. On one hand, the capable and *creative army* can use cyberattack to confuse the enemy when quick decisions are need, thus creating a 'friction imbalance', which may force the opponent to make bad decisions in battle. On the other hand, friction still seems to be playing a role, as it remains impossible to completely overcome human mistakes, to see through the complexities of cyberspace and to assess the relative strength of oneself and the opponent through the information gathered.

Not only the army, but also the *passionate people* play a vital role in any war. In this regard, success is challenged by the fact that cyberspace provides information to an extensive number of people. During the Vietnam War, it was the pictures and video footage from Vietnam that acted as friction by mobilising global anti-war movements. Today any given attack in war – whether through cyberspace or not – is vulnerable to large online leaks, which have been made possible by the increasing number of confidential information stored in cyberspace. Spontaneous leaks similar to Wikileaks and the Snowden-leaks, which portrayed the horrors and double standards of American wars and intelligence gather, may have the same effect on people's support for the decisions in war as the pictures from the Vietnam War.

***

The above discussion of the limits and opportunities provided by cyberattacks in war has shown that if actors accept the risk of discovery, there are possibilities for the offence in searching for vulnerabilities in other state's vital infrastructures *before* war breaks out. When war comes, the pre-planned cyberattacks create advantages either through direct physical damage or as a force multiplier. But when war continues, the use of cyberattacks depends on the opponent's failure to protect infrastructures and correct known vulnerabilities as well as the offence's continuous discovery of new vulnerabilities. Counting on victory based solely on cyber-capabilities would therefore be a mistake. And friction is not the only reason for this. The nature of cyberspace makes it extremely difficult to know whether the opponent is able to exploit yet unknown vulnerabilities in one's own IT-infrastructure. Furthermore, the neglect of defensive cyber-measures provides individuals and groups, infused with hatred and enmity, with the ability to cause annoyance and damage. Thus cyberattacks are likely to play a role in future war, but not necessarily the leading one.

CONCLUSION

The article has shown that Carl von Clausewitz's *On War* (1832) brings useful insights to the cyberwar-debate. Motivated by a desire to theoretically correct, strengthen and move beyond the scholars that criticise the term *cyberwar*, it was argued, in the first section, that the oft-cited cyber-events in Estonia, Syria and Iran, when analysed through Clausewitzian lenses, could neither confirm nor deny future cyberwar, as the cyberattacks experienced so far have proved capable of causing physical damaged and have been used as tactical purposes instrumental towards reaching a political objective.

While this finding corrects critical scholars, such as Thomas Rid (2011), the second section took the cyber-critique a step further by arguing that cyberwars, when viewed through Clausewitz's idea of war as reciprocal interactions, are unlikely to come. Cyberwar will not replace conventional wars because strong states, attacked through cyberspace, are more likely to retaliate using conventional weapons, due to cyberattacks' inferior ability to cause physical damage. The article then took a step further, and examined the opportunities and challenges of using cyberattacks as weapons within conventional wars.

Inspired by Clausewitz's trinity, it was argued that cyberattacks provide possibilities for the *creative army* to find and exploit vulnerabilities in a potential enemy's IT-infrastructure, but that cyberattacks remain useful only in the initial phase of war. States, like the United States, which are dependent on insufficiently protected IT-infrastructures, are further vulnerable to *friction* as well as *the passionate people* that take up cheap and easy cyber-arms.

Offensive cyber-capabilities are cheaper than conventional military equipment and are politically more attractive than putting demands and restricting cyber-security measures on private businesses. Thus, countries have increasingly prioritised offensive cyber-capabilities. But, it remains vital for the governments who consider upgrading their military capabilities to assess the extent to which cyberattacks are useful against the current enemies, be they terrorist cells or state actors. In recent years where most wars have been fought against non-state actors, who are rarely bounded by a specific territory, or failed states without much IT-infrastructure, it is illogical for cyber-dependent states to upgrade cyber-offences at the expense of cyber-security measures. Thus, for an offensive cyber-unit to justify its existence, it needs to create new enemies that can be targeted with cyber-weapons. In this regard, the

increasing focus in the United States on the China as both a cyberthreat and economic competitor point to a possible return to bipolar balance of power in which cyber offensive measures may have a future role to play.

Throughout history, the military has shown an extreme resilience in maintaining government funding. Thus it is likely that upgrading offensive cyber-capabilities will continue. With further militarisation of cyberspace and new technological development in conventional weaponry such as drone technology, the future is likely to bring even more complexity, and with it comes an increasingly muddied picture of what war is, when war is, and how to control war. Clausewitz and his classical theory of war is an invaluable aid in cutting through this fog.

BIBLIOGRAPHY

Adams, J. (1998), *The Next World War*, New York: Simon & Schuster

Andres R. (2012), 'The Emerging Structure of Strategic Cyber Offence, Cyber Defence, and Cyber Deterrence', in D. Reveron (ed.), *Cyberspace and National Security – Threats, Opportunities, and Power in a Virtual World*, Washington D.C.: Georgetown University Press

Arquilla, J (2012), 'Cyberwar is already upon us', Foreign Policy, March/April, available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

Arquilla, J. & D. Ronfeldt (1993), 'Cyberwar is Coming!', *Comparative Strategy*, 12(2): 141-165

—— (1996), *The Advent of Netwar,* Santa Monica, CA: RAND Corporation

—— (1997), 'A New Epoch-and Spectrum-of Conflict' in J. Arquilla and Ronfeldt, D.F (eds), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND

Berkowiz, B. (1997), 'Warfare in the Information Age', in J. Arquilla and Ronfeldt, D.F (eds), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND

Betz D. & T. Stevens (2011), *Cyberspace and the State – Towards a Strategy for Cyber-Power*, Abingdon: Routledge

Brito, J. & Watkins T. (2011), 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy', Working Paper no. 11-24, Mercatus Center, Geroge Maso University Press. Available at http://mercatus.org/sites/default/files/WP1124_Loving_cyber_bomb.pdf

Brook, C. & E. Tikk-Ringas (2013), 'The Cyber Attack on Saudi Aramco', *Survival: Global Politics and Strategy*, 55(2): 81-96

Cavelty, M.D. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge

—— (2012) 'The Militarisation of Cyberspace: Why less may be better', Paper for the 2012 4th International Conference on Cyber Conflict, NATO CCDCOE, Tallinn. Available at: http://www.ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf

Clark, D. & S. Landau (2011), 'Untangling Attribution', *Harvard National Security Journal*, 2(2): 25-40

Clarke, R. & Knake R. (2010), *Cyber War: The Next Threat to National Security and What to Do About it*, New York: HarperCollins

Clausewitz, C.v. (2007 [1832]), *On War*, translated by M. Howard and P. Paret, edited by B. Heuser, Oxford: Oxford University Press

Clemmons B. & G. Brown (1999), 'Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction', *Military Reveiew*, 79(5): 35-45

Cornish, P., D. Livingstone, D. Clement & C. Yorke (2010), 'On Cyber Warfare', Chatham House Report, available at: http://www.chathamhouse.org/publications/papers/view/109508

D'Amato, A. (1983), 'Israel's Air Strike upon the Iraqi Nuclear Reactor, Editorial Comment', *American Journal of International law*, 77: 584-588

Davis, N. (1997), 'An Information-based Revolution in Military Affairs', in in J. Arquilla and Ronfeldt, D.F (eds), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND

Dennings, D. (2001), 'Activism, Hacktivism, and Counterterrorism: The Internet as a tool for influencing foreign policy', in J. Arquilla & D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica CA: RAND Corporation

Echevarria II, A. (1995-96), 'War, Politics and RMA—The Legacy of Clausewitz', *Joint Force Quarterly,* winter: 76-80

Farwell J. & R. Rohozinski (2011), 'Stuxnet and the Future of Cyber War', *Survival: Global Politics and Strategy*, 53(1): 23-40

—— (2012), 'The New Reality of Cyber War', *Survival: Global Politics and Strategy*, 54(4): 107-120

Foltz, A.C. (2012), 'Stuxnet, Schmitt Analysis, and the Cyber "use-of-force" Debate', *Joint Force Quarterly*, 67(4): 40-48

Fulghum, D., R. Wall & Amy Butler (2007), 'Israel Shows Electronic Prowess', Aviation Week, 25 November

Gartzke, E. (2013), 'The Myth of Cyberwar – Bringing War on the Internet Back Down to Earth", *International Security*, forthcoming

Geers, K (2009), 'The Cyber Threat to National Critical Infrastructures: Beyond Theory', *Information Security Journal: A Global Perspective*, 18(7): 1-7

—— (2011), *Strategic Cyber Security*, Tallinn: CCDCOE Publication

Gray, C.S. (2005), *Another Bloody Century. Future warfare*, London: Phoenix

—— (2007), *War, Peace and International Relations – An Introduction to Strategic History*, Abingdon: Routledge

Guha, M. (2011), *Reimagining War in the 21st Century – From Clausewitz to network-centric warfare*, Abingdon: Routledge

Hansen L. & H. Nissenbaum (2009), 'Digital Disaster, Cyber Security and the Copenhagen School', *International Studies Quarterly,* 53(4): 1155-1175

Herberg-Rothe, A. & W. Honig (2007), 'War Without End(s): The end of Clausewitz?', *Distinktion*, 8(2): 133-150

Heuser, B. (2002), *Reading Clausewitz*, London: Pimlico

—— (2007), 'Introduction', in Clausewitz (2007 [1832]), *On War*, translated by M. Howard and P. Paret, edited by B. Heuser, Oxford: Oxford University Press

JCS, Joint Chiefs of Staff (2006), 'Joint Doctrine for Information Operation', Joint Publication no. 3-13, 13 Feb.

Keegan, J. (1993), *A History of Warfare*, London: Hutchinson

Kenyon, H. (2011), 'DARPA to develop offensive cyberspace capabilities' DefenseSystems.com, available at: http://defensesystems.com/articles/2011/11/07/darpa-offensive-cyber-capabilities.aspx

Krepinevich, A.F. (2012), 'Cyber Warfare – A "Nuclear Option"?', Paper from Center for Strategic and Budgetary Assessment, Available at http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/

Lander, M. & J. Mankoff (2007), 'Digital Fear Emerges After Data Siege in Estonia', The New York Times, 29 May, available at: http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&

Langø, S. (2013), 'Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security', NUPI Working Paper 820, Norwegian Institute of International Affairs.

Langner R. (2011), 'Cracking Stuxnet, a 21st-century cyber weapon', TED Talks, available at: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

—— (2013), 'Stuxnet's Secret Twin', Foregin Policy, 19 November, available at http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack

Lawson, S. (2011), 'Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History', Working Paper, Fairfax, VA: Mercatus Center.

—— (2012), 'Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States', *First Monday*, 17 (7) – 2 July

Lesk, M. (2007), 'The New Front Line – Estonia under cyberassuault', *IEEE Security and privacy*, July/August: 76-79

Libicki M. (2009a), *Cyberdeterrence and Cyberwar,* Santa Monica: RAND

—— (2009b), 'Sub Rosa Cyber War', in C. Czosseck & K. Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam: IOS Press

Liff, A, (2012), 'Cyberwar: A New 'Absolute Weapon'? The Strategic Proliferation of Cyberwarfare Capabilities and Interstate War', *War of Strategic Studies,* 35(3): 401-428

Lonsdale, D. (2004), *The Nature of War in the Information Age – Clausewitzian Future*, New York: FRANK CASS

Maurer, T. (2011), 'The Case for Cyberwarfare', Foreign Policy, 19 October, available at: http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar

McConnell, M. (2010), 'Mike McConnell on how to win the cyber-war we're losing', Washington Post, 28 Feb., available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

McGraw, G. (2013), 'Cyber War is Inevitable', *Journal of Strategic Studies*, 36(1): 109-119

McGraw, G. & N. Fick (2011), 'Separating the Threat from the Hype: What Washington Needs to Know About Cyber Security', in American's Cyber Future: Security and Prosperity in the Information Age Volumes I and II, Washington DC: Center for a New American Security)

Miranda, R. (2011), 'Offensive Cyber Warfare', Marine Corps Gazette, 11 September

Moss, K.B (2013), 'Ambiguity and Accountability in War: The Challenge of Cyber and Unmanned Systems', Presentation at the Danish Institute for International Studies, 20 June

Mount M. (2012), 'U.S. Officials believe Iran behind recent cyber attacks', CNN.com, 16 January, available at: http://edition.cnn.com/2012/10/15/world/iran-cyber

Nachenberg, C. (2012), 'Dissecting Stuxnet', presentation at Stanford University, available at: http://www.youtube.com/watch?v=DDH4m6M-ZIU

Nye, J. (2009), *The Future of Power*, New York: PublicAffairs

Owens, W., K. Dam and H. Lin (2009), *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capability*, National Research Council, Committee on Offensive Information Warfare, Washington D.C.: The National Academies Press

Palmer, S. (2010), 'Cyber-Terrorism vs. Cyber-Warfare', *The Entertainment and Sports Lawyer*, 28(1): 22-24

Patrick S.M. (2013), 'Israel's Preemptive Strikes on Syria: Self-Defense Under International Law?', Council of Foreign Relations Blogs, available at: http://blogs.cfr.org/patrick/2013/02/05/israels-preemptive-strikes-on-syria-self-defense-under-international-law/

Peterson, D. (2013), 'Offensive Cyber Weapons: Construction, Development, and Employment', *Journal of Strategic Studies*, 36(1): 120-124

Rid, T. (2011), 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35(1): 5-32

—— (2012), *Cyber War Will Not Take Place*, London: Hurst & Company

—— (2013), 'More Attacks, Less Violence', *Journal of Strategic Studies*, 36(1): 139-142

Rid, T. & P. McBurney (2012), 'Cyber-Weapons', *the RUSI Journal,* 157(1): 6-13

Roscini, M. (2010), 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force', Max Planck Yearbook of United Nations Law, 14: 85-130

Samaan, J. (2010). 'Cyber Command: The Rift in US Military Cyberstrategy', *The RUSI Journal,* 155(6): 16-21

Sanger D.E. (2012), Confront and Conceal – Obama's Secret Wars and Surprising Use of American Power, New York: Random House

Schneier, B. (2013), 'Bruce Schneier: NSA Spying Is Making Us Less Safe', MIT Technology Review, 23 September, available at: http://www.technologyreview.com/news/519336/bruce-schneier-nsa-spying-is-making-us-less-safe/

Schreier F. (2012), 'On Cyberwarfare' DCAF Horizon 2015 Working Paper no.7, available at: http://www.dcaf.ch/Series-Collections/DCAF-Horizon-2015-Working-Paper-Series

Shackelford S.J. (2009), 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', *Berkeley Journal of International Law*, 27: 192-251

Sheldon J. (2011), 'Deciphering Cyberpower – Strategic Purpose in Peace and War', *Strategic Studies Quarterly*, Summer: 95-112

Shlaim, A. (2000), *The Iron Wall – Israel and the Arab World,* London: Penguin

Sharma, A. (2009), 'Cyber Wars: A Paradigm Shift from Means to Ends', in C. Czosseck & K. Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam: IOS Press

Stone, J. (2013), 'Cyber War Will Take Place!', *Journal of Strategic Studies*, 36(1): 101-108

Strachan H. & A. Herberg-Rothe (2008), *Clausewitz in the Twenty-first Century*, Oxford: Oxford University Press

Tikk, E, K.Kaska, K. Rünnimeri, M. Kert, A. Talihärm and L. Vihul (2008), 'Cyber Attacks Against Georgia: Legal Lessons Identified', Paper, CCDCOE, Tallinn. Available at:: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

van Creveld, M. (1991), *The Transformation of War*, New York: The Free Press