GÖTEBORGS UNIVERSITET

DEPARTMENT OF POLITICAL SCIENCE

UPLOADING WAR:

The Weaponisation of 0s and 1s and the Changing Nature of War

NOAH BELL

Abstract

As digital technology revolutionises the world, it is not surprising that it is altering the way states conduct themselves, especially in terms of war. War is a powerful policy tool of states and its implications are massive. This thesis looks at how existing definitions of war are insufficient in dealing with cyberwar and what are the implications by relying on them. It addresses a gap within political science of the nature of cyberwar and how it relates to the concepts of violence, legitimacy, targets, and political outcomes. This thesis highlights how a reluctance to reassess war as a solely physical phenomenon is problematic. Using a heuristic comparative case study analysis of i) Stuxnet (Israel and US attacks on Iranian nuclear facilities); (ii) Russian election interference in the 2016 US Presidential Election; and (iii) NotPetya (Russian cyberattacks on the Ukraine), a foundational theory is developed. This foundation is built around a concept of an extended causal chain that better describes the mechanisms through which cyberwar is an effective tool. This will provide a basis for further research to build on, as the field is impeded by a lack of data to conduct rigorous theory testing.

Keywords*: war; cyberwar; cyberattacks; violence; legitimacy*

Master's Thesis	30 HEC
Programme:	Master's Programme in Political Science
Submitted:	18 August, 2020
Supervisor:	Ulrika Möller
Words:	19,951

Contents

1. Introduction

When one thinks of war, often fields of soldiers with weapons in their hands, and corpses littered in between come to mind. There is a sense of chaos and physical destruction. This image reflects how wars have been fought for thousands of years. Perhaps, you conjured a more modern image: tanks, airpower, bombs, drones flying over foreign lands. This too makes sense, with the history of WWI and WWII being oft studied and war in the Middle East defining a new generation. These images however, despite technological advances, have one thing in common. They rely on physical destruction through munitions.

Political science literature also reflects this physical nature of war. Theorists and practitioners have dedicated many volumes to how the interactions between states and their numbers of munitions, military strategies, and global interconnection has shaped war. However, the invention and massive uptake of the internet has revolutionised how war can be conducted.

Internet-based technologies have weaved their way into almost every facet of modern life. Digital technology can and is used for warfare and aggression between states - a shift from the physical world into the intangible – cyberspace. 0s and 1s, pulses of electricity or electromagnetic waves, travelling through undersea cables and the air, can be weaponised. We live in a period of near total saturation of devices that civilian lives can, quite literally, rely on. This means that the risks associated with cyberwar have multiplied.

In a way, this weaponisation is fitting given the internet was created by the US military; albeit as a solution to "how do government officials and military officers communicate and maintain control in the aftermath of global thermonuclear war?" (Streck 2013, p.18). The internet can be used to wreak havoc as an instrument of war as humans and our surroundings become increasingly (inter)connected. Former White House security advisors, Richard Clarke and Rob Knake provide an ominous description of a worst-case cyberwar scenario:

> *"…classified Defence networks are compromised […] oil refineries are on fire and exploding, releasing toxic fumes, simultaneously chlorine gas is being released from chemical plants. Air traffic control is wiped out, […] trains have derailed or collide as signals are taken offline. The financial system is in meltdown as the servers that manage the entire banking system have been compromised."*
>
> (2010, p.47).

Given this destructive potential, it is important that cyberwar be investigated further so that governments can determine how to best protect their citizens. For the field of political science, this research is important because whilst the literature has begun to address the possibility of cyberwar, it is often rooted in an understanding of conventional war. Based on the available literature today, it is unclear whether Clarke and Knake's scenario would be captured as a war, if caused by a foreign state. Whereas, if a state were to cause that kind of damage using munitions, it is highly likely that a war would be declared.

As the world in which states conduct themselves has been revolutionised by Information Communication Technologies (ICTs), it is important that political science too evolves the definitions and assumptions from the 18th, 19th and 20th centuries that underpin the mechanisms of international relations (IR) theory and more specifically for this thesis, war.

1.1 The Problématique

At the beginning of any new epoch there is a period of transition where old definitions that shaped the past begin to give way to definitions that will shape the future. This thesis argues that how we think about and define interstate warfare is an important definition to reassess. Especially because the current literature is deeply connected to definitions of war created when airpower did not exist, let alone the internet. Thomas Rid, in casting doubt about cyberwar inadvertently illuminated this, "commentators fail to grapple with a basic question: What counts as warfare?" (2013.b). For Rid and many of his contemporaries, war is still as described in the opening paragraph – violent and physically destructive. However, this type of warfare is no longer representative of how states are using new capabilities.

The changes that have been occurring that this thesis argues warrant further investigation into the changing nature of war are: (i) a change in the nature of violence; (ii) changes to the concept of legitimacy; (iii) a broader possibility of targets; and (iv) a change in expected and possible outcomes. Whilst there are sub-categories, e.g. guerrilla, naval, and information war, that already exist and address these points, the concept of war is based on kinetic capabilities. [1] The thinkers and practitioners who have relied on and developed these sub-categories of war had no possible way of knowing how war could be conducted in the future when they formed those definitions.

1.2 Research Question and Aim

By answering the following research questions this thesis aims to lay the groundwork for full theory development of incorporating cyberwar as a feature of war. Recognising that digital technologies have reshaped that world and the tools available to states. The two research questions are:

How is the current definition of war (within political science) insufficient to properly explain cyberwar?

What are the implications of relying on established definitions of war in relation to cyberwar?

1.3 Outline

This thesis will begin by exploring modern international relations theory and how it attempts to explain interstate relations and war. It will proceed by exploring in greater depth the nature of war and the limitations that these traditional understandings of war pose in the present. Thirdly, this thesis will delve into cyberspace and cyberattacks. These sections will attempt to only be as technical as necessary in order to shape understanding in the political realm and will not examine specificity of how these attacks are carried out. Fourthly, the most likely targets in a cyberwar will be specified. Fifth, drawing on the above, this thesis will explore what cyberwar is, making linkages specifically back to IR theories and war. Sixth, a heuristic multi-case study will be conducted to create a framework for future theory development in this area. Finally, a results and concluding section will form a foundation of a new theory of war.

[1] i.e. based on physical munitions.

2. International Relations (IR) Theory

Presently, the body of literature that addresses the nature of state relations, inclusive of war, is IR theory. Since the end of WWII and then after the Cold War, there has been a stability in the international system that has tempered the warring nature of states. This relative stability led to the development of modern IR theory. There are two main paradigms, realism, and liberalism. Both rely on different assumptions from which sub-theories have developed. These theories are not exhaustive but they aim to explain state relations through "mutual deterrence and balanced arms control, stability and instability, national interests and international security; […] crisis management, regional integration, and the viability of alliances under strain" (Dougherty and Pfaltzgraff 2000, p.1). The theories developed attempt to explain relations between states in times of peace and how war can be avoided, but also what precipitates the outbreak of war (Levy 1998, pp.141-143).

2.1 Realism

Realism is the formalisation of centuries of philosophical thought about the nature of human beings and by extension the nation-state. At the heart of realism is a Hobbesian idea that humans are inherently violent; therefore, so are states (see Hobbes 1651). In a way, there is a paradox at the heart of the nation-state, it has been noted that the state is born of war and war is born out of states (Kapferer 2004; Porter 2002). Porter says, "war is an organising force," not only does warfare require the mass ordering of society to produce enough resources to sustain a war (e.g. munitions, skilled fighters etc.) but this order also shapes the nation-state (2002, p.1). It is a state's capacity to use their monopoly on the legitimate use of violence to both enable domestic law and order, but also to defend itself from external threats or seek expansion.

The formalisation of these ideas produced a set of basic assumptions that explain state relations and why they go to war. Namely that: (i) states are the primary agents; (ii) states are rational; (iii) states are security maximisers in a zero-sum world, i.e. power is relative; and (iv) the international system is anarchic, i.e. there is no universal authority (James 1995, p.183; Waltz 2010). This anarchic environment and the desire to always be a security maximiser, could create the conditions for a rationally acting state to go to war to maximise their security by eliminating another state or their military capabilities.

Within realism, two of the best theories to explain tensions between states are deterrence theory and the security dilemma. Deterrence theory has four components: (i) a 'red line' in which behaviour that crosses it is unacceptable; (ii) communication of this red line to an adversary, such that they know violations will be punished; (iii) the capability to carry out the threat; and (iv) in the case of non-compliance, carrying out the threat (Jervis 1979 & 1989). Ultimately, the failure of a state to obey the command of another could lead to war as (iv) is enacted.

Secondly, the security dilemma argues that as states increase their military capabilities to defend themselves, other states become increasingly nervous that they are under threat and accordingly increase their own security. Jervis was an early pioneer of this theory, linking it to the game theory game stag hunt. Whereby cooperation is often the best outcome for all parties involved; however, many are often tempted to seek their own security in the hope that others disarm (Jervis 1978, pp.167-168; Glaser 1997, p.171). The security dilemma posits that as states become hyperaware of security and relative power, each increasing their own leads to a spiralling arms race, which makes it more

likely for states to make mistakes or remain stuck in predetermined ideas and shut down the possibility to take in new information and due to the increase in military capabilities could make an ensuing misstep more violent (Van Evera 1998).

Shortcomings of realism are its reliance on clear communication and the ability for states to conduct a rational calculus on the information that they have. If the information is incomplete or failed to be communicated correctly, it is possible that a state acts against their own interest. As will be explored later, this has implications when looked at later in relation to cyberwar (**Section 8.2**).

2.2 Liberalism

Liberalism shares some assumptions with realism but has several notable differences. One key difference is that power is a positive sum game, i.e. one state's gain in security is not necessarily the loss of another's; collectively security can be gained without minimising the security of other states. Liberalism argues that through interdependence, the anarchic system described by realists can be mitigated, thereby reducing the likelihood of the security dilemma from occurring (Nye 1988). Another tenant of liberalism is democratic peace theory, which states that liberal democracies do not go to war with other democracies (Buchan 2002, p.407).

Interestingly, the liberal war thesis suggests that war is, paradoxically, an inbuilt feature of liberalism's desire for peace and freedom. Dillon and Reid suggest that liberalism is reliant on a commitment to war, it is an actively sought-after policy tool that governs both its internal functioning through states of emergencies and war preparedness but also its external relations in terms of spreading peace and freedom (2009, p.8). For example, this appears to be true for many of the wars that the US has been involved in in the late 20th and early 21st centuries.

Liberalism has arguably tempered war, condemning the use of total war,[2] and establishing a more formal set of rules about it. Nevertheless, it has patently been a beneficiary of war. Dillion and Reid note that the political transformation that the two World Wars enabled was far greater than that achieved by social and political reformers (2009, p.9). Liberal war theory suggests wars that promote freedom and peace are legitimate, despite international humanitarian law (IHL; an important part of liberalism's attempt to temper the inherent anarchy of the system) paradoxically requiring the opposite. Dillon and Reid add that this is just one type of war and that liberal states can war for geopolitical reasons too (2009, p.84).

2.3 IR Theory Shift

In the late 20th century, democratic peace theory seemed to win the debate, with war by developed Western states declared "subrationally unthinkable – rejected […] because it remains subconscious and never comes off as a coherent possibility" (Mueller in Dougherty and Pfaltzgraff 2000, p.3). Whilst this may have resulted in states limiting their use of force and drawn out wars, as liberalism has long sought, it has not tempered liberal states' use of violence. There have still been many battle-related deaths in interstate conflicts (**Figure 1**) and it has been said that "major war, not war in general […] is obsolete" (Mandelbaum 1998, p.20). This, as will be seen later, reflects the nature of cyberwar, which

[2] Total war refers to war that abides by no rules or norms. That is, civilians are an acceptable target, the same as a military target.

does not require the same scale of war to occur. Rather, highly targeted attacks can be effective without inflicting death to such a degree.

As war evolves, our understanding of IR will also need to evolve as they are grounded in a specific understanding of how states conduct themselves, in times of peace and war. If how states behave during war is fundamentally different then the calculus of these theories may prove incorrect and may no longer predict state relations.

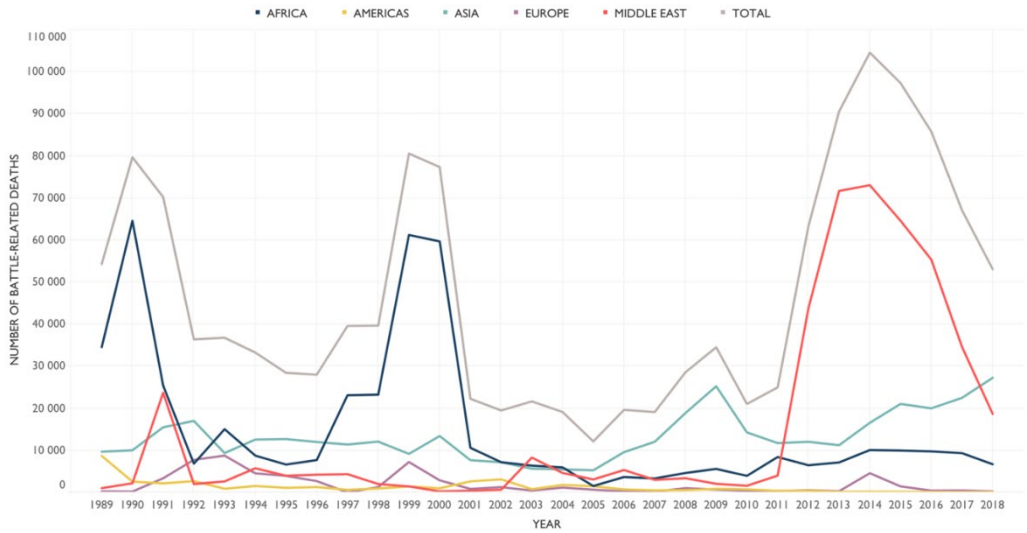

Figure 1: Interstate Battle-Related Deaths by Regions, 1989-2018 (UCDP 2020.a).

3. War

The etymology of war, *verwirren*, meaning 'to confuse, perplex', provides a helpful basis for understanding war. Sun Tzu's *The Art of War* (500 BCE) also noted that, "all warfare is based on deception," and, "in the midst of chaos, there is also opportunity." There is such diversity and nuance in what war is, that we must analyse it, so we are aware of the limitations of existing definitions (Most and Starr 1983, p.139). By analysing two core components of war, this section explores the existent conceptualisation of war and highlights some of the emerging changes. The first section will explore *why* war is conducted before proceeding to violence, or the *what* of war. Finally, by examining legitimacy, a greater understanding of *who* can conduct war, *when* they can conduct it, and *how* they can conduct it will be gained.

3.1 War as a Political Tool

To begin, it is important to understand why war exists, why would a state use such a catastrophic thing? Bruce Porter wrote that (emphasis original),

> *Wars are not mere intermissions in a human drama of relentless progress; their organisational residues are woven too deeply into the fabric of modern politics for that. But neither is war necessarily an engine of progress. It is instead a powerful catalyst of* ***change****, the direction of which is always morally problematic and often deleterious in effect.*
>
> (2002, p.9)

Porter is building on the concept introduced earlier, that the nature of a state is one of war, "states make war, but war also makes states." (p.14). This provides a useful segue to one of the most enduring definitions of war, from an 18th century Prussian General and military theorist, Carl von Clausewitz (2007 [1832]).

1. War is a natural, primal violence born of hatred;
2. War is instrumental, there must be a means (force) and an end (goal); and
3. War is political in nature, 'the mere continuation of politics by other means.' War is an act of policy.

War is a political tool available to governments to achieve political outcomes. This means that states have carried out a rational cost-benefit analysis and determined that violence is the best way for them to achieve their goals (e.g. territorial expansion). Though, it has been noted that often wars do not lead to the *desired* outcomes of the aggressor state (Sullivan 2007). Ultimately, war exists as the final defence or forceful implementation of diplomatic interests, as a last resort of conflict resolution or territorial expansion (Holsti 1996).

3.2 Violence

The Oxford English Dictionary defines violence as "the deliberate exercise of physical force against a person, property, etc." The physical force component underpins the idea of kinetic war, and up until the development of the internet, was the only possible form of warfare. Even psychological warfare has been reliant on the trauma of kinetic war, or dissemination of news and propaganda through pamphlets or newspapers (Doob 1949; Speier 1948, p.7). The inclusion of 'deliberate' introduces the concept of legitimacy, which will be addressed later.

In his exploration of the concept of violence, Benjamin Valentino has two key observations. Firstly, pre-1990s, political scientists' focus was not on violence per se but rather the causes of war; therefore, the conclusion drawn was that violence against civilians, in particular, was irrational and random. Subsequently however, the conclusion that violence is "primarily, if not exclusively, instrumental and coordinated by powerful actors seeking to achieve tangible political or military objectives," has been formed (2014, p.91). Violence plays a specific purpose and can be actively used to achieve certain outcomes.

Koloma Beck and Werron have created a model to understand violence in general (**Figure 2**). Their model shows the interaction between three entities when an act of violence occurs. The entities are the performer – who carries out the violence; the target – who suffers harm; and an observer – who sees the action. For this thesis, we can equate the performer and target as state(s) and the observer at the international community, and on a subnational level, civilians.

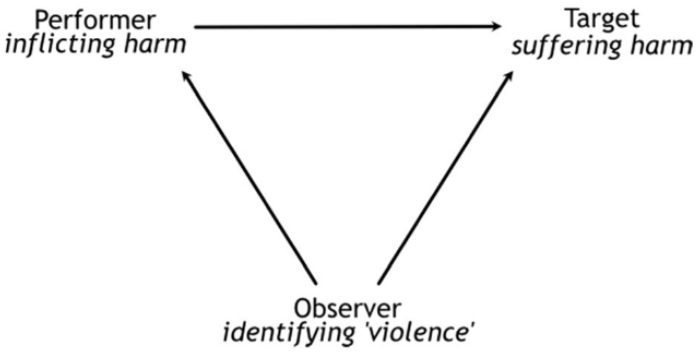

Figure 2: The triangular dynamics of violence (Koloma Beck and Werron 2018, p.281).

Intuitively, one might limit their analysis of violence as between two actors, the 'performer' and the 'target'. However, Koloma Beck and Werron argue this is insufficient because violence can be extremely contextual, especially across borders and over time. This model emphasises the existence of social aspects to acts of violence. "Violence is a matter of observation of, and discourse about physical action," they conclude (2018, p.280). This is illustrated by describing the Hobbesian monopoly of violence, with different formulations, "'military' or 'police operations,' 'humanitarian interventions,' 'arrests,' or 'preventive custody.'"

Violence in the context of war, traditionally occurs in a primary sense, that is, casualties as a direct result of a kinetic object (e.g. bullets, munitions dropped etc.). The International Institute for Strategic Studies (IISS) compiled a capability matrix for modern militaries about what attributes should be possessed by 'Global Military Powers' (see **Appendix A**; Giegerich, Childs and Hackett 2018). These are the tools available to powers who want to pursue war. Of the 11 criteria the IISS maps out, ten of them are kinetic capabilities, the 11th recognises the role of cyber. This matrix shows that there is a strong bias for militaries to acquire kinetic capabilities over cyber, focussing on the intrinsic physical and kinetic nature of violence.

Moreover, this is the yardstick that the Uppsala Conflict Data Program (UCDP) uses to define war; where a war is defined by the number of casualties, 'a state-based conflict or dyad which reaches at least 1,000 battle-related deaths in a specific calendar year' (UCDP 2020.b).[3] This definition means that unless there are substantial deaths, a specific violent event(s) will not be considered war. However, technology has meant that these definitions that rely on both primary kinetic events and specific levels of lethality which do not necessarily reflect the nature of violence in modern war and how new capabilities inflict their violence in an indirect fashion. For example, if electricity grids are crippled, no one may directly be harmed; however, people in hospitals reliant on electricity may die because of the attack. This is a major point of departure as a new theory of war is developed. Capabilities have altered how war can be conducted, which in turn, requires an improved understanding of the consequences of this.

[3] Where a conflict is, 'an armed conflict is a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in one calendar year.' And a dyad as, 'two actors, with one or more being the government, that have a stated incompatibility'. (Pettersson 2019, pp.4).

3.2.2 Reduction in Physical Violence

As technologies have advanced, some authors have put forward theories of nonlethal war, questioning the essentiality of violence to war. David Morehouse defines nonlethal weaponry as being able to incapacitate a "warring effort without causing significant injury, excessive destruction of personal property, or widespread environmental damage." (1996, p.12). Therefore, technologies available to states to conduct war potentially could reduce the lethality of war, corresponding with a dramatic reduction in violence. Technology has deemphasised the need for extreme violence as similar outcomes can be gained through less violent means. That is, extreme violence may not be a core means of war to achieve some political end as that same end can be obtained through non-lethal means.

3.2.3 Ideological Violence

One thing that is not addressed readily in the literature is whether state attacks on democratic apparatus (e.g. elections, parliament) constitute war. Attacks on ideology such as this have tended to be the domain of terrorism or coercion through violence by certain sub-state groups (Chaturvedi 2004). However, the internet has enabled foreign states to undermine the core principles of democracies through the interruption or manipulation of elections for example. These acts do not inflict physical harm or rely on the threat of violence on citizens; however, it can undermine trust in the capacity of the state to deliver critical services. As 'the West' has attacked autocracies throughout the 20th century, there has been a rise in autocracies subverting democracies through the use of modern technology, this amount not to physical violence but a form of destruction.

3.3 Legitimacy

Legitimacy is a fundamental concept in political science and there is a lot of literature that aims to understand legitimacy in different domains: electoral; state; violence; appropriations etc. Legitimacy can be defined as, "conformity to the law, to rules, or to some recognised principle; lawfulness. Also: conformity to sound reasoning; logicality; justifiability." This is important because as noted earlier, there are rules associated with war. The model of violence (**Figure 2** above) *de facto* introduces this through the observer. In relation to war, there are several 'legitimacies' that apply, *who* can use war, *when* can war be used, and *how* is war conducted. The following section will explore these three forms of legitimacy.

Regarding the *who*, Bruce Gilley outlines three dimensions of political legitimacy, (i) legality of the state; (ii) moral justification of the state; and (iii) consent enjoyed by the state (2012, p.693). Stemming from this legitimacy is the nation-state's right to the use their monopoly of violence. This is a Hobbesian/Weberian concept that posits that sovereign states possess the legitimate use of violence exclusively (Dillon and Reid 2009, p.83).

Regarding the *when*, the relevant body of literature is 'Just War Theory', which has its origins in roughly 400 ACE (St Augustine). It has since been revised several times, in the 1200s (St Aquinas), the 1500s (De Vitoria), and most recently and relevantly to Westphalian politics by Grotius in the 1600s (Silverstone 2011). Socrates claimed that in practice, states are not able to rule out war, because, "firstly every nation must be free to make war in self-defence, and secondly every nation must be free

to make war in defence of those whom it is bound in honour or by treaty to protect." (Jelf 1933, pp.104-105).

Acting outside of Socrates' framework would constitute an 'aggressive war.' Jelf tries to parse the line between aggressive and defensive, ultimately concluding that, "no general rule can be laid down; every-thing will depend upon the circumstances of the particular case" (1993, p.109). This conclusion is necessary because for these matters, context is essential. Modern world politics has determined that defensive wars are legitimate; however, initiating a war, for any purpose is illegitimate (UN Charter 1945). This acknowledges the importance of the precursors to war as being essential to our understanding of war. State A, defending themselves is justified in warring with its aggressor, State B. However, State B was unjustified in starting the war. Whilst this has produced *a war,* the justification of said war would require the observance and acknowledgement of which state acted violently first.[4]

This is a determination made by the observer from the model of violence (**Figure 2**). Currently, war can only be conducted legitimately through petition of the UN Security Council (UNSC) – the UNSC being the observer – who must agree that the petitioned war is legitimate. However, in opposition to decisions taken by the UNSC, wars have still gone ahead (Armstrong and Farrell 2005, p.3; Morris and Wheeler 2007, pp.214-215). This shows the fragile nature of legitimacy in relation to starting war. It is more idealistic than pragmatic.

Generally, the rules of war are more generally adhered to in terms of *how* war is conducted, who or what can be targeted and through what means. Most IHL is based on the 19th century Lieber Code, which introduced the concept of military necessity (Carnahan 1998; Akande and Hill-Cawthorne 2014). It provides conventions on when war can be used, and what are acceptable targets and acceptable means of warring (e.g. banning certain weapons that are likely to harm civilians). The rules apply to many different things, e.g. cultural items of indeterminable value. In terms of infrastructure, it should only be targeted if it can be shown that the military advantage outweighs the costs to civilians who might also be reliant on the infrastructure.

The concept of the *fog of war* is one used to downplay breaches of IHL. It is generally understood to be a state in which "even well-intentioned people have a hard time discerning what the right thing to do during wartimes is" (May 2013, p.327). However, May acknowledges that "during war, political leaders sometimes seem to make these decisions effortlessly" (p.327). Which again points to the strategic as opposed to morally justified use of violence in a state of war.

Military strategy is an important part of this. One of the major developments in strategy has been a shift to asymmetrical/guerrilla war, pioneered by Mao ZeDong in China. This was once seen as a strategy of large-scale war but has come to be a "political-military strategy in its own right," according to Münkler (2003, p.7). Some of the key components of asymmetric war are: (i) "less military focussed and more multidimensional"; (ii) a shift from territory to a human centric focus, borders don't matter as much; (iii) information as a burgeoning tool of power; (iv) war is now protracted; and (v) the dispersion of combatants amongst the citizenry, without traditional military targets (Manwaring 2012, pp.4-5). This strategy is one of eroding liberalism's attempts of delimiting civilians from military combatants and targets.

[4] Recently, the UN has adopted a third pillar of Responsibility to Protect, which is a form of legitimate war to prevent mass humanitarian crises. It is seen as a defensive war against the violence on civilians.

Overall, states have shown to not be very compliant with norms of legitimacy, Patricia Weitsman argues that states "seek legitimisation and international sanction for their actions," to enhance their standing, however, care little about the actual morals behind the use of violence (2014, p.3). This indicates that states are willing to put up a façade of adhering to legitimacy, when, in actuality, they are willing to use violence in any which way to achieve their goals. However, this wantonness opens the door to it being abused further, especially in terms to the *how* war is conducted, more so with modern military capabilities.

It has been noted that, "the majority of wartime violence against civilians [is] carried out by governments, [who are] more likely to possess the capabilities to kill in large numbers" (Valentino 2014, p.94). With this in mind and the fact that the nature of violence is changing, to be more in-direct and less aggressive, it is possible that governments opt to more readily target civilians, especially as there is a strong proven track record of flouting the rules of war. The development of military capabilities in the cyberspace have expanded militaries' ability to negatively impact civilians en masse due to their interconnectedness and reliance on modern technology.

3.4 Summary

At this point, it is helpful to summarise what conventional war is into a simple causal equation.

$$X \rightarrow Z_p \rightarrow P$$

Equation 1: Causal chain for conventional war

Where *X* is an act of violence (legitimate or illegitimate), Z_p is the damage inflicted to legitimate or illegitimate targets, as a direct result of *X,* and *P* is a political outcome (desired or undesired). For example, *X* is the launching of a missile. And Z_p is the physical damage caused by the missile (e.g. infrastructure, human, psychological). This is a helpful summary as a causal chain can be mapped from the act(s) of violence to the political outcomes. Where the size of Z_p is important in determining/indicating *P.* Z_p is determined by the number and severity of acts of violence but also the legitimacy.

4. Cyberspace

In 2015, Jovana Davidovic noted that technological developments changed the nature of war. The paradigms in which Just War Theory and other definitions of war were developed are no longer in sync with the realities of war today. Notably, Davidovic says the "temporal and spatial scope of war," have contributed most to this change (2015, p.603). This has a direct impact on legitimacy and the scale of violence that can be inflicted. Technology has also uniquely shifted violence from a primary occurrence to a secondary effect. This technology is cyberspace, it is a unique advancement because it is both its own, separate domain, but also can be used to dramatically enhance the other domains of war (naval, land, air, and space).

Defense University provides a rich definition of cyberspace, "a global domain within the information environment,[5] whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communications technologies" (2009, p.28). This definition raises two important aspects of cyberspace, information, and networks. Information that exists on an isolated device would not be in cyberspace as it has no ability to be moved around except through some physical manipulation. However, this can be manually breached to spread an attack (even through an unknowing agent).

The UK Ministry of Defence and the US Department of Defence's definitions are very similar and highlight that cyberspace is: complex and dynamic; interdependent with the electromagnetic spectrum; global and influential to all military functions on land, sea, air, and space; based on the internet, telecommunications networks, computer systems, and embedded processors and controllers (Theohary 2020, p.1; UK Ministry of Defence 2018, p.4). However, the US Joint Doctrine for Information Operations introduces three critical domains, "the physical, informational, and cognitive" that enhance this understanding of cyberspace (US Office of CJCS 2012, p.I-1). In combination these three designs are the pillars of cyberspace (**Figure 3**).

The physical represents: wires, computers, phones, the devices, components, and humans that enable the computation and storage of information. The informational dimension is the "content and code […] produced and curated." The cognitive dimension relates more to the human input, being "thought, reason, and decision-making" (Crowell 2017, p.4; Libicki 2009, p.12). This three-dimensional approach to cyberspace is common throughout the literature and shall be used going forward.

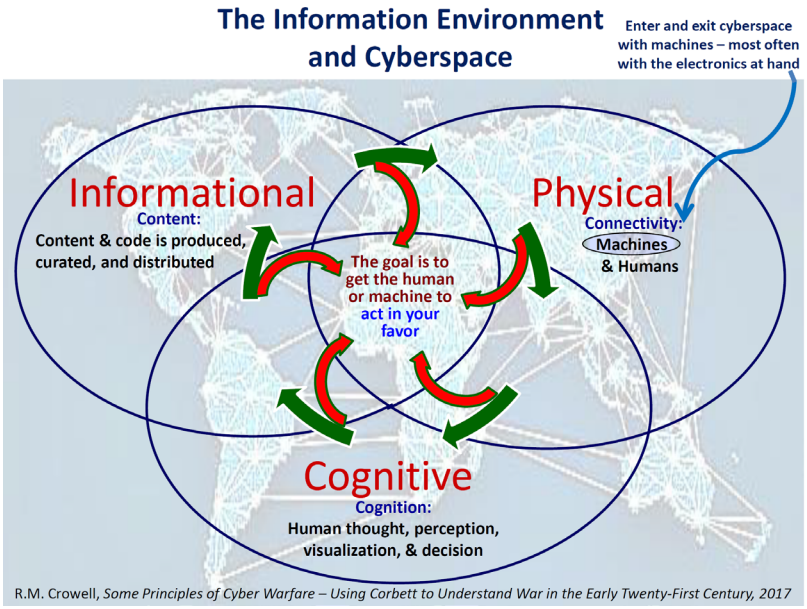

Figure 3: The information environment and cyberspace (Crowell 2017, p.4).

[5] In the context of this thesis, the definition of information environment comes from the US Department of Defence: the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information," with the Joint doctrine further adding, "there is an electromagnetic spectrum portion of the information environment." (in Porche *et al.* 2013, p.11).

5. Cyberattacks

Whilst there exists a consensus as to what cyberspace is, there is little agreement or clear definition on what a cyberattack is. In its most simplistic form, a cyberattack is the exploitation of a vulnerability in cyberspace. There are three critical components of a cyberattack that are relevant for this thesis with respect to warfare. The *means*, the *intent*, and the *impact.* A specific type of means could have different impacts, sometimes regardless of intent. It has been noted that the impact and intent of a cyberattack are more important than the means themselves (McGavran 2009, p.261).

The US Joint Chiefs, after establishing the US Cyber Command, issued a definition of a cyberattack that does not provide much detail about the means and instead focusses on intention and impact.

> *A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. […] not necessarily limited to the targeted computer systems or data themselves. [… it] may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyberattack may be widely separated temporally and geographically from the delivery.*
>
> (Hathaway *et al.* 2012, p.824)

Additionally, before delving into means, intent, and impact, the UK's National Cyber Security Centre also makes an important distinction between targeted and untargeted attacks. Whereby an attacker either designs and instigates an attack precisely or indiscriminately (NCSC 2016). Untargeted cyberattacks tend to be more used by cybercriminals, aiming to cast a wide net to get as much money as possible and tend not to be conducted by states; however, this is just a pattern not a rule. More relevant are targeted attacks. This is because if it is targeted there is more of an idea of what the impact is. It is also easier to link the intent behind the attack, as targeted attacks need to be better resourced in order to effectively carry out the attack (Cavaiola, Gompert, and Libicki 2015).

5.1 The Means – How Cyberattacks are Conducted

There are several ways to conduct a cyberattack. The purpose of this thesis is not to explain these in technical detail, however, an introductory knowledge of what these attacks are, is important. A summary of some of the most used types of attacks can be found in **Appendix B**.

An extremely helpful definition for cyberattacks was formulated by Lin, which is based on three factors, (1) Access,[6] (2) vulnerability,[7] and (3) payload[8] (Lin 2012, pp.517-518). This trinity of factors in combination make up the means, "the use of deliberate activities [...]," which leads to the outcome, "[…] to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks" (pp.518-519).

[6] Remote access (e.g. over the internet), physical (e.g. undercover agent or manipulated hardware).
[7] Design or implementation flaw exploited, or an introduced flaw (see access), or a bug ("unintentionally introduced defect").
[8] The exploit itself, e.g. a virus that is programmed to alter files or steal information etc.

It is critical to stress the importance of vulnerabilities in cyberattacks. Vulnerabilities are the weaknesses in hardware, software, physical connections, or human operators that allow for cyberattacks to be conducted. Often, human operators are the weakest link; however, there are many known cases of exploiting software and hardware that has not been patched that has enabled cyberattacks to occur (Oakley 2019 pp.25-39). Differing degrees of complexity and possible damage inflicted depend on which vulnerabilities are being exploited and the available resources of the state behind the attack (**Appendix B**).

5.2 The Intent – Why is the Attack Conducted?

In this thesis, intent can be linked back to Clausewitz's definition of war and is summarised well by Hathaway *et al.* They explicitly identify two intentions behind attacks, "political or national security" (2012, p.826). They go on to also distinguish between cyberattacks and cyber-espionage or cyber-exploitation, as the latter two do not undermine the functionality of the network or computer and instead focus on the extraction of information (Hathaway *et al.* 2012, p.829). The key take-away from their definition is that cyberattacks are political in their intent to target national security apparatus.

5.3 The Impact – What Was the Effect of the Cyberattack?

An important dichotomy exists within the domain of impact of a cyberattack, whether it is 'contained' or 'spread'. Well-developed and resourced cyberattacks can be contained and have a limited reach. This may mean that the attack is present on non-targeted devices and networks; however, it only activates when specific configurations are detected (Sood and Enbody 2012). Others can be spread, meaning that there is an effect on every infected device, this could be roughly equated to a total war scenario, this could also be by design too.

Cyberattacks can have two broad effects on data and information or on physical things that are connected. Data and information often underpin how humans and machines behave. Therefore, manipulating data can result in suboptimal actions as a result. In terms of physical things, manipulated data can cause machines to operate outside of specification and can result in permanent damage (see **Case study 1**). Cyberattack impacts are different than that of conventional kinetic attacks because the initial attack does not often produce the direct result. Rather, it cascades into an event that then induces some effect. Cyberattacks are unique too in that they can be rendered completely useless if vulnerabilities in devices or networks are patched, meaning the attack is useless before it has even launched.

5.3.1 Disinformation cyberattacks

Whilst all cyberattacks are related to information, an important modern development is the ability to directly target civilians through legitimate mediums. Some states have actively used social media platforms to provide disinformation and polarise other states' citizens. This has most notably been conducted by China and Russia (Bennett and Livingston 2018, p.132). This is not a new phenomenon; it has been readily deployed by militaries in the past and is commonly known as psychological / information war (PSYOPS).

What is novel about the modern usage is that it is now easier than ever to disseminate disinformation to people around the world. Over half the world is online and the internet enables this to be easily

conducted during peacetime too. The two prominent and most researched examples of this occurred during the 2016 US Presidential election and Brexit vote (Bennett and Livingston 2018; Faris *et al.* 2017). The justification for the inclusion of PSYOPS as a cyberattack lies in our definition of cyberspace. Critical to it, is both the physical layer, which includes humans, and the cognitive layer, which is the human interaction with ICTs. If humans are reliant on information that is provided by ICTs it is vital that it is true and accurate for Today, human decision making relies on data provided by and stored on digital systems and networks, if these data or systems are compromised, human analysts and operators are likely to make poor decisions.

It is also possible for an attack on non-civilians to use disinformation in order to fool the adversary that all is normal when in fact another (perhaps conventional) attack is occurring. Israel successfully fooled Syrian air defences that their airspace was clear when in fact, Israeli planes were actively destroying a suspected nuclear warhead facility (Geers 2010).

6. Threat-scape

This section looks at different targets of cyberattacks. Tarah Wheeler said, "the nature of cyberwarfare is that it is asymmetric. Single combatants can find and exploit small holes in the massive defences of countries and country-sized companies" (2018, p.36). Hence, the broad nature of targets. The interconnectedness of state apparatus now means that the state is vulnerable on a scale not before comprehensible. Both democratic and autocratic states possess cyber risks. Arguably, there are larger cyber risks in democracies which have greater unfettered access to the internet, whereas autocracies often provide stringent control and censorship of ICTs (Christensen 2019). The following are potential targets of cyberattacks that would pose the biggest threat to states.

6.1 Military Targets

Naturally, military targets are extremely valuable, as disabling these would provide extreme strategic advantage(s) in the event of full-scale kinetic war. Militaries have incorporated more portable and powerful cyber technologies into more facets of a soldier's working life. From personal equipment to advanced weapons systems (nuclear, command and control, UAVs, and missiles etc.), militaries use vast amounts of connected technologies (Nygren 2002; Walrath 2005). The more that militaries utilise these technologies, the greater the risk there is that they can be compromised in a cyberattack (disabled systems, espionage, and other intelligence). If any of the targets listed in **Table 1** below were to be compromised by a cyberattack there could be significant ramifications for a state's military.

Weapons Systems	C4ISR*	Personal Equipment	Organisational
– Nuclear weapons	– Command and control	– Health tracking devices	– Payroll
– Missile launches	– Communication systems	– Augmented reality devices	– Healthcare
– UAVs	– Intelligence	– Mobile phones	– Logistics
– Air, Land, Naval Vehicles	– GPS		– Policy
	– Secure data transmission		– Legal
			– Research
			– PR

Table 1: Types of military systems that could be potential cyber targets. *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

The ability to disable important weapons systems such as nuclear weapons could have important implications for traditional theories of war and security, such as nuclear deterrence. If a state is unaware they have been cyberattacked, a hypothetical attacking state (A) now knows that its adversary (B) no longer possess the ability to use their nuclear warheads. If this is the case, A may choose to escalate violence as they are no longer deterred by nuclear retaliation (Unal and Lewis 2018).

6.2 Collective Defence Agreements

In 2014, NATO affirmed that a cyberattack could trigger collective defence obligations under the treaty (Daugirdas and Mortenson 2015, p.211). Consequently, if a NATO member experiences a significant cyberattack, other treaty members would be compelled to respond to the aggressor. This decision has significant implications for NATO members and if adopted by other collective security organisations, such as the UN, there would be even further reaching consequences.

Whilst not a collective defence organisation per se, the EU, in 2017, acknowledged that malicious cyberattacks could warrant a response from member states (Ivan 2019, pp.4-5). The EU Diplomatic toolbox does not explicitly sanction conventional war responses but does leave the door open for member states to respond within the full range of their legal rights under international law. Whilst there are not then obligations for EU-27 members to also aid a targeted state in a conflict (like with NATO), they are; however, obliged to provide support using other means (diplomatically or economically).

6.3 Critical and Co-Dependent Infrastructure

Critical infrastructure has been best defined by the EU as "an asset, system or part thereof […] which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have significant impact in a […] state as a result of the failure to maintain those functions." (EU Council 2008).[9] Bronk and Tikk-Ringas highlight that critical infrastructure is often privately owned but requires government intervention for its protection (2013, p.91). This creates a unique political situation – whereby something that is vital to the functioning of society is no longer the primary responsibility of a government. Naturally, this will have complications for cyberattacks and potential political outcomes.

Jacques Shore describes the difficulties of this relationship in the context of Canada, "responsibility for cyber security is shared between the owners and operators of critical infrastructure and the federal, provincial, and territorial governments." (2015, p.241). The first issue is the shared responsibility, governments have a duty to protect their citizens but corporations who own these services have a responsibility to protect them from cyberattacks too. Continuing, Shore says that, "decentralisation can lead to confusion regarding the respective responsibilities of the various agencies." (2015, p.41). This can add to the potential risk as there exists the possibility for unclear accountability and obligations.

Similarly, co-dependent infrastructure focuses on infrastructure that if disrupted would have implications for multiple states, due to the interconnected reliance that states have on international

[9] Examples include: electricity generation, water treatment, air traffic control, traffic management systems, and dams.

trade and in some cases shared assets or flow on effects. "The global economy and trade relations between countries rely on electronic communications that facilitate ties, commercial transactions and transmission of information and knowledge around the world," these ties could cause significant harm, especially for example, the reliance of energy sources (fossil fuels) from overseas (Menashri and Baram 2015, p.81). To provide an additional example around energy and resources, if a hydroelectric dam in an upstream country was compromised, that could have significant impacts on a downstream state(s) in terms of both water flows and electricity needs.

6.4 The Economy / Financial Institutions

Whilst exceptionally broad, it is important to combine these two domains as financial institutions are the backbone to the economy, without which money would not be able to circulate. The European Parliamentary Research Service reported that cyberattacks could have a large economic impact, estimating the cost of all cyberattack related activities had a total economic impact of €530 billion globally (2019, p.1).

More than this, financial institutions themselves: tax agencies; central- business- and retail-banks; payment platforms (e.g. credit cards, PayPal, Klarna); international payment settlement houses; and share markets, are potential targets (Kopp, Kaffenberger and Wilson 2017). There are significant impacts if these institutions fail. For example, the ramifications for governments if tax agencies are no longer able to collect taxes could possibly prevent the functioning of public services. If banks can no longer grant access to money it means individuals and businesses cannot function. Similarly, if central-banks close, business- and retail-banks close. If financial markets crash, retirees could be left without a pension, similarly investors all around the world could be stranded. An example of the damage that can be inflicted by targeting the economy and financial institutions is explored in greater depth in **Case Study 3**.

6.5 Democratic and Electoral Targets

Whilst the preceding targets are generally applicable to all government regimes, the following disproportionately affect democracies. Many democracies have published warnings about their vulnerabilities to cyberthreats, highlighting the international consensus that adversaries can exploit different parts of society or institutions.[10] Moreover, cyberattacks specifically open up the possibility of war, as these fundamental institutions can be undermined without physical destruction.

6.5.1 Elections

Elections are at the core of modern democratic societies; they are the gateway to peaceful transitions of power and are the expression of the people's will on how they wish to be governed. They are one of the most fundamental democratic functions. The EU Parliamentary Research Service noted this

[10] See: Canada - https://www.canada.ca/en/democratic-institutions/services/protecting-democracy.html; UK - https://www.ncsc.gov.uk/news/ncsc-defends-nation-against-more-than-600-cyberattacks; Australia - https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security; Sweden - https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213; EU - https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

threat, "risks from the digital realm can destabilise governments and political systems, sow societal divisions and increase the risk of internal and external conflict." (2019, p.1). After the 2016 US Presidential election and UK referendum on EU membership, there has been a heightened concern about the use of cyberattacks in electoral events.

6.5.1.1 Disinformation

Thomas Jefferson wrote that democracies should have a well-informed electorate. In this digital era where almost all human knowledge exists on the internet, it could be assumed that there would not be substantial hurdles to this goal. However, the nature of the internet has enabled the manipulation of information.

One of the issues is that disinformation is spread via legitimate means, mainly through social media companies (e.g. Twitter and Facebook; Lazer *et al.* 2018). Moreover, using the advertising tools that these companies provide allows disinformation to be targeted at specific groups of people that can lead to socio-political polarisation (Lukito 2019). "The aim is to cause and feed instability, to weaken the social fabric within a society and to complicate and undermine decision-making" (Hansen 2017, p.10). This could lead to citizens making their decisions on wrong or misleading information. It is especially damaging for liberal democracies that are by nature balancing the freedoms of individuals, the will of the majority, and minority rights.

6.5.1.2 Illegal Disclosure of Information

The other informational attack possible on elections is the disclosure of illegally obtained (hacked) information. In the 2016 US Presidential election, this occurred with the Democratic National Committee's emails being released on WikiLeaks after Russian hacking (Rid 2016). Rid, in an article for VICE News, was clear (emphasis original),

> *"This tactic and its remarkable success is a game-changer: **exfiltrating** documents from political organisations is a legitimate form of intelligence work. The US and European countries do it as well. But digitally exfiltrating **and then publishing** possibly manipulated documents disguised as freewheeling hacktivism is crossing a big red line and setting a dangerous precedent: an authoritarian country directly yet covertly trying to sabotage an American election"*

Whilst there are of course democratic arguments to be made for transparency and openness, the central factor of this story is that a foreign state was actively interfering in a democratic election. If foreign actors steal and then selectively leak information this could have an influence on how voters make their determinations.

6.5.1.3 Voting Machines

In some countries, votes are counted on electronic vote counting machines. In theory, these machines accurately record citizens' votes and provide an instant digital tally at the conclusion of the polling period. However, because it is digital, it can be hacked, especially those that are connected to the internet (Rid and Buchanan 2018, p.11). Rid and Buchanan quote Joseph Stalin to highlight the issue, "I consider it completely unimportant who in the party will vote, or how; but what is extraordinarily important is this – who will count the votes and how." (p.11). It has been found that voting machines used in the US can be exploited in numerous ways to "manipulate vote-counting functions." (p.11).

If a foreign state manipulated voting machines, this could have large implications for democracies. Whilst the solution is simple, revert to pen and paper, for nation-states where there is widespread use of electronic and internet-enabled voting machines there is a clear and well-known vulnerability.

6.5.2 Parliamentary Operations

Whilst under researched, there have been a few examples of cyberattacks against parliaments. Notably in the UK and Australia. In 2019, Australia alleged that China disrupted the running of the parliamentary network and the networks of the two major political parties. The attack was serious enough for the Australian Signals Directorate (ASD),[11] to declare it a 'C1 – National Cyber Crisis', the first of its kind in Australian history (ASD 2019, p.23).

There is not any specific literature that addresses the consequences of cyberattacks on parliaments. However, the fact that these attacks have been occurring is illustrative of the fact that it is possible for these institutions to be taken offline by a hostile actor and that they are a worthwhile target. The attack on Australia's parliament and political parties is illustrative that, should cyberattacks be levelled against these institutions, there could be significant consequences for the capacity of legislative institutions to complete their work.

6.6 Summary of Targets

Cyberspace has an unprecedented reach, it has altered the targetability of traditional targets of war but has also meant that there are new targets too. Moreover, physical proximity is no longer a relevant factor in damaging these targets. In sum, many important military assets are targetable which could alter the calculus of warfare by disabling important components of a state's defence force. Additionally, international agreements may oblige third-party states to become involved in a conflict, should a cyberattack reach an established threshold.

Diverging from more traditional targets, critical and co-dependent infrastructures are important building blocks of society, providing water, electricity, healthcare etc., ensuring standards of living and wellbeing. Targeting these infrastructure could have extremely negative impacts on states or regions.

Even more broadly, and novel to being targets of warfare, the interconnected nature of financial institutions, states' domestic economies and the global economy means that a cyberattack on major corporations or institutions would have profound international impacts. Moreover, democratic participation can be readily undermined by foreign interference through cyberattacks. In the case of voting machines, this could result in a situation where election results cannot be trusted. However, broad based misinformation campaigns can also sow discord and distrust amongst the populace. Finally, targeting government institutions themselves could disable governments from properly functioning.

7. Cyberwar

Cyberwar is a contested topic in political science literature. With some arguing it is overhyped (see Libicki 2009 and Rid 2013.a) and others arguing that it should be taken more seriously (Stone 2013). As a first point of demarcation, existing literature has begun to break down cyberwar into two distinct phenomena, *operational* and *strategic* cyberwar. An operational cyberwar is the use of cyberattacks

[11] ASD is a SIGINT agency within the Depart of Defence.

in the context of a kinetic war, i.e. an extension of existing military operations. Whereas, *strategic* cyberwar is war conducted solely in cyberspace with no other domains of the military included (i.e. land, marine, air) (Libicki 2009, p.8).

Each of these has specific implications for the violence and legitimacy dynamic. Operational cyberwar could potentially multiply the violence component, enhancing the effectiveness of kinetic capabilities (Libicki 2009, p.139). In terms of legitimacy, the same set of considerations would apply as to the use of kinetic weapons. For example, utilising a cyberattack against a combatant would not be considered an escalation of physical war, but rather another element in the theatre of war (pp.139-140). In his work, John Sheldon implies that cyberwar is of the operational nature. Stating that, "cyberpower is complementary," and "cyberpower is ubiquitous" (2011, p.99) He explains that cyberpower "generates strategic effect in all domains so absolutely and simultaneously" (p.99). To the extent that cyber is linked to the enhancement of the traditional domains of war, this is true.

In terms of *strategic* cyberwar, Libicki states that if a series of cyberattacks (as the only tool of war) are used to change a state's behaviour then it becomes a strategic cyberwar (2009, p.117). Libicki rightly argues that cyberwar in the absence of kinetic aid cannot occupy territory. However, potentially more open to debate is his dismissiveness of its ability to change a state's government. As cyberwar can focus purely on information, it is possible that attacking democratic processes and institutions could result in the change of a government (Rid and Buchanan 2018).

7.1 Cyberwar and IR Theory

The realist and liberalist paradigms emphasise the need for certainty and clarity of communication. However, cyberattacks suffer from an attribution problem which goes to the core of strategic cyberwar (Libicki 2009). The nature of the internet allows for anonymity when attacking, the origin of the attack is able to be digitally masked or purposely positioned in another place (Oakley 2019).

Deterrence theory requires clarity of information, however, if a cyberattacker cannot be identified, there could be issues with whether or not deterrence could effectively take place. For example, if the attacker cannot be properly identified, the targeted state may not know which behaviours to change. It is possible there are several aggressors, each seeking different political outcomes, meaning that identification is important so that a state could pursue the 'correct' course of action. This issue can somewhat be eliminated the longer a cyberwar continues as other signals would make apparent the actors (Libicki 2009, p.133; Oakley 2019).

Attribution is also not always publicly declared so that capabilities and vulnerabilities are not publicly known. It is in no state's interest to reveal vulnerabilities until they are patched. Moreover, as cyberwar is more likely to be operational rather than strategic, i.e. coupled with kinetic war, publicly attributing attacks could result in the use of kinetic warfare against a state, which would be detrimental.

Libicki's detailed exploration of deterrence in cyberwar can be boiled down into the issues of conventional deterrence; clear communication of the red line, capacity to carry out a threat, and follow through (2009). These issues can be complicated because states are secretive about their cyber-capabilities and reluctant to admit being targeted. The security dilemma is a difficult theory to apply in cyberwar because it is unclear the capabilities that a state possesses. Importantly, cyberattacks are

only possible due to vulnerabilities that can often be patched, so it would be strategically foolish for a state to publicise their capabilities because this would flag to potential targets areas in which they are vulnerable.

Additionally, David Benson is developing a new balance of power theory, modernising the strategy of handicapping. In this, the connected nature of cyberspace allows for aggressor states to disarm an adversary's military capabilities (Benson forthcoming 2020). This would change the nature of external balancing, with states not necessarily needing to bandwagon or balance (form strategic alliances with either a potential aggressor state or form a coalition with other weaker states respectively). Rather the calculus would be conducted on newly manipulated military capabilities. For example, if a state could successfully prevent another from using their aircraft capabilities, that would alter the calculus of an aggressor state escalating their acts of violence (Benson forthcoming 2020).

In terms of liberalism and the legitimacy of cyberattacks, the main issue is the prolific use of cyberspace by non-combatants. Whilst well-designed cyberattacks can limit their impact to only targeted devices or networks, (**Case Study 1**). It is also possible that, either carelessly or intentionally, attacks can spread throughout the interconnected digital world and affect millions of citizens (**Case Study 3**; Sanger 2018; Greenberg 2018). Moreover, recalling the threat-scape for cyberattacks, the scope has clearly expanded beyond purely military targets and there are now present dangers in civilian infrastructure and institutions. Together, both the broadened scope of targets and potential inability to control the spread of a cyberattack, raises issues of legitimacy. Given evidence of uncontained cyberattacks, there is a need to reassess how the current understanding of war deals with issues of legitimacy, in terms of cyberwar.

7.2 A Causal Chain of Cyberwar

Many of the coercive effects of cyberwar would be secondary in nature. Meaning that the cyberattacks themselves do not directly cause the political outcome desired, rather they induce a secondary event that leads to the desired political outcome. This can be expressed into the equation that was introduced in relation to conventional war:

$$X \rightarrow Y \rightarrow Z_S \rightarrow P$$

Equation 2: A causal chain of cyberwar

Where *Y* is directly caused by the cyberattack (*X*) and that results in Z_s (outcomes in a secondary sense). *P* would then be based on the size of Z_s. The reason this is significant is because cyberwar is able to challenge the existing norms of war. Firstly, there is a drastic reduction in direct violence – violence through cyberwar is primarily going to result in property damage, rather than human fatalities or casualties, which are more likely to be secondary but would depend on what exactly was being targeted. Secondly, intwined throughout is legitimacy and who is affected by the attacks. Moreover, Z_S can now be a broader selection of targets. For a hypothetical example, State A launches a cyberwar against State B (*X*), causing the electricity grid to fail (*Y*) and as a result people are injured or die (Z_s), this in turn causes State B to alter their policies.

If it is the case that cyberwar can produce political outcomes, where diplomatic or economic means have failed, then our current understanding of war is missing critical acts of violence taking place in

cyberspace. Whilst these attacks do not necessarily have human casualties directly, the ability for the attacks to wreak havoc outside of the military realm certainly can.

8. Methodology

This thesis will utilise a qualitative method approach to answer the research problems proposed earlier. A qualitative approach here is motivated by two main reasons. Firstly, that there is an inability to source any comprehensive quantitative data on the topic and secondly, that a deeper exploration of diverse data will enable a richer analysis with a focus on 'how' and 'why' (Yin 2009, p.11). This paper will utilise a heuristic comparative case study method to develop a 'soft line' theory.

In his exploration of case study methodology, Eckstein argues that case studies are an important tool to use when developing theory, especially in relation to macropolitical phenomena, of which war is a part (2000, pp.119-120). The use of case studies is important as it can help uncover causal mechanisms and provide detail as to how a theory works, grounded in reality. In their exploration of case studies, George and Bennett note that case studies offer the ability to provide "contextualised comparison," thus enabling a researcher to better understand why a phenomenon exists (2007, p.19).

This study design will help illustrate the limitations of the conventional understanding of war in the modern context and build a foundation for future research to further develop the issues raised. This requires the case study to show the limitation in the existing definition of war and demonstrate how changing the definition might provide an improved understanding of war. This has practical uses for policy makers and researchers. As has been explored throughout this paper, the nature of war is changing.

The methodology builds on the principles outlined by Eckstein in relation to what he terms 'soft line' theory, or the breakdown of complex systems into more comprehendible components (2002, p.125). Eckstein says that for such a theory to be 'good' it needs to "state a presumed regularity in observations […], permits the deduction of some unknowns, and is parsimonious enough to prevent the deduction of so many that virtually any occurrence can be held to bear it out." (p.126). Moreover, the type of design used here fits into his fourth description of a case study in theory building, that it can shed light on the "plausibility, hence whether proceeding to the final, generally most costly, stage of theory building [theory testing] is worthwhile." (p.129).

The use of a comparative case study is justified for several reasons. Firstly, in terms of war, there is no ability for the researcher in the field to manipulate variables experimentally (Yin 2018, p.13) and also, the diffuse nature of evidence available, rarely available through official sources (due to the nature of national security among other factors). The lack of data is a further justification for utilising Eckstein's approach as there is an insufficient amount of data to thoroughly test theory with any reliability or validity.

By employing Eckstein's heuristic approach of 'building blocks' this study will create different elements of a 'soft line' theory, that will resemble a theory after looking at the three cases. The heuristic approach allows for the "imagination" of the theorist and a recommendation to use a rich array of data, and a more thorough investigation of variables which might yield serendipitous relationships, those that may not be clear from the outset but emerge from a deeper look (Eckstein 2002, pp.137-

138). Therefore, the expected results of this study are not a fully formed new theory of war, but rather the foundations of what a new theory of war can be built on.

To achieve this research goal, the analysis must highlight how the existing understanding of war as explored in depth earlier fails to capture the reality of how states are behaving now. It must then illustrate how a potential new understanding would better enhance both political scientists' and policy practitioners' ability to conduct research and act.

George and Bennett note that when conducting comparative case studies, it is important for the class of case being analysed to be clearly stated, this ensures that a structured comparison can occur and that the same phenomenon is being examined rather than similar but adjacent cases (2007, Ch.3). The cases used in this research all belong to the same class of cyberattacks conducted by foreign states, that originally targeted another foreign state.

Moreover, George and Bennett specify two other requirements for a comparative case study, that they be structured and focussed (2007, Ch.3). For structure, the researcher should ask standardised questions of each case that reflect the research objectives. In terms of focus, the analysis of the case must maintain a focus on the relevant theoretical world. Therefore, this thesis will ensure that the cases used here are analysed within the framework of war, specifically in relation to the two major facets of war discussed earlier, violence and legitimacy. Additionally, the focus will incorporate the expansion of possible targets which closely interrelates with violence and legitimacy.

Equifinality is an issue that political scientists must struggle with when developing theory. It is a problem about how similar outcomes have disparate causal mechanisms (George and Bennett 2007, Ch.8). Despite no two wars being the same, any number of different variables interact in any number of combinations; wars typically come to an end either through peace treaty or elimination of the adversary (De Franco, Engberg-Pedersen and Mennecke 2019). Within the boundaries of this thesis, it will be difficult to fully address concerns of equifinality due to the lack of data available; however, some researchers have addressed equifinality within conventional war and further research on cyberwar could use their work as a foundation (see Stanley and Sawyer 2009). Moreover, there has never been a full-scale strategic cyberwar that could illuminate and offer insights into how such a war would end.

8.1 Case Selection

To achieve these goals, the selection of cases is important. Three case studies have been selected primarily because they each represent typical cyberattacks committed by foreign states. However, each case also provides a unique factor when comparing cyberwar to conventional war. The cyberattacks are: (i) Stuxnet; (ii) Russian Disinformation in the US; and (iii) NotPetya.

Stuxnet, conducted by the US and Israel on Iranian nuclear facilities, is a clear representation of utilising cyberattacks in a means highly reflective of conventional war, where a military would have used airpower to disable the nuclear facility. It is the first attack that was launched digitally and caused physical damage.

Russian election interference in the 2016 US General Election illustrates a modern non-violent form of cyberattacks, in which a state's entire system of government can be undermined without lethality.

This type of attack is unprecedented because a foreign state is able to manipulate the free flow of information within another state and cause distrust in politicians, democratic institutions and among members of society. This attack is increasingly common with Russia targeting the Brexit referendum and other European states' elections. Moreover, China has been known to use similar tactics in Taiwan (Wang *et al.* 2020).

Finally, the Russian NotPetya attack against Ukraine, which quickly propagated around the world. This case shows the extreme end of cyberattacks, a more total war situation, where adhering to the rules is no longer a feature of the conflict. NotPetya's spread wreaked global economic havoc, temporarily grounding 20% of global shipping and had other large flow on effects.

As noted earlier, these cases are not of full-scale strategic war. Whilst utilising such cases would be of immense academic benefit, especially for the aims of this thesis, one has simply not occurred, or at least one that the public is aware of. These cases, although centred around individual attacks are illustrative of the breadth and extent that cyberattacks can be utilised. They provide a critical insight into sorts of attacks that could be expected to occur as part of a full-scale strategic cyberwar.

8.2 Data

The case studies will rely primarily on secondary materials: research conducted by academics, journalists, and cybersecurity experts. However, where possible official statements from state officials and governmental reports will be used. This is because within this area there is little official data publicly available. For example, from the aggressor state's perspective, they do not want to necessarily admit they have attacked another state for fear of retaliation or highlighting their capabilities. For a targeted state, they may not want to declare that they have specific vulnerabilities which they have not yet rectified.

Steps have been taken to collect data from a wide variety of perspectives to ensure that there is a triangulation of knowledge. This will enable conclusions to be drawn from disparate starting points as lines of focus converge. Utilising multiple sources of evidence is encouraged by Yin, arguing that it can result in a more critical analysis and that conclusions from the study are "more convincing and accurate" (2018). The limited available data also shaped the type of case study to be concept building rather than theory defining. At this time, the available data is not perceived as strong enough to draw definitive conclusions. It is rich enough, however, to illustrate the need for further rigorous academic research and in this case provide a foundation and framework for an evolution of our current theory of war.

8.3 Structured Focus

For the study to have a structure to enable comparison, the different cases will all be used to answer the following:

- What is the nature of violence in this case?
- Was the attack legitimate?[12]
- What was targeted?
- What were the political outcomes?

These questions relate to the conceptual differences that have been developed throughout the thesis. Moreover, through answering these questions the theoretical building blocks will emerge, thus fulfilling the aim of this thesis. After exploring each case a comparison will be undertaken of the three cases to find commonalities and differences and further build a theoretical foundation. Moreover, the causal chains that have been developed earlier will be utilised to explore the contrasting explanations.

9. Case Studies

9.1 Case 1 – Stuxnet

For years, Iran has been developing nuclear capabilities, with the US and Israel particularly worried about their ability to make nuclear weapons. It has been speculated that the US and Israel would eventually conduct a military strike to prevent Iran from weaponising (Sebenius and Singh 2013, p.52). Despite, Iran's assurance, the UNSC and International Atomic Energy Agency were not convinced that the programme was entirely peaceful and was, therefore, inconsistent with their ratification of the Nuclear Non-Proliferation Treaty (Bowen and Brewer 2011, p.923). The US President Bush, who did not want to conduct an airstrike on Iran and cause another regional war, insisted on an alternative method to cripple the state's nuclear programme (Sanger 2018).

The alternative was Stuxnet, a piece of malware (see **Appendix B**) that targeted the Iranian nuclear programme, specifically their centrifuges at the Natanz Nuclear Facility (Farwell and Rohozinski 2011, pp.23,28; Sanger 2018). The malware eventually spread to thousands of computers around the world. However, was designed to only activate when it met a network that fulfilled certain requirements, matching the design of Iranian nuclear centrifuges. The malware was delivered to the air gapped (never connected to the internet) Iranian centrifuges most likely via an unsuspecting Siemens employee or Iranian engineer (Sanger 2018).

When the malware activated, it subverted control of the centrifuges and forced them to operate at speeds and pressures that would cause them to malfunction. The malware also reported back to the operators that everything was normal and also prevented digital safety procedures form shutting the facility down (Langner 2011). It forced the engineers to start taking unaffected centrifuges offline to make sure they were not going to be destroyed too, further crippling the nuclear facility (Sanger 2018).

Stuxnet is the first attack of its kind in terms of states opting for a non-violent/non-lethal means of stopping Iran's nuclear program (Sanger 2012). It has been argued by military ethicists that Stuxnet can be fully analysed within the existing frameworks of conventional war, one concluded that it was

[12] As the class of all the case studies is attacks carried out by states it is determined the legitimacy criteria of who, being a nation-state, is fulfilled.

not an "insurmountable" challenge to argue that the effects occurred in physical reality; and therefore, does not need a new conceptualisation (Jenkins 2013). However, Jenkins dismisses important aspects of the act of aggression, claiming simply that because the impact occurred in Iran it can fit this conceptualisation. This ignores the fact that Stuxnet was not isolated only to Natanz but instead spread around the world to non-targeted networks and devices.

Analysts breaking down the code concluded that there were probably three well-resourced teams who worked on Stuxnet. Moreover, it would have required reconnaissance missions and other complex intelligence gathering operations to inflict the kind of damage done (Zetter 2014). The size of the malware was over 5-10 times the sizes of a traditional piece of malware, which cyber-experts say indicates the sophistication and resource intensity of its development (Zetter 2014).

What is the nature of Violence in this case?

Ultimately, Stuxnet caused 1,000 or 10% of nuclear centrifuges to be destroyed. However, the buildings themselves, as well as lives of engineers and other employees were not harmed, contra to what would have occurred if Israel and the US opted for a traditional airpower solution. The leading cybersecurity expert that analysed Stuxnet, Ralph Langner, claimed the attack was generic and could have damaged chemical plants or powerplants (causing chemical leaks or meltdowns that could have threatened civilians) that had a similar technical configuration, he equated it to a weapon of mass destruction (2011).

In a conventional sense an airstrike (X) would have destroyed the facility (Z_P). Within the elongated cyberwar sense, this act of violence, the Stuxnet attack itself (X), that assumed control of the centrifuges (Y), causing their destruction (Z_S).

Was the attack legitimate? –

There are a few levels of legitimacy that need to be looked at in this case. Firstly, the legitimacy of attacking infrastructure. At a broad level, Weinberger concluded that Stuxnet indicated that critical infrastructure (around the world) was vulnerable to cyberattacks and that many of these infrastructure possess acutely insufficient cybersecurity (2011, p.142).

Secondly, this cyberattack, despite being against a facility illegally manufacturing weapons grade uranium was not sanctioned by the UNSC. Therefore, it is de facto illegitimate within existing structures. However, an argument for legitimacy can be made as the facility had been the subject of several UNSC resolutions imposing economic sanctions on Iran, due to its repeated breaches of the NPT (Özcan and Özdamar 2009).

Thirdly, this attack relied on using a very significant vulnerability called a zero-day exploit. These are serious vulnerabilities that can allow for almost total control of a system. It has been noted by some people that exploiting such a vulnerability poses an issue because it means that the state has not notified vendors of the weakness and leaves their own infrastructure vulnerable (Zetter 2014, Ch.12). This is because the nature of operating systems means that any patches are known around the world.

Finally, as this cyberattack spread around the world, there was an issue of collateral damage, which the rules of law are designed to avoid or significantly minimise. Whilst the attack did not ultimately result in damage to any other networks, there is a possibility that if a matching system existed in the world it could have been inadvertently affected.

What Was Targeted–

The targeting of a nuclear facility that is producing illegal nuclear weapons does not indicate an expansion in the types of targets. It would be expected that within the bounds of a conventional war this would be a legitimate target, due to the overwhelming militaristic strategic advantage nuclear weapons have, not to mention Iran's alleged illegal pursuit of them. However, the targeting in this case makes it one of the most targeted military actions ever, with zero collateral damage and signifying that cyberattacks can be conducted successfully against infrastructure.

What Were the Political Outcomes?

This is harder to assess because there has been no official claim of responsibility by either the US or Israel. Therefore, we cannot be sure of the expected outcome. Whether that was to merely slow down Iran's production capabilities or if it was to eliminate it. Either way, there has been speculation over the effectiveness, with a short-term delay being caused but no longer-term implications (Warrick 2011). Furthermore, General Cartwright, who's tenure within the Joint Chiefs at the White House spanned the Bush and Obama administrations, indicated that in order for the US to be taken seriously, in terms of cyber deterrence, they had to illustrate their capabilities (Sanger 2018, p.32). In this sense, the Stuxnet attack not only necessarily achieved the objective of slowing down Iran but also indicated to the world that the US and Israel had developed significant capabilities.

Although, to be effective, deterrence requires clear communication, the fact that neither the US or Israel have officially claimed responsibility might limit the deterrent impact. However, most cyber-experts have steadfastly held that Israel and the US were responsible for this attack. Returning to the two equations, in both instances the desired political outcome Iran's attempts to make nuclear weapons were delayed (P), a political goal of both the US and Israel.

Summary –

If this case were to be summarised through a conventional lens, it would appear like this:

$$Airstrike\ (X_1) \rightarrow Nuclear\ Facility\ Destroyed\ (Z_P) \rightarrow Nuclear\ Programme\ Delayed\ (P_1)$$

Versus the cyberwar chain,

$$Stuxnet\ Code\ Spread\ (X_2) \rightarrow Control\ of\ Facility\ Systems\ (Y) \rightarrow Centrifuges\ Malfunction\ (Z_S) \rightarrow Nuclear\ Programme\ Delayed\ (P_2)$$

P is the same in both cases; however arguably P_1 would have been longer lasting as $Z_P > Z_S$ (i.e. more damage inflicted). However, X_2 is more legitimate, as Z_S has no civilian casualties. The extra layer of nuance, *Y*, allows for a military intervention that was less violent, more legitimate, in terms of reduced civilian impact, and could have similar political outcomes. The facility was also recoverable for civilian nuclear operations, should that be allowed to continue.

X_2 though poses a different issue of legitimacy, with cybersecurity experts such as Langner suggesting that the attack was generic in nature, meaning that the *Y* component could have produced other secondary (unintended) effects, some of which could be entirely unforeseen. For example, if the code had spread to an allied state's infrastructure that had a similar configuration as the Iranians, for another industrial control system, it is possible that such a facility would have been impacted too.

9.2 Case 2 – Russian Disinformation Campaign (2016 US Presidential Election)

In 2013, the Chief of the Russian General Staff, Valeri Gerasimov, announced the Russian intention of using "non-military capabilities to incite chaos and instability" (Ziegler 2017, p.566). This general idea was rapidly adopted by the Russian government, with the establishment of the Internet Research Agency (IRA; Sanger 2018, Kriel and Pavliuc 2019).[13] Russia's assertive use of cyberattacks has been escalating since their annexation of Crimea from Ukraine and its take down of a commercial airliner (MH17) in 2014 (Gould-Davies 2020). In response, the US and its allies ostracised Russia, imposing economic sanctions and suspended their membership in high-level multilateral talks (e.g. G8). However, Russia's most audacious cyberattacks began in 2016.

2016 marked the final year of the Obama presidency and the US presidential election. In the lead up to the election, there were reports of Russian interference in electoral processes. However, it was the decision of the Obama administration to not publicly intervene for fear that that intervention may be interpreted as political interference (Sanger 2018, pp.223-225).

Whilst it might be impossible to ever quantify how much Russian (dis)information campaigns influenced the US election, there is no doubt that Russia was trying to manipulate the electoral process (US Senate Intelligence Committee 2020.a). The Russian subversion campaign was multifaceted, utilising more than cyberattacks. RAND Corp outlines the many ways that Russian apparatus work together to subvert electoral processes around the world (**Table 2**). The most relevant to this case are the information and cyber aspects that are highly skilled and prevalent. The table illustrates that Russia is utilising cyberattacks as part of a broader suite of diplomatic, economic, and military means to destabilise the US. This is a clear use of operational cyberwar.

How Do Russian Organizations Engage in Subversion?

	State	Attributed and Unattributed Proxies	Foreign Partners of Russia	Major Challenges to Target
Military	GRU-Spetsnaz; VDV	Private military companies (Wagner Group)	Separatists	• Relatively highly capable light forces • Difficult to distinguish from armed civilians at the beginning; a law enforcement response might be insufficient, while a military response bears political costs and may contribute to Russian propaganda
Political	Possibly executed by intelligence agencies (GRU, FSB, SVR)	State-linked patriotic groups (e.g., Night Wolves biker gang)	Ataka in Bulgaria, Front National in France, AfD in Germany	• Political influence in target countries • Attribution to Russian government • Grounded in preexisting political divisions
Economic	State-owned enterprises (e.g., Gazprom, Rosneft)	Private, state-linked companies (e.g., Lukoil)	Trade partners with Russia	• Extensive European trade links with Russia • Difficulty distinguishing legitimate activity
Information	RT, Rossiya Segodnya, Sputnik, security services	Internet Research Agency (and other troll farms)	Users who amplify Russian media or unknowingly participate—"useful idiots"	• Deceptive or false content • Difficult to regulate • Attribution • Global reach
Cyber	GRU, FSB, SVR	Co-opted independent hackers: APT28, APT29	Patriotic hacking groups: CyberBerkut	• Highly capable • Attribution • Global reach

SOURCES: Robinson et al., 2018; Helmus et al., 2018; Larrabee et al., 2017; Radin et al., 2019.

NOTES: APT = advanced persistent threat; Ataka = Attack Party (Bulgaria); FSB = Federalnaya sluzhba bezopasnosti [Federal Security Service] (Russia); GRU = Glavnoye razvedyvatelnoye upravleniye [Main Intelligence Directorate] (Russia); GRU-Spetsnaz = Special Forces of the GRU; VDV = Vozdushno-desantnye voyska [Russian Airborne Troops]; SVR = Sluzhba vneshney razvedki [Foreign Intelligence Service]. While we use the term GRU because it is known as such, the organization is now formally "Glávnoe upravlénie Generál'nogo shtába Vooruzhjonnyh Sil Rossíjskoj Federácii" [Main Directorate of the General Staff of the Armed Forces of the Russian Federation] and abbreviated GU.

Table 2: How Russian Organisations Engage in Subversions (Radin, Demus and Marcinek 2020, p.9).

[13] For information on how Russian interference is thought to impact voters, see Hansen and Lim (2019).

Whilst going to war over regimes has been a feature of many states' foreign policy, it has tended to be against dictatorships, or specific leaders. However, cyberspace, a domain that was heralded as something quintessentially democratic, has enabled democracy itself to be undermined. The Russian Defence Minister, Sergei Shoigu, admitted the use of "information troops," to disseminate "smart, competent and effective" propaganda (Reuters 2017). Moreover, Chekov *et al*, highlight how Russian strategy is clearly evolving to make full use of cyber-capabilities as an offensive tool. This combination has led to an effective Russian military influence over information in democratic countries that increases during election times (2019).

What is the nature of Violence in this case?

Within this case, there is neither property damage nor physical violence inflicted on US citizens. Rather, if it is to be framed as such, violence occurs in the information space, manipulating information that voters access. Conventional war; however, has no way of realising this as an act of violence. The 'damage' inflicted is on information and ideas – but democracy also encourages the free and open exchange of ideas. This complicates the issue further as to defend against this kind of act is arguably antithetical to democracy itself.

Was the attack legitimate?

The method of this attack is seemingly legitimate. It utilised both sanctioned platforms and utilised freedom of speech. It replicated actions that any American citizen could have done themselves. This is because for a democracy, free speech and access to information are fundamental principles. This attack is unique is exploiting this very openness to manipulate the information layer and target US voters.

This attack is also unprecedented in terms of its reach, with at least 126 million citizens (non-combatants) being exposed to the attacks (Isaac and Wakabayashi 2017). The ability to try and affect so many citizens poses an important obstacle to using a conventional war framework, especially because the operations carried out by Russia were run through the GRU and the FSB and a linked agency called the Internet Research Agency (IRA; Mueller 2019; US Senate Intelligence Committee 2020a.b.).[14] This is a clear use of the military carrying out attacks on civilians through means that are clearly designed to be used as part of civil society and had no strategic military purpose when originally designed.

Targets –

This cyberattack had three main targets: voters and the information they receive; the DNC; and voting infrastructure. Voters were exposed to thousands of Russian fake news stories and targeted advertising. The information space in the US was weaponised where it became difficult for voters to distinguish truth from fiction. Moreover, targeted ads polarised people or targeted people to suppress voter turnout (Tomz and Weeks 2019; Norris 2018).

When combined with the findings of the Mueller Report, that the Russian government "interfered in the 2016 [election in a] sweeping and systematic fashion," and, "violated US criminal law," there is a clear indication that American democracy was under attack (Mueller 2019, p.1). One such violation

[14] Russian military intelligence and Federal Security Service (formerly the KGB), respectively

was the incursion into the Democratic National Committee's private servers and its subsequent release to WikiLeaks.

Furthermore, it was not just the information space that was manipulated, the US Senate Intelligence Committee released a report in 2020 that found that Russia used "extensive activity […] against US election infrastructure at the state and local level" (p.3). The report concluded that there was no evidence that any votes were changed (acknowledging their insight into this issue was limited), but admitted that the Russian government might have been "probing vulnerabilities" in order to manipulate future elections (pp.3-4).

Political Outcomes –

The aim of the attack was to produce confusion in the US and sow discord between citizens and to presumably have a more pro-Russian president elected. Internal turmoil especially from nationalists is good for Russia as it means a withdrawal of the US from the international sphere and could have broader military strategic intent as Russia can more easily expand their international military presence. However, with much of the two official reports classified, it is difficult to determine the exact impact that was created. Both reports illustrate the enormity of the Russian campaign, providing insight into the intent of Russia's involvement. The Alliance for Securing Democracy reported that the purposes of Russian interference were to co-opt extreme ends of the political spectrum to advance Russia's foreign policy in liberal democracies (Rosenberger and Morley 2019).

The objectives of Russia's interference include destabilising NATO by strengthening nationalist parties who are generally opposed to intergovernmental organisations, and reducing the allure of democracy for other states especially for close European neighbours such as the Ukraine (Ziegler 2017, pp.569-570; Karlsen 2019). Russia's more assertive foreign policy goals aim to return it to its former power as the Soviet Union, demonstrating that liberal democracy as well as multilateral organisations (that have recently been restraining Russia).

Summary –

It would be extremely difficult, if not impossible to achieve this kind of attack in a conventional sense. The absurdity of it becomes apparent when we map it into the equation,

Manually distribute propaganda and break into facilities to steal information, manual manipulation of voting machines; use of military force to coerce voters(!)(X) → Uncertainty about validity of election results (Z_P)? → Democratic norms and institutions undermined(P)

It is likely that a physical war would rather have a rallying effect of the citizenry, as they defend their territory. However, because it is difficult to detect fake news and its origins, the cyberwar method becomes much more effective at creating rifts amongst the public. This could be transcribed as,

Disinformation and information theft; voting machine hacking (X) → False and stolen data consumed by voters; votes manipulated (Y) → Voters Cognition and Behaviour Changes (Z_S) → IGOs and norms eroded, weakening democratic adversaries (P)

This type of attack would never be conducted without cyberspace. It is inconceivable that Russia would have such a large physical presence in the US to successfully conduct this, distributing propaganda and controlling media narratives. Moreover, to manually manipulate enough voting machines to change the result would also require an enormous investment in Russian agents within

the US. Additionally, coercive military force would be easily met with retaliation from the US. Other methods to control or subvert electoral outcomes would require physical destruction of apparatus or institutions or the mass killing of civilians which would likely immediately lead to conventional retaliation.

By expanding our understanding through a cyberwar lens, a richer understanding of the attack is gained. This is because such an attack would be inconceivable to have been carried out physically. The militarisation of cyberspace allows for the illegal retrieval of information and manipulation of voting machines in a much quicker, discrete and effective manner resulting in minimal retaliation. Secondly, the direct targeting of civilians (illegitimate targets) through legitimate infrastructures (social media) can more easily be understood. Moreover, attacking democratic institutions is now a viable possibility. There is no violence in this case. It is nearly impossible to illustrate violence against an idea or feeling of trust and this was the goal of Russian interference.

9.3 Case 3 – NotPetya - Russian Cyberattacks on Ukraine

In 2017, Russian military hackers released, into thousands of already compromised Ukrainian devices that used *M.E.Doc* accounting software, one of the most complex and destructive cyberattacks – NotPetya (Greenberg 2018; Nakashima 2018). What originally appeared to be ransomware, where data is encrypted and released upon payment, was something far more destructive, was irreparably destroyed (Ivanov and Mamedov 2017).

The cyberattack was part of the continued Russian campaign against Ukraine following Crimea's annexation in 2014. Nakashima reported that the GRU has been launching cyberattacks repeatedly against the Ukraine since that time (2018). It has been estimated that there were over €9 billion in global damages from significant disruption of industry. Former Homeland Security advisor Tom Bossert said that, "while there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory." (Greenberg 2018).

One of the major companies affected was Maersk, the largest shipping company in the world that accounts for over 20% of international shipping. These disruptions to business, banks, and government had significant flow on effects. The Maersk disruption alone caused truckdrivers and Maersk's clients tens of millions of dollars in potential damages to their own businesses (Greenberg 2018).

Violence –

Whilst it is unclear if anyone died as an indirect result of this cyberattack (X), it did result in the physical destruction of data by corrupting the hardware that it was located on (Y) (Greenberg 2018). This attacked the physical and information layers of cyberspace. Despite no reports of any harm to property or people, the economic flow on effects of this were enormous, as citizens and businesses needed to recover their data and were unable to access financial and government services. It is unknown whether this inability of people to access their money or other services resulted in any adverse effects; however, it is a conceivable possibility.

Legitimacy –

This cyberattack was originally targeted at Ukraine as an operational cyberwar in conjunction with their ongoing war with the Ukraine over Crimea. However, the attack exclusively targeted businesses, civilians and government bureaucracies that utilised the accounting software, making it illegitimate. The massive international propagation of the attack is highly illegitimate as businesses and civilians around the world were also impacted, despite having no involvement with the Russia/Ukraine conflict.

NotPetya highlights how easily a cyberattack like this can jump from network to network around the world and wreak havoc as it spreads. Once launched it can only be stopped if networks and devices are patched before it reaches them or whole networks are taken offline to isolate themselves.

Target –

The attack was targeted at Ukraine, as the accounting software was one primarily used only in Ukraine. However, the nature of cyberspace meant that international businesses that had the software on their devices in the Ukraine and were connected to networks were also affected. In this way, the target was not just the Ukrainian government, financial sector, and economy, but also the international economy. In the Ukraine, the second largest bank had 90% of its network and devices taken offline making it impossible for people to withdraw cash or make card payments (Greenberg 2019).

Political Outcomes –

The political objective was a clear expansion of destabilising efforts against Ukraine in their ongoing war over Crimea. Further, it is generally understood that Russia's goal is to undermine Ukraine's alignment with the EU and cause instability in the region (Greenberg 2018). Russia's attempt to hide the attack behind the guise of old attacks to deflect responsibility is also a key part of this, as they attempt not to stoke the ire of NATO and the EU. However, despite their attempts in 2018, Ukraine, the US and UK (among others), formally attributed blame to Russia (CyberPeace Institute 2019).

Summary –

NotPetya resembles a total war situation; however, the key difference in this situation is that the aggressor state had little to no control over the spread of the attack. In this sense, it is an extremely illegitimate attack that once launched was known to be able to spread. Compared to physical war, the aggressor state is at anytime able to command their forces to stand down. However, a piece of malware once released cannot be contained by the aggressor. This introduces a unique dynamic to a cyberattack that must be considered.

If this attack were to be conventionally conceived,

Conduct more geographically disparate physical attacks (X) → Loss of life, physical destruction, massive disruption to global supply chains (Z_P) → Economic and governmental chaos (P)

The conventional means of getting to the same political outcome is highly destructive both in terms of human casualties and physical destruction. Whilst these would result in massive economic chaos, as society would now have to reorganise into a war footing, it also invites massive retaliation from the target states. Moreover, a conventional war would be much slower to inflict this damage internationally. Requiring Russian forces to simultaneously attack several nations at once – which is also inconceivable.

However, when looked at through the cyberwar lens,

Launch of NotPetya to devices (X) → Hardware wipes data (Y) → Governments, financial institutions, businesses unable to deliver services (Z_S) → Economic and governmental chaos (P)

The interconnectedness and inter-reliability of cyberspace on delivering and supporting the local and global economies make them exceedingly vulnerable to a cyberattack that can spread across borders with minimal effort from the Russian aggressors massively increasing the size of Z_S. This form of attack means that Russia requires no physical presence around the world to inflict damage, rather a carefully crafted attack that propagates itself and inflicts increasing damage the more it spreads. Additionally, Russia does not require to move its own economy on to a war footing as a cyberattack does not require massive military movements. This means that the *P* is larger with a cyberattack because the cost to Russia is minimal.

Moreover, the NATO Cooperative Cyber Defence Centre warned that this could be a "violation of sovereignty," and lead to "countermeasures" (Hern 2017). This illustrates the breakdown of barriers between cyberwar and conventional war and illustrates the need for incorporation of cyberwar into the understanding of war itself. This is an important development for the largest military alliance as it suggests that the nature of war is shifting to a more digital theatre. Their willingness to consider conventional retaliation is evidence of the growing concern states have about cyberwar.

Whilst this attack would have unlikely been conducted conventionally due to logistical and strategic obstacles, the nature of cyberspace means that the attack was able to successfully spread around the world and result in some equally destructive results without physical consequences. The attack conducted either conventionally or digitally illegitimately targeted civilians.

9.4 Results and Theory Development

Each case presents different characteristics of cyberattacks that have occurred and will likely be used in the future. Stuxnet is unique in that it caused physical (non-data) damage. Moreover, it reflects a conventional understanding of war, and as noted by analysts, it is a proof of concept attack. Whilst its political outcomes only had short-term success, it proved that infrastructure is susceptible. Stuxnet highlights a new evolution of military capabilities. A cyberwar lens, compared to a conventional understanding, provides a more wholistic understanding of how the attack manifested into political outcomes. Moreover, Stuxnet showed that violence, through property damage, still has a role to play; however, the violence can be more readily directed to property over humans. Persisting with a conventional understanding based on this case would mean the potential for collateral damage is ignored.

Common throughout all three cases, is their failure to adhere to the existing rules of legitimacy. All three cases highlight that civilians are vulnerable to cyberattack. Whilst Stuxnet tried to limit the fallout by utilising highly sophisticated and targeted malware, it still spread throughout the world and could have affected non-targeted infrastructure. Moreover, the two cases of Russian cyberattacks, explicitly targeted civilians. Existing political science literature shows, as previously discussed, that targeting civilians has long been a feature of conventional war to force political outcomes, so it is unsurprising that this is the case with cyberattacks. However, it has historically never been so easy to readily target so many non-combatants simultaneously.

Importantly, the theatre of war is now every device connected to the internet. The cases highlight that this can either be done intentionally through demographic targeting through legitimate means (targeted advertising of social media platforms) or with intentional recklessness or total negligence as seen with NotPetya. The expansion of the theatre of war to encompass every geography will have large implications for the formalisation on any theory of war that more comprehensively incorporates cyberwar. The ability to target anyone, anywhere in the world enables both extremely targeted or unprecedently massive cyberattacks. The limiting factor of physical proximity or numbers of munitions has become de facto irrelevant. Moreover, citizens now bear responsibility for defending themselves against acts of cyberwar by keeping their devices updated. The responsibility of militaries to defend citizens from foreign attacks has now become an impossibility.

A revised theory of war will need to factor in to account the erosion of respect for legitimacy in the context of interstate war due to the near certainty that civilians will somehow be affected or directly targeted. This relates too with the expansion of targets that cyberwar opens. Once abstract and intangible elements of society (e.g. democracy; the economy) are now intertwined with cyberspace, making them no longer an abstraction but targetable. Whilst these are undoubtedly affected by conventional war, they can now be isolated and impacted directly, rather than secondarily. The two latter cases highlight Russia's pursuit of targeting these two areas.

The two cases about Russian cyberattacks, on the other hand, are unable to be readily explained within the traditional conceptualisation of war. In the case of Russian attacks on American democracy, it is a target that is incapable of being destroyed by physical means. Ultimately, democracy is an idea that has physical manifestations, but it is a belief that people have the right to govern themselves. Ideas cannot be shot or targeted by missiles; however, they can be undermined by manipulating the information-scape. Cyberattacks allow a foreign state to alter and specifically target (dis)information to individuals. This is further enhanced not by the destruction of election infrastructure but its manipulation, so that doubt about the process is raised. The manipulation of the physical layer is only minor but can have profound Impacts on the cognitive level.

This is highly reminiscent of the Cold War and the ideological battle between democracy and socialism. However, different this time is the way that Russia is able to directly manipulate information that is consumed by millions of people simultaneously and also in ways that can be directly targeted. Moreover, the possibility of remotely hacking the way vote machines record votes is another manifestation of this that could have profound electoral ramifications.

Together these cases have highlighted the precision and ease that new cyber-capabilities have given to militaries. Militaries are experimenting with how they can use these tools to conduct activities they would have been hesitant to conduct in a physical means or would be so large-scale as to be unfathomable to entertain. Changing human behaviour has become more of the primary object of these cyberattack than taking life. Conventional theories of war's focus on violence and an adherence to rules of legitimacy are being usurped by the reality to how state's are being aggressive towards one another. By expanding the causal chain when looking at cyberwar, these changes are more apparent, and it allows researchers and practitioners to more fully comprehend the nature of cyberwar.

10. Conclusion and Directions for Future Research

This thesis has explored war's enduring links to a physical reality that have existed for millennia and still thrive today. This thesis recognises that this will be a consistent component of war. However, it has proposed that the expansion of cyberspace and militaries' use of it, especially over the past decade has had a profound shift in how wars can now be fought. This has been looked at through the lens of four components, (i) violence; (ii) legitimacy; (iii) targets; and (iv) political outcomes.

Through a heuristic comparative case study and four overarching themes, this thesis has suggested foundations a new theory of war, centred around the secondary effects of cyberattacks and their reduction in physical violence. Cyberattacks enable civilians to more easily be targets of military actions. Moreover, cyberattacks enable the wholescale ability to undermine fundamental principles of democracy and the infrastructure that enables democracy to function, broadening our understanding of what is targetable in war. Additionally, if cyberwar capabilities are ignored, theorists and more importantly, practitioners will not be prepared to act either defensively against, or offensively with the powerful utility of cyberwar.

Conventional war has always relied on violence to produce political outcomes, as destruction of life and property was (and continues to be) a motivating catalyst of change. States wield violence as an organising force internally and attempt to control externalities through violence too. Cyberattacks are capable of inflicting property damage and potentially through causal mechanisms that need to be researched further, injure humans.

Legitimacy has been long recognised as another important factor of war, that war should only be used defensively and methods that unduly or explicitly harm non-combatants are off limits. The ubiquity of digital devices in the lives of humanity now means cyberwar can affect non-combatants more than military targets, providing a major need to reassess the rules and norms of war in the digital age as seen in the Russian electoral cyberattacks and NotPetya attacks. Whereas, for the most part, rules of war in respect to conventional war are adhered to.

Cyberspace allows for intangible things to become targets such as economies and forms of government. The implications of this are wide ranging as states need novel defences for these types of attacks but also a different spectra of retaliatory options as responding with conventional weapons might be in breach of international law regarding proportionality. Moreover, the ability to disable infrastructure without necessarily destroying it is another type of cyberattack that warrants caution.

Finally, in terms of political outcomes, the cases illustrate the ability to achieve at least some degree of political outcome equal to what has been possible through conventional war. The nature of new targets, however, has also opened up the ability to achieve other political outcomes, such as manipulating electoral outcomes or hampering economies without being embroiled in long drawn out physical war. The digital interconnectedness of many facets of life means that huge disruption can be wrought without having to leave the confines of your own territory.

Through introducing an extended causal chain to explain the nuance of cyberwar, a stark difference can be seen between the kinetic and the digital. These cases have illustrated that cyberwar needs to be more thoroughly researched. Militaries are no longer solely relying on physical war. With advances in quantum technology and advanced AI, the capabilities of cyberwar are only set to expand beyond the analysed cased. We are at a point in time with unprecedented technological change and insights

into the possibilities of our future capabilities, as theoretical science proceeds what we have been able to manufacture.

This area of research will be plagued by lack of transparency for the foreseeable future. Research can only be conducted behind the closed doors of security clearances or after events have spilled into the public domain. This will make theory development and testing difficult for academics and research in this field will be dominated by actors from within military and government establishments – which will have consequences on the neutrality, transparency, and generalisability of this research.

Future research should explore the links between government policies and military action within cyberspace and their political outcomes. Furthermore, how cyberwars are concluded should be researched. This thesis has only briefly touched on this issue. However, the end of war and how it comes about is vital to understand. Moreover, given Russia's stance that there is no longer a clear distinction between peace and war, rather on-going latent conflict, this will have important impacts on the nature of war itself and relationships between states.

References

Akande, D. and Hill-Cawthorne, L., (2015). The Lieber Code and the Regulation of Civil War in International Law. *Columbia Journal of Transnational Law*, 53(3), pp.638-651.

Armstrong, D. and Farrell, T., (2005). Force and Legitimacy in World Politics: Introduction. *Review of International Studies*, 31(S1), pp.3-13.

Australian Signals Directorate (2019). *Annual Report 2018-19*. [online] Canberra: Australian Department of Defence. Available at: https://www.asd.gov.au/sites/default/files/2019-10/annual_report_2018-19.pdf [Accessed 2 Mar. 2020].

Bennett, W. and Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), pp.122-139.

Benson, D., (2020). Handicapping Your Enemy: How the Internet Changes Balance of Power Politics. *Unpublished*.

Bowen, W. and Brewer, J. (2011). Iran's nuclear challenge: nine years and counting. *International Affairs*, 87(4), pp.923-943.

Bronk, C. and Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival*, 55(2), pp.81-96.

Buchan, B. (2002). Explaining War and Peace: Kant and Liberal IR Theory. *Alternatives: Global, Local, Political*, 27(4), pp.407-428.

Carnahan, B., (1998). Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity. *The American Journal of International Law*, 92(2), pp.213-231.

Cavaiola, L., Gompert, D. and Libicki, M. (2015). Cyber House Rules: On War, Retaliation and Escalation. *Survival*, 57(1), pp.81-104

Chaturvedi, A. (2005). Rigging elections with violence. *Public Choice*, 125(1-2), pp.189-202.

Chekov, A., Makarycheva, A., Solomentseva, A., Suchkov, M. and Sushentsov, A., 2019. War of the Future: A View from Russia. *Survival*, 61(6), pp.25-48.

Christensen, B. (2019). Cyber state capacity: A model of authoritarian durability, ICTs, and emerging media. *Government Information Quarterly*, 36(3), pp.460-468.

Clarke, R. and Knake, R. (2010). *Cyberwar*. HarperCollins.

Clausewitz, C. (2007) [1832]. *On war*. 2nd ed. Oxford: Oxford University Press.

Crowell, R. (2017). Some Principles of Cyberwarfare: Using Corbett to Understand War in the Early Twenty-First Century. Corbett Paper: No.19. London: King's College London.

CyberPeace Institute, 2019. *Case Study: Wreckweb*. Geneva: CyberPeace Institute.

Daugirdas, K. and Mortenson, J. (2015). NATO Affirms that Cyberattacks May Trigger Collective Defense Obligations. *The American Journal of International Law*, 109(1), pp.211-213.

Davidovic, J. (2015). Should the Changing Character of War Affect Our Theories of War?. *Ethical Theory and Moral Practice*, 19(3), pp.603-618.

De Franco, C., Engberg-Pedersen, A. and Mennecke, M. (2019). How do wars end? A multidisciplinary enquiry. *Journal of Strategic Studies*, 42(7), pp.889-900.

Dillon, M. and Reid, J. (2009). *The Liberal Way Of War: Killing To Make Life Live*. London: Routledge.

Doob, L. (1949). The Strategies of Psychological Warfare. *Public Opinion Quarterly*, 13(4), p.635.

Dougherty, J. and Pfaltzgraff Jr, R. (2000). *Contending Theories Of International Relations*. 5th ed. New York, NY: Addison Wesley Longman, Inc.

Eckstein, H. (2002). Case Study and Theory in Political Science. In: R. Gomm, M. Hammersley and P. Foster, ed., *Case Study Method*, 2nd ed. London: SAGE Publications Ltd.

EU Council (2008). *Council Directive 2008/114/EC*. 8 Dec. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN [Accessed 20 Feb. 2020].

European Parliamentary Research Service (2019). *Cyber: How Big is the Threat?*. Brussels: European Parliament, pp.1-2.

Faris, R., Roberts, H., Etling, B., Bourassa, N., Zuckerman, E. and Benkler, Y. (2017). *Partisanship, Propaganda, & Disinformation: Online Media & the 2016 U.S. Presidential Election*. Berkman Klein Center for Internet & Society Research.

Farwell, J. and Rohozinski, R. (2011). Stuxnet and the Future of Cyberwar. *Survival*, 53(1), pp.23-40.

Geers, K. (2010). The challenge of cyberattack deterrence. *Computer Law & Security Review*, 26(3), pp.298-303.

George, A. and Bennett, A. (2007). *Case Studies And Theory Development In The Social Sciences*. 3rd ed. Cambridge, MA: MIT Press.

Giegerich, B., Childs, N. and Hackett, J., 2018. *Military Capability And International Status*. [online] International Institute for Strategic Studies. Available at: <https://www.iiss.org/blogs/military-balance/2018/07/military-capability-and-international-status> [Accessed 1 August 2020].

Gilley, B. (2012). State legitimacy: An updated dataset for 52 countries. *European Journal of Political Research*, 51(5), pp.693-699.

Glaser, C. (1997). The Security Dilemma Revisited. *World Politics*, 50(1), pp.171-201.

Gould-Davies, N. (2020). Russia, the West and Sanctions. *Survival*, 62(1), pp.7-28.

Greenberg, A. (2018). The Untold Story of NotPetya, The Most Devastating Cyberattack in History. *WIRED*.

Greenberg, A. (2019). *Sandworm*. New York: Knopf Doubleday Publishing Group.

Hansen, I. and Lim, D. (2018). Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics*, 25(2), pp.150-171.

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012). The Law of Cyberattack. California Law Review, 100(4), pp.817-885.

Hern, A. (2017). 'NotPetya' malware attacks could warrant retaliation. *The Guardian*, [online] Available at: <https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik> [Accessed 13 July 2020].

Isaac, M. and Wakabayashi, D. (2017). Russian Influence Reached 126b Million Through Facebook Alone. *New York Times*, [online] Available at: <https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html> [Accessed 22 June 2020].

Ivan, P. (2019). *Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox*. Europe in the World Programme. Brussels: European Policy Centre.

Ivanov, A. and Mamedov, O. (2020). *Expetr/Petya/Notpetya Is A Wiper, Not Ransomware*. [online] Securelist.com. Available at: <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/> [Accessed 4 June 2020].

James, P. (1995). Structural Realism and the Causes of War. *Mershon International Studies Review*, 39(2), p.181-208

Jelf, E. (1933). What Is "War"? And What Is "Aggressive War"?. Transactions of the Grotius Society, 19, pp.103-114.

Jenkins, R. (2013). IS STUXNET PHYSICAL? DOES IT MATTER?. *Journal of Military Ethics*, 12(1), pp.68-79.

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics*, 30(2), pp.167-214.

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics*, 31(2), pp.289-324.

Jervis, R. (1989). Rational Deterrence: Theory and Evidence. *World Politics*, 41(2), pp.183-207.

Kapferer, B. (2004). Introduction. In: B. Kapferer, ed., *State, Sovereignty, War: Civil Violence in Emerging Global Realities*. New York: Berghahn Books.

Karlsen, G. (2019). Divide and rule: ten lessons about Russian political influence activities in Europe. *Palgrave Communications*, 5(1), pp.2-14.

Koloma Beck, T. and Werron, T., (2017). Violent Confliction: Armed Conflicts and Global Competition for Attention and Legitimacy. *International Journal of Politics, Culture, and Society*, 31(3), pp.275-296.

Kopp, E., Kaffenberger, L. and Wilson, C. (2017). *Cyber Risk, Market Failure, and Financial Stability*. IMF Working Paper (WP/17/185). Washington D.C.: International Monetary Fund.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In: F. Kramer, S. Starr and L. Wentz, ed., *Cyberpower and National Security*, 1st ed. Washington DC: National Defense University Press, pp.24-42.

Langner, R. (2011). *Cracking Stuxnet, A 21St-Century Cyber Weapon*. [video] Available at: <https://www.youtube.com/watch?v=CS01Hmjv1pQ> [Accessed 10 June 2020].

Lazer, D.M., Baum, M.A., Benkler, Y., Berinsky, A.J., Greenhill, K.M., Menczer, F., Metzger, M.J., Nyhan, B., Pennycook, G., Rothschild, D. and Schudson, M. (2018). The science of fake news. *Science*, 359(6380), pp.1094-1096.

Levy, J., (1998). The Causes of War and the Conditions of Peace. *Annual Review of Political Science*, 1(1), pp.139-165.

Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.

Lijphart, A. (1971). Comparative Politics and the Comparative Method. *American Political Science Review*, 65(3), pp.682-693.

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, 94(886), pp.515-531.

Lukito, J. (2019). Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017. *Political Communication*, pp.1-18.

Mandelbaum, M. (1998). Is major war obsolete?. *Survival*, 40(4), pp.20-38.

Manwaring, M. (2012). *The Complexity Of Modern Asymmetric Warfare*. Norman, OK: University of Oklahoma Press.

Maurer, T. (2019). A Dose of Realism: The Contestation and Politics of Cyber Norms. *Hague Journal on the Rule of Law*.

May, L. (2013). Jus Post Bellum Proportionality and the Fog of War. *European Journal of International Law*, 24(1), pp.315-333.

McGavran, W. (2009). Intended Consequences: Regulating Cyberattacks. *Tulane Journal of Technology and Intellectual Property*, 12(1), pp.259-276

Menashri, H. and Baram, G. (2015). Critical Infrastructures and their Interdependence in a Cyber Attack – The Case of the U.S. *Military and strategic Affairs*, 7(1), pp.79-100.

Morehouse, D. (1996). *Nonlethal Weapons: War Without Death*. Westport, London: Praeger.

Morris, J. and Wheeler, N. (2007). The Security Council's Crisis of Legitimacy and the Use of Force. *International Politics*, 44(2-3), pp.214-231.

Most, B. and Starr, H. (1983). Conceptualizing "War": Consequences for Theory and Research. Journal of Conflict Resolution, 27(1), pp.137-159.

Mueller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Washington, D.C.: US Department of Justice.

Münkler, H. (2003). The wars of the 21st century. *International Review of the Red Cross*, 85(849), pp.7-21.

Nakashima, E. (2018). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA Concludes. *Washington Post*, [online] Available at: <https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html> [Accessed 4 June 2020].

National Cyber Security Centre (2016). *How Cyberattacks Work*. [online] GCHQ: National Cyber Security Centre. Available at: <https://www.ncsc.gov.uk/information/how-cyberattacks-work> [Accessed 19 April 2020].

National Cyber Security Centre (2017). Annual Review. *GCHQ:* London.

Norris, P., 2018. Do perceptions of electoral malpractice undermine democratic satisfaction? The US in comparative perspective. *International Political Science Review*, 40(1), pp.5-22.

Nye, J. (1988). Neorealism and Neoliberalism. *World Politics*, 40(2), pp.235-251.

Nygren, K. (2002). Emerging Technologies and Exponential Change: Implications for Army Transformation. *Parameters*, 32(1), pp.86-99.

Oakley, J. (2020). *Waging Cyber War*. Online: APRESS.

Özcan, N. and Özdamar, Ö., 2009. Iran's Nuclear Program and the Future of U.S.-Iranian Relations. *Middle East Policy*, 16(1), pp.121-133.

Pettersson, T., Högbladh, S. and Öberg, M. (2019). Organized violence, 1989–2018 and peace agreements. *Journal of Peace Research*, 56(4), pp.589-603.

Porche, I. and Paul, C., York, M., Serena, C., Sollinger, J., Axelband, E., Min, E., and Held, Bruce. (2013). Redefining Information Warfare Boundaries For An Army In A Wireless World. Santa Monica, Calif.: RAND.

Porter, B. (2002). *War And The Rise Of The State*. 1st ed. New York: The Free Press.

Radin, A., Demus, A. and Marcinek, K. (2020). *Understanding Russian Subversion*. Perspective. Santa Monic, CA: RAND Corporation.

Reuters. (2017). Russia sets up information warfare units. *Reuters*, [online] Available at: <https://www.reuters.com/article/russia-military-propaganda/russia-sets-upinformation-warfare-units-defence-minister-idusl8n1g753j> [Accessed 24 June 2020].

Rid, T. (2013). *Cyber War Will Not Take Place*. 1st ed. New York: Oxford University Press.

Rid, T. (2013). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. *Foreign Affairs*, 92(6), pp.77-87.

Rid, T. (2016). All Signs Point to Russia Being Behind DNC Hack. *VICE*. [online] Available at: https://www.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack [Accessed 28 Feb. 2020].

Rid, T. and Buchanan, B. (2018). Hacking Democracy. *SAIS Review of International Affairs*, 38(1), pp.3-16.

Rosenberger, L. and Morley, T. (2019). *Russia's Promotion Of Illiberal Populism: Tools Tactics, Networks*. Policy Brief. Washington, D.C: Alliance for Securing Democracy.

Sanger, D. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times*, [online] Available at: <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> [Accessed 10 June 2020].

Sanger, D. (2018). *The Perfect Weapon*. London, UK: Scribe.

Sebenius, J. and Singh, M. (2013). Is a Nuclear Deal with Iran Possible? An Analytical Framework for the Iran Nuclear Negotiations. *International Security*, 37(3), pp.52-91.

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

Shore, J. (2015). An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security. *International Journal of Intelligence and CounterIntelligence*, 28(2), pp.236-251.

Silverstone, S. (2011). Just War Theory. *Oxford Bibliographies Online Datasets*,.

Sood, A. and Enbody, R. (2012). Targeted Cyber Attacks - A Superset of Advanced Persistent Threats. *IEEE Security & Privacy Magazine*, 11(1), pp.54-61.

Speier, H. (1948). The Future of Psychological Warfare. *Public Opinion Quarterly*, 12(1), p.5.

Splidsboel Hansen, F. (2017). *Russian hybrid warfare: A study of disinformation*. DIIS Report, No. 2017:06. [online] Copenhagen: Danish Institute for International Studies. Available at: http://hdl.handle.net/10419/197644 [Accessed 4 Mar. 2020].

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

Streck, J. (2013). Pulling the Plug on Electronic Town Meetings: Participatory Democracy and the Reality of the Usenet. In: C. Toulouse and T. Luke, ed., *The politics of cyberspace: a new political science reader*, 2nd ed. Milton Park: Routledge, pp.18-47.

Sullivan, P. (2007). War Aims and War Outcomes. *Journal of Conflict Resolution*, 51(3), pp.496-524.

Theohary, C. (2020). *Defense Primer: Cyberspace Operations*. In Focus. Washington DC: Congressional Research Service, pp.1-3.

Tomz, M. and Weeks, J., 2020. Public Opinion and Foreign Electoral Intervention. *American Political Science Review*, 114(3), pp.856-873.

UK Ministry of Defence (2018). Cyber Primer. London: UK Ministry of Defence.

Uma, M. and Padmavathi, G. (2013). A Survey on Various Cyberattacks and Their Classification. *International Journal of Network Security*, 15(5), pp.390-396.

Unal, B. and Lewis, P. (2018). *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences*. [online] London: Chatham House: The Royal Institute of International Affairs. Available at: http://www.menacs.org/wp-content/uploads/2018/01/Beyza_Cybersecurity-nw.pdf [Accessed 2 Mar. 2020].

United Nations' Charter. (1945)

Uppsala Conflict Data Program (2020.a). *Battle-Related Deaths By Region, 1989-2018*. [image] Available at: <https://ucdp.uu.se/downloads/charts/> [Accessed 19 May 2020].

Uppsala Conflict Data Program (2020.b). *Definitions*. [online] Uppsala Conflict Data Program. Available at: https://www.pcr.uu.se/research/ucdp/definitions/ [Accessed 13 Feb. 2020].

US Office of the Chairman of the Joint Chiefs of Staff (2012). *Information Operations*. Joint Publication (JP) 3-13. Washington DC: CJCS, p.I-1.

US Senate Intelligence Committee. (2020a). *RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCEIN THE 2016 U.S. ELECTION: Volume I: Russian Efforts Against Election Infrastructure with Additional Views*. Washington D.C.: US Senate.

US Senate Intelligence Committee. (2020b). *RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCEIN THE 2016 U.S. ELECTION: Volume II: Russia's Use of Social Media with Additional Views*. Washington D.C.: US Senate.

Valentino, B. (2014). Why We Kill: The Political Science of Political Violence against Civilians. *Annual Review of Political Science*, 17(1), pp.89-103.

Valeriano, B. and Maness, R. (2015). Cyberwar Versus Cyber Realities: Cyber Conflict in the International System. 1st ed. New York: Oxford University Press.

Van Evera, S. (1998). Offense, Defense, and the Causes of War. *International Security*, 22(4), pp.5-43.

Walrath, J. (2005). *Information Technology for the Soldier: The Human Factor*. [online] Adelphi: Army Research Laboratory. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a435271.pdf [Accessed 2 Mar. 2020].

Waltz, K. (2010). *Theory Of International Politics*. 5th ed. Long Grove: Waveland Press.

Wang, M., Nguyen, N., Dai, S., Chi, P. and Dow, C. (2020). Understanding Potential Cyber-Armies in Elections: A Study of Taiwan. *Sustainability*, 12(6), p.2248.

Warrick, J. (2011). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. *Washington Post*, [online] Available at: <https://www.washingtonpost.com/world/irans-natanz-nuclear-facility-recovered-quickly-from-stuxnet-cyber-attack/2011/02/15/ABUIkoQ_story.html> [Accessed 10 June 2020].

Weinberger, S. (2011). Computer security: Is this the start of cyberwarfare?. *Nature*, 474(7350), pp.142-145.

Weitsman, P. (2014). *Waging War: Alliances, Coalitions, And Institutions Of Interstate Violence*. Stanford: Stanford University Press.

Wheeler, T. (2018). In Cyberwar, There Are No Rules. *Foreign Affairs*, (230), pp.34-41.

Yin, R. (2018). *Case Study Research And Applications*. 6th ed. Thousand Oaks, CA: SAGE Publications Inc.

Zetter, K. (2014). *Countdown To Zero Day*. New York: Crown.

Appendix A – International Relations and War

Criterion	Global Military Power
Nuclear-delivery capability	Intercontinental, triad
Strategic mobility (air and sea)	Comprehensive inflight and afloat support, capable independently of routine continental reach
Strategic intelligence, surveillance and reconnaissance (inc. military satellites)	Yes; independent constellation
Cyber capability	Comprehensive offensive and defensive capability
Expeditionary combat-air capability	Full-spectrum capability at strategic range, including HQ and command-and-control assets
Aircraft carrier	Full multiple carrier-strike-group capability
Attack submarines	Nuclear-powered with land-attack capability
Amphibious combat	Yes; independently sustained, globally deployable
Armoured warfare	Comprehensive, independently deployable combined-arms capability
Intervention capability	Multiple divisions, all arms
Recent high-intensity combat experience	Yes

Summarised capability matrix from the IISS 2018.

Appendix B – Cyberattacks

Name of the Attacks	Description	Examples
Reconnaissance Attacks	Type of attack which involves unauthorized detection system mapping and services to steal data	a) Packet sniffers, b) Port scanning, c) Ping sweeps and d) DNS(Distributed Network Services) Queries
Access Attacks	An attack where intruder gains access to a device to which he has no right for access	a) Port trust utilization b) Port redirection c) Dictionary attacks d) Man-in-the-middle attacks e) Social engineering attacks and Phishing
Denial of Service	Intrusion into a system by disabling the network with the intent to deny service to authorized users	a) Smurf b) SYN Flood c) DNS attacks d) DDos(Distributed Denial of Services)
Cybercrime*	The use of computers and the internet to exploit users for materialistic gain	a) Identity theft b) Credit card fraud
Cyber espionage	The act of using the internet to spy on others for gaining benefit	a) Tracking cookies b) RAT controllable
Cyber terrorism	The use of cyber space for creating large scale disruption and destruction of life and property	a) Crashing the power grids by al-Qaeda via a network b) Poisoning of the water supply
Cyberwar	The act of a nation with the intention of disruption of another nations network to gain tactical and military advantages	a) Russia's war on Estonia (2007) b) Russia's war on Georgia (2008)
Active Attacks	An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise	a) Masquerade b) Reply c) Modification of message
Passive Attacks	An attack which is primarily eaves dropping without meddling with the database	a) Traffic analysis b) Release of message contents
Malicious Attacks	An attack with a deliberate intent to cause harm resulting in large scale disruption	a) Sasser Attack
Non-Malicious Attacks	Accidental attack due to mis-handling or operational mistakes with minor loss of data	a) Registry corruption b) Accidental erasing of hard disk
Attacks in MANET	Attacks which aims to slow or stop the flow of information between the nodes	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack d) Byzantine Wormhole Attacks
Attacks on WSN	An attack which prevents the sensors from detecting and transmitting information through the network	a) Application Layer Attacks b) Transport Layer Attacks c) Network Layer Attacks d) Multi-Layer Attacks

*Non-state actors

Uma and Padmavathi (2013, p.395).

	What	Specificity of Target
Denial of Service (Dos)	These attacks overwhelm a specific system so that it can no longer fulfil legitimate requests.	Highly targeted
Distributed Denial of Service (DDos)	As above, however, launched from multiple devices or a botnet.	
Malware	Software (inc. spyware, ransomware, viruses, and worms) that breach a system through a vulnerability that can then block access to parts of a network, disrupt certain aspects of a system, covertly acquire, and send information	Targeted
Phishing	Sending communications that aim to gather information or other sensitive data that can be used for financial gain or more significant exploitation (e.g. system/network access).	Highly targeted
Man in the Middle (MitM)	Data exploitation by sitting in the middle of a data exchange between two parties. [Espionage]	Targeted
SQL Injection	Inserting code into SQL databases forcing a server to reveal information it should not normally [Espionage]	Targeted
Zero Day Exploit	Exploiting a publicly known or unknown exploit in hardware/software on systems that have not been updated	Highly specific, targeted, becomes widespread
Sub-verting Supply Chain	Compromise software or equipment before it is delivered to a target	Highly targeted
Disinformation	Actively creating and disseminating disinformation to deceive or polarise a population, often utilising free and legitimate social media services.	Either highly targeted or broadly disseminated.