The Hammer and the Scalpel

Information Warfare in the 21st Century

George Sklavounos

A thesis submitted in partial fulfilment of the requirements

of a Bachelor of International Studies (Honours) Degree.

School of International Relations, Faculty of Arts and

Social Sciences, University of New South Wales, October 2017.

Words: 19,995.

"If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner."

– Omar Bradley (1948)

"A popular audience means an ignorant audience, doesn't it?"

– Socrates (Plato, 1960: 37)

STATEMENT OF ORIGINALITY

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgment is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Signed

………………………………………………………………

Approved as suitable for submission by

……………………………………………………………… (Supervisor)

Abstract

Information wars have become the main type of warfare in the information age. This seems fairly axiomatic: with an enormous expansion in the amount of data and information available to people in the 21st Century, it is only natural that the systems which contain and process that data and information – in the form of computers and people – would be exploited. Modern information warfare falls into two categories: cyber war, which targets the data created and stored on computers, and propaganda and disinformation, which target the information and knowledge people create. These two methods are the eponymous hammer and scalpel; cyber is the hammer, an incredibly powerful tool which is often deployed with brute force to attack the hardware and software on computers. The scalpel, on the other hand, is the targeted use of propaganda and disinformation – grouped together as 'active measures' – which can be incredibly effective at influencing the human mind, but must be used precisely and sparingly if they are to achieve results. Utilising a linear conception of the relationship between data, information, and knowledge, this thesis will examine trends in cyber war and active measures to argue that while cyber war is highly effective at targeting the data which underpins the Internet and computers, it is also largely relegated to the data level and rarely affects the more complex aspects of knowledge creation. In contrast, active measures – if utilised with precision and purpose – can have a devastating effect on the knowledge creation process, altering the subject's perception of the world around them. Overall, the hammer and the scalpel are two incredibly effective tools available to the modern information warrior, and when used correctly against their natural targets, they can achieve tremendous results.

Acknowledgements

There are a number of people who have helped me tremendously in the writing of this thesis, and without whom it would probably not exist. First off, many thanks to Will Clapton, whose guidance and comments were nothing short of greatness. Thanks to my parents, who acted as sounding boards and patiently listened to me prattling on about firewalls and Russian conspiracies. Thanks to Tom for all the Simpsons memes which perfectly encapsulated our theses. And thanks to Matt Blackburn for all the burgers, and for reminding me there’s a world outside Honours. I began this year thinking I would explore Australia’s cyber security, and ended up writing about how we are all being brainwashed from afar by nefarious actors. I spent roughly six months exploring the nature and origins of known cyber attacks, and four months in the weeds on Russian conspiracy theories. It’s been interesting.

Table of Contents

Introduction

"Most people, in fact, will not take trouble in finding out the truth, but are much more inclined to accept the first story they hear."

– Thucydides (1954: 47)

"Nobody has the monopoly on truth."

– Czech President Milos Zeman (Faiola, 2016)

In its 2017 *Global Trends* report – entitled 'Paradox of Progress' – the United States' National Intelligence Council predicted a disturbing trend. It suggested that nuclear weapons – as well as increasingly advanced conventional weapons – would result in an increase of "…lower levels of security competition…" in the next 20 years (National Intelligence Council, 2017: 216). Such competition would include "…indirect application of military power…" in the form of cyber war techniques, psychological warfare, and manipulation of politics, the media, and society (National Intelligence Council, 2017: 216). The purpose of this thesis is to examine such indirect applications of power in the form of information warfare (IW), exploring new and emerging trends in IW in the 21st Century to determine what its modern incarnations look like and how it is likely to manifest in the future.

In the wake of the 2016 US Presidential election – which will be viewed by future historians as a benchmark in IW in the 21st Century – this thesis will explore two modern incarnations of IW: cyber attacks – such as the hacking of the Democratic National Committee's (DNC) servers – and propaganda and disinformation – such as the advent of 'fake news'. IW is being recognised as a threat to all levels of civil society, government, and corporations, as it becomes increasingly apparent that the global hegemon's democracy has come dangerously close to being compromised by foreign actors (Boot, 2017). With Facebook being scandalised for allowing Russian ads to exacerbate social divides in the US during the 2016 election (Matsakis, 2017) and Hillary Clinton calling out Russian IW as a ‘clear and present danger’ to Western democracies (Zappone, 2017b), IW is becoming – in the words of Dmitry Kiselev, the host of a popular Russian propaganda show – the main type of warfare in the 21st Century.

By examining emerging trends in IW through the lens of knowledge creation – at the three levels of data, information, and knowledge (discussed below) – this thesis argues that IW in the 21st Century is divided into two broad categories. The first is cyber war techniques, which have only existed for the past 20 years but have become a highly publicised aspect of modern IW. The second is a combination of propaganda and disinformation – referred to as ‘active measures’ – disseminated widely through the Internet and social media but crafted meticulously to affect the way a subject perceives the world around them. The use of the term ‘active measures’ does not imply that cyber war techniques are ‘passive’ measures; rather, the term refers to a KGB IW campaign run during the Cold War, which focused on subversion and psychological operations and was publicly revealed by former KGB archivist Vasili Mitrokhin (Pomerantsev & Weiss, 2014: 4-5; Mitrokhin & Andrew, 2000: 224).

Together, cyber war and active measures are indicative of a new approach to IW enabled by advancing technology. Information warriors in the 21st Century can target every level of the knowledge creation process by choosing the right tool for the job. At the data level, cyber prevails; its cost-effectiveness and relative ease of access make it the proverbial ‘hammer’ of IW, a tool that requires no great skill to use but will nevertheless crack a subject’s defences with enough time and effort. Yet as effective as it is in targeting the data created and stored on computers, cyber is also very limited: cyber weapons targeting data are widely available, however, there are very few instances of cyber attacks affecting humans psychologically. Active measures, on the other hand, are incredibly effective at targeting the information and knowledge level. Disinformation and propaganda are the ‘scalpel’ of IW in the 21st Century: a highly nuanced instrument designed to penetrate the human body, they operate precisely to affect the way individuals and groups understand the world around them. These two implements are separated not just by what they can accomplish, but also who can use them: while anyone can pick up a hammer and use it semi-effectively, the scalpel must be used by a skilled operator if it is to be effective.

Methodology

Data, Information, and Knowledge

Ian Leslie, a correspondent for *The Economist*'s *1843* magazine, wrote "…the Internet makes information billionaires out of us all." (Leslie, 2012) The Internet facilitates the highest level of connectivity in human history and allows anyone connected to it to access massive amounts of information in moments. Yet access to such information is dependent on data: the binary and code which makes digital devices and the Internet possible and ensures their continuing operation. This data, created and stored on digital devices, allows users to access information and synthesise it into knowledge (Hey, 2004: 2). This process is usually depicted as either a line (where the relationship is linear and unidirectional) or a pyramid (where the relationship is hierarchical and based on the quantity of each of the stages).The linear or hierarchical relationship between these three phenomena is rarely questioned despite the blurred nature of the distinctions between each of the stages in the Data-Information-Knowledge (DIK) paradigm (Hey, 2004: 2). Zins (2007: 479), for example, notes the equation 'e=mc^2', which can be considered both information and knowledge, as it is both data placed into context and, simultaneously, a foundation for understanding the world. For the purposes of this thesis, it is important to define each of these aspects individually and describe how they interact with one another.

Data is the lowest level of the DIK paradigm and is the foundation for the creation of information and knowledge. Data describes an object (Hutchinson & Warner, 2001: 1); it is defined in information science as 'unprocessed information' and is considered to be objective (Hey, 2004: 5). It is perceived as a manipulable resource which can be quantified, with data in the 21st Century measured in 'bytes' (Hey, 2004: 5). Information, in contrast, is perceived as processed data; a phenomenon is termed information when the raw material (the data) has been codified and collated into a product which is useful or palatable for human consumption (Hey, 2004: 12). Information is essentially data in context (Hutchinson & Warner, 2001: 1), and as information has become integral to wealth in post-industrial states (Boisot & Canals, 2004: 44) the amount of information available to individual users has increased dramatically. Finally, knowledge is related to how information is interpreted (Hutchinson & Warner, 2001: 1); it involves the internalisation of external information, synthesising it into a picture of the world (Hey, 2004: 13). A number of authors draw a distinction between objective and subjective knowledge, where objective knowledge is that which exists in the world while subjective knowledge is that which is possessed by a person (Zins, 2007: 486; US Army, 2015: 3; Hey, 2004: 13).

This thesis will not delve deeply into the theoretical underpinnings of objective or subjective knowledge, or the philosophical question of whether there is an objective ‘truth’. Whether or not e=mc^2 is a form of objective or subjective knowledge is a predicament for philosophers; information warriors have already firmly decided that knowledge is subjective. IW techniques – most notably active measures – presume that there is no objective truth (Pomerantsev & Weiss, 2014), and in so doing are able to influence the information a subject receives and, in turn, their worldview. In this way, the information warrior’s understanding of the DIK paradigm is more in line with conceptions of subjective knowledge than objective knowledge. The idea behind this is essentially that the knowledge a particular person has does not necessarily correspond with the knowledge someone else may have on the same topic; it is precisely these subjectivities which active measures target. This is an issue which Henry Kissinger has also highlighted in *World Order*, where he argues that the amount of information accessible to us today has stymied and/or corrupted the synthesis of such information into knowledge (Kissinger, 2014: 349). The author notes that two users typing the same question into Google will receive two different results based on the data Google and other companies have collected on them. The issue here is that the information is presented as unbiased and objective, yet it has been relativised and selected based on what tech companies believe the user would want to see (Kissinger, 2014: 352).

This ‘poisoning of the well’ of information is incredibly problematic, as an example of the DIK paradigm will illustrate. A bomb goes off in the United States, injuring a number of people. In this instance, the events as they occur are the raw data; essentially, that a bomb has exploded at a location and at a particular time. This event is covered by news companies and disseminated by witnesses or people nearby through social media; this is the process of the data becoming information, as each individual – or company – places the bombing in its context, giving details of the people involved. Essentially, they go beyond what is immediately apparent (the data) to create patterns, thereby placing data into its context and making it palatable for human consumption, i.e., information (Hey, 2004: 12). This is the information which is perceived to be 'flooding' users in the 21st Century (Hey, 2004: 8-9); the event in question only happened in one place at one time, yet the patterns drawn in the data are endless as news channels and social media feeds are swarmed with information. This is where the metaphorical poisoning of the well can occur; there is mainstream information which would likely be reported by media companies such as CNN and *The Washington Post*, detailing the facts and placing them into their context as objectively as possible. Then there is an alternate narrative, propagated by websites such as *InfoWars* or *Russia Today*, which is more conspiratorial and intentionally highly subjective. The mainstream narrative might outline the characteristics of the suspected bomber, but the alternate narrative will question the bomber themselves, instead suggesting it was the work of US Navy SEALs as part of a complex 'false flag' operation. The choice of a bombing in the US for this example is not a coincidence, and the outlining of the conspiratorial narrative is not fiction. This is precisely what happened in the wake of the Boston Marathon bombings in 2013, and in a number of other similar incidents afterwards (Starbird, 2017) including the mass shooting in Las Vegas in 2017 (Barojan, 2017). The networks which propagated these rumours on social media often involved a number of botnets, suggesting an organised and dedicated effort to spread disinformation and undermine the mainstream narrative (Starbird, 2017).[1]

This deliberate spread of disinformation (in the form of conspiracy theories) will be examined in the 'active measures' section of this thesis. With regards to the DIK paradigm, however, disinformation can be incredibly problematic at the levels of information and knowledge, as well as the paradigm's oft-invoked but rarely witnessed fourth level, referred to as 'wisdom' (Kissinger, 2014: 349-350). Manifesting in different ways throughout human history and varying across different cultures, wisdom is generally based on knowledge and good judgement. Yet, as

[1] A botnet is a collection of computers or digital devices which are operated by a single person, often related to fake social media accounts.

Robert D. Kaplan notes, "…too much narrow expertise is the inverse of wisdom" (Kaplan, 2007). By having the information we receive filtered by what we want to see, we cannot always see sources or opinions which conflict with our own. This reinforces whatever it is we think or believe and crystallises into knowledge, at which point it becomes the basis of our understanding of the world around us.

IW techniques which target the information level are designed to bombard a target with information which crystallises into knowledge, reinforcing itself over and over to the exclusion of all other sources of information. Indeed, as argued by an unknown author in a 1976 issue of *Psychological Perspectives* (1976: 5), the only requirement for brainwashing to be effective is "…the capacity to rigidly control input…to so saturate the sensory circuits with desired information that undesired information is effectively blocked." In the past this would have required sealing a subject off from the world; this would have been the only way to ensure they received no other information. Yet today, with information a subject receives through the Internet being dictated by algorithms, the subject will effectively seal themselves off from the world as tech companies feed them only what they want to see. Once an IW narrative has been synthesised from information into knowledge (Zins, 2007: 479), the subject will effectively brainwash themselves. This self-invoked brainwashing is an issue that this thesis will explore in the context of active measures.

Method and Sources

This thesis will utilise a textual analysis to examine trends in IW in the 21st Century. It is important to note that peer-reviewed journals are in the minority of sources used in this thesis; this is not through negligence, but rather due to the nature of the topic itself. IW in both its forms resists academic study. Cyber war is fast-paced, cutting-edge, and highly classified. The vast majority of literature on it is written in technology magazines – such as *WIRED* or *Recode* – or by cyber security firms – such as FireEye, Mandiant, or Symantec. Academic literature is limited in this area because it either does not exist or is out of date; by the time an academic paper has been written and peer-reviewed, the next generation of smartphone has been released and with it a host of new cyber war techniques. Active measures, too, resist academic study; the value of disinformation and propaganda lies in being hidden from scrutiny. Conspiracy theories – a lynchpin of active measures in the 21st Century – have long been considered by academia as outside their purview (Yablokov, 2015: 301), meaning the literature on them simply does not exist. For the active measures section, sources include a number of publications on modern Russia – all of which, it should be noted, deal with Russian IW in one way or another – as well as publications on information warfare more broadly, and emerging reports from news organisations which have delved into Russia's role in the 2016 US election. This thesis will also utilise a number of conspiracy theory websites and articles as primary sources to demonstrate how such narratives are created and spread. All this is not to suggest that there are no academic sources whatsoever, but simply to clarify what may be perceived as a scarcity of such literature by an academic reader.

Outline

This thesis will examine IW in the 21st Century in two segments: the hammer and the scalpel. The first chapter relates to cyber war, and will describe current cyber war techniques and trends and argue that cyber is the proverbial 'hammer' of modern IW: widely publicised and incredibly effective, it is also limited as it only targets the data level of the DIK paradigm and largely relies on brute force. The second chapter will deal with active measures – propaganda and disinformation – focusing in particular on Russia's proclivity for such tactics. Active measures are the proverbial 'scalpel' of IW in the 21st Century, as their success is based less on repeated use and more on nuance and precision. The active measures section will cover the effects propaganda and disinformation have had when applied in a number of situations over the past decade, as well as exploring the effect conspiracy theories can have on a population.

The Hammer

Cyber War in the 21st Century

"The more that advanced economies and militaries come to rely on information technology, the more their enemies will seek to disrupt those vital networks."

– Max Boot (2007: 447)

IW targets information systems, and in the 21st Century these information systems come in two forms: computers and people. Cyber is the information warrior's weapon of choice in targeting the former; an incredibly versatile and effective medium, cyber war has a unique capacity to disrupt or destroy computers.[2] Yet as such devices have proliferated, so too has cyber war; the same tools and techniques originally used to target classified military servers have exceeded their mandate, and are used today to attack anything from a power generator to an individual's smartphone.

This chapter will argue that cyber war is an increasingly prevalent form of IW in the 21st Century, and while effective and highly publicised, it is relatively limited in its scope and its potential targets. Working from a linear understanding of the DIK paradigm, this chapter will argue that cyber war is an incredibly effective method of attacking the data level of knowledge creation, but is rarely used to influence the information level. This chapter will begin with a definition of cyber war and discussion of its differing interpretations, which is designed to impress upon the reader the uncertain and contested nature of cyber war and cyberspace overall; as Kissinger (2014: 344) suggests, in terms of cyber, "…capabilities exist for which there is as yet

[2] While 'cyberwar' and 'cyberattack' are the more common terms, this thesis will endeavour to avoid using 'cyber' as a prefix. A new form of conflict does not, in the opinion of the author, justify altering the basis of language. We do not say 'airwar' or 'nuclearwar', hence we should not say 'cyberwar'. The term 'cyberspace', however, is an exception to this.

no common interpretation – or even understanding."[3] This will be followed by a discussion of the actors in cyberspace – states, non-state actors, and corporations – as well as their roles and relationships with one another. This is a necessary component for organising what follows; the dynamics of cyberspace are different to the real world, and given that cyber war and active measures both utilise the digital realm, many of the concepts introduced in this section will be expanded upon as the thesis progresses.

The next section will deal with the aspects of cyber war which make it effective at targeting data, focusing on cyber's array of weaponry, asymmetric nature, pinpoint accuracy, and unforeseen consequences. The final section will examine trends in both destructive and disruptive cyber attacks, arguing that the former have remained relatively static and uncommon over time while the latter have become increasingly frequent and sophisticated in line with advances in technology. Despite their differences, there have been cyber attacks – both destructive and disruptive in nature – which have gone beyond data and targeted the information level of the DIK paradigm. Distinguishing between the two types is important to understanding not only cyber's broad capabilities, but also the different ways in which it might affect the information level.

It is important to note that unlike the manipulation of information (which can have knock-on effects at the knowledge level), targeting data will rarely influence the higher levels of the DIK paradigm without an operator's express intention to do so. This is because, for the most part, data is not something humans interact with on a daily basis, while information and knowledge are. While it is true that information in the 21st Century is overwhelmingly based on data in the form of ones and zeros, these fundamental building blocks are processed by computers, not people. Information, as noted prior, is essentially a way of making data palatable for human consumption (Hey, 2004: 12); the inputs people receive from screens on a daily basis are not data, they are information. The data is the binary or code which allows the computer to function. Cyber affects this level because cyber involves manipulating the code itself, thereby changing the way the computer or program functions. This can undoubtedly be used to affect the information level – such as

[3] In this instance, cyberspace is considered to be anything connected to a network. The US military's classified servers, for example, while not connected to the Internet, are still considered to be part of cyberspace.

having a security camera loop a certain section of footage to suggest to an observer that it had not detected any activity – however, data alteration alone cannot proceed beyond the information level. A guard who witnesses looped security camera footage can be fooled in the short term, however, they are unlikely to return home with a fundamentally different understanding of the world after this deceit. It is also important to note that while cyber is certainly capable of affecting the information level, the vast majority of known cyber attacks have not done so; broadly speaking, unless cyber is used as part of a larger strategy, its tremendous effectiveness at manipulating data means it does not necessarily need to be deployed beyond the data level.

Defining Cyber War

The term ‘cyber war’ is currently contested, with a number of scholars and researchers invoking different interpretations of it. Cyber war is only one aspect of cyberspace, however, the lack of clarity or consensus on the subject is an indication of the challenges that cyber issues pose in the 21st Century. Many definitions of cyber war presume that the nation-state is the primary actor in cyberspace, and essentially try to expand notions of conventional warfare to fit cyberspace. Kshteri (2014: 185), for example, defines cyber war as one nation-state taking actions against another nation-state with the hope of economic gain or material or prestige loss for the opponent. Clarke & Knake (2010) take this argument one step further and note that cyber war occurs primarily on computer, however, their definition still centres on the nation-state. Such definitions are rooted in a realist understanding of war (Goodin, 2010: 133), as they focus on nation-states and ignore the fact that the very nature of cyberspace allows non-state actors to exert considerable influence (Boot, 2007: 315). Indeed, if warfare in the 21st Century has taught strategists and policymakers anything, it is that war – be it cyber or conventional – can be fought by a myriad of actors, including nation-states and non-state organisations (Kim, 2012: 324).

There are, however, a number of scholars who view cyber war more broadly. Liff, for example, defines cyber war as occurring between “…two or more political actors” (Liff, 2012: 404), which could reasonably encompass states as well as non-state actors. Having said this, the author also suggests that any definition should not necessarily treat cyber war as inherently different from conventional warfare (Liff, 2012: 405). This is an idea echoed by Healey (2013: 11), who suggests that despite the technical and tactical aspects of cyber war being completely different from conventional warfare, at the strategic level it becomes strikingly similar, particularly when core concepts must be translated to policymakers and commanders. This is because knowing the intricacies of how something functions – be it a combustion engine, a jet, or a firewall – is not always necessary to understanding its capabilities (Healey, 2013: 11). It is important to note, however, that unlike any other domain of warfare, cyberspace is entirely man-made and is constantly in flux (Kan, 2013b: 111). This phenomenon is also not limited to the technological aspects of cyberspace; as Denning (1999: 67) suggests, cyber war "…is seen as a transformation in the nature of war that is about organization and psychology as much as technology." These fundamental disagreements between scholars regarding who can participate in cyber war and what qualifies as a cyber attack are indicative of issues not just in cyberspace, but in IW in the 21st Century more broadly. Many of the technologies and techniques which have allowed IW to proliferate – be it cyber war or active measures – have only existed in the late 20th Century or the early 21st, and in many cases, policymakers are unprepared to combat these techniques effectively.

Interestingly, one definition has stood the test of time, and is the basis for this thesis' definition of cyber war. Arquilla and Ronfeldt defined cyber war in 1993 less by which parties are involved and more by its objective; in their view, anything which involved the destruction or disruption of information and communications systems could be considered an act of cyber war (Arquilla & Ronfeldt, 1993: 30). This definition is the most inclusive, and is also the most accurate for current cyber war techniques: they can be performed by anyone but always target computers in one way or another. This, too, is indicative of cyber war's role in IW in the 21st Century overall: it is incredibly effective at disrupting or destroying computers – which create and store data in the form of files and directories (Denning, 1999: 21) – yet its unique capabilities in the digital realm also limit its ability to affect users in reality, i.e., the information or knowledge level.

Whosoever Holds the Hammer: Actors in Cyberspace

Before discussing the features of cyber war which make it effective at targeting data, or examining trends in cyber war, it is important to outline the actors which influence cyberspace. The first are states. Regardless of the power or influence which may have been gained in cyberspace by non-state actors, states are still the primary actors in this arena, as they are the regulatory bodies which govern the creators of software and hardware and can still influence users in the physical world (Segal, 2016: 27). While cyber power is not necessarily linked to conventional military power, it is perhaps not surprising that the world's only two cyber superpowers are China and the United States (Segal, 2016: 40). This is based not only on their digital infrastructure, political status, soft power, and openness to innovation (Burns & Cohen, 2017), but also on the narratives they create about cyberspace. These narratives shape the nature of the Internet as well as world politics (Singer & Friedman, 2014: 10), as other states either lean towards the United States' side – that the Internet should remain free (Segal, 2016: 39) – or China's side – that the Internet should be regulated by the state (Chuanying, 2016). It should also be noted that states employ some of the most sophisticated cyber war tools and techniques, such as the CIA's hacking arsenal released earlier this year (WikiLeaks, 2017) or China's 'Great Cannon', which – in line with Beijing's idea that states should be able to control traffic within their borders – temporarily redirects all web traffic routed through China towards specific targets in a massive DDoS (Distributed Denial-of-Service) attack (Stevens, 2015).[4]

Despite notions of cyber superpowers, it is non-state actors – particularly groups and corporations – who have benefited most from advances in communications and information technology. Indeed, the US National Intelligence Council's *Global Trends* report noted that while authorities have been given ever-greater tools to identify and track threats, such threats have also discovered new ways to facilitate their communications and recruitment (National Intelligence Council, 2017: 42). In the past, it was much easier for governments – authoritarian or not – to achieve 'information dominance' over dissident groups by, for example, shutting down a printing press (Byman, 2016: 77). Yet today, ISIS can wage a war

[4] DDoS: flooding a website or system with requests, causing it to load slowly or shut down completely. Often used in conjunction with botnets. A common brute force cyber war tactic.

against the West both on the ground and online, its digital presence allowing it to strike its aggressors at home. ISIS, however, is not the best example of a non-state actor utilising cyberspace; while active on social media (Alexander, 2017), their cyberspace activities are technically unsophisticated (Higgins, 2017).

Anonymous, in contrast, is far more hands-on, launching DDoS attacks at a number of targets including the Church of Scientology (Coleman, 2015: 5). Interestingly, Anonymous has actually engaged in cyber war against ISIS by hacking its websites or notifying Twitter of ISIS-linked accounts (Brooking, 2015). Non-state actors whose influence in cyberspace is advanced enough to attack one another in the digital realm is something which would have been inconceivable in the 20th Century, and is one of the defining characteristics of IW in the 21st Century. The increased capacity of non-state actors – notably individuals and groups – in cyberspace has resulted in the proliferation of cyber war techniques and is a contributing factor to the notoriety and public awareness of hacks in the 21st Century. Put simply, the simplicity of executing a cyber attack has dramatically increased the number of participants in cyber war. The hammer can be wielded effectively by any actor.

The third and final actor of note in cyberspace are corporations, whose motivations are largely profit- and data-driven. The private sector forms the backbone of the Internet, with a number of private companies controlling the vast majority of the physical infrastructure of cyberspace (Sheldon, 2014: 287). Such companies gather data on users in order to improve or create new products (*The Economist*, 2017) as well as using such data to target advertisements and marketing to specific users (Segal, 2016: 36). Tech companies have a lot of data on individual users, which is why they are incredibly attractive to state security and intelligence organisations such as the US National Security Agency (NSA) (Segal, 2016: 36). Given that they largely exist in the digital realm, tech companies are often far more formidable than states when it comes to cybersecurity. Indeed, when Georgia received DDoS attacks which overwhelmed its systems in 2008, it was able to stream much of its traffic through the US, and “Google, with its much larger infrastructure and bandwidth…was barely affected” (Segal, 2016: 69). The same DDoS attacks which crippled a nation-state were barely even registered by a tech company.

These companies' interactions and occasional disagreements with governments often have far-reaching implications for cyberspace. Encryption is the key factor in such disputes: governments want access to data that tech companies have, and these companies feel no compulsion to comply with such privacy violations (Lovejoy, 2017; Williams, 2017). This has caused a tremendous amount of tension between private companies and the US government, as after the Edward Snowden leaks US tech companies feared that their non-US customers – which in 2014 made up 58% of Google's revenue, 55% of Facebook's, and 88% of Intel's (Segal, 2016: 20) – would assume the NSA had built backdoors into all their software and stop purchasing their products (Kaplan, 2016: 235). Snowden's leak was devastating to relations between Silicon Valley and Washington, with the trust existent beforehand being almost completely eroded (Burns & Cohen, 2017).

This tension between governments and corporations is not universal, however. In contrast with Washington, Beijing has had far greater success with Silicon Valley; in 2016 Facebook began working on censorship software for the Chinese government (Gibbs, 2016), and in mid-2017 Apple removed a number of VPN apps from its app store in China based on Chinese regulations (Panzarino, 2017).[5] Overall, the actors listed above are vital to any understanding of cyber war, as the range of parties represented in cyberspace is indicative of the increased prevalence of information systems and, hence, the IW techniques designed to disrupt or destroy them.

The Glass Wall: Cyber War and the DIK Paradigm

Having examined definitions of and participants in cyber war, this section will outline the aspects of cyber war techniques which make them incredibly effective at targeting data, which in the 21st Century is almost exclusively created and stored on computers. Following the conceptualisation of cyber war as a hammer, cyber security measures (such as firewalls and anti-virus software) can be envisioned as a glass wall preventing an intruder from gaining access to the data contained within. While the glass wall can withstand the hammer for a time depending on its sophistication and density, cracks will eventually appear. This section will begin by

[5] A Virtual Privacy Network (VPN) allows a user to connect to a server in a different country, bypassing government censorship or detection.

examining cyber's asymmetry and inverting effect on power, followed by an analysis of its accuracy and potential consequences, and finally the specific features of cyber weapons which are uniquely capable of affecting data and have made cyber war ubiquitous in the 21st Century.

The Right Tool: Cyber's Asymmetry

In strategic parlance, cyber capabilities are considered an 'asymmetric' advantage (Kim, 2012: 324). In contrast to a symmetric advantage – which is gained by equalling the opponent in resources – an asymmetric advantage is gained by targeting an adversary's vulnerabilities (Galula, 1964: 6). Essentially, it is "…the ability to inflict great damage on a powerful adversary by using unconventional weapons" (Boot, 2007: 351). While cyber fits into this paradigm, it should be noted that cyber is not just asymmetric, but is actually capable of inverting conceptions of power.

This is one of the primary reasons why cyber war has become so effective at targeting the data level of the DIK paradigm. In the past, power – in both the military and economic senses of the word – was tied to manufacturing, or the ability to produce things on a large scale (Segal, 2016: 18-19). This is still the prevailing order of the world, yet cyber presents a challenge to it. The creation of malicious software ('malware') or cyber weapons does not require large-scale industrial production capacities; all it takes is a small number of computers and an equal number of people trained in their operation (Kaplan, 2016: 5). Furthermore, an actor's sophisticated digital infrastructure – the very tools which determine its role and influence in cyberspace (Burns & Cohen, 2017) – can actually make it more vulnerable to a cyber attack (Entous et al., 2016). Essentially, cyber is an effective tool at targeting data because the data itself – in the form of computer networks – is incredibly vulnerable (Uchill, 2017; Newman, 2017), and the increasing importance and prevalence of data in cyberspace, in everything from commerce to social media, expands the number of actors who wish to target it, thereby increasing the number of parties utilising cyber war. As cyber war techniques become more profitable, the actors with the most data realise they have the most to lose. To compare this situation with conventional warfare, it is almost unthinkable to suggest that the United States' incredibly advanced military makes it more vulnerable to a conventional attack. Yet the building blocks of the United States' power in cyberspace mean that it will always be vulnerable, and conduct cyber war from within glass walls (Kaplan, 2016: 216). This inverting effect is critical to understanding cyber's ubiquity; essentially, the more connected an actor is to cyberspace, the more vulnerable they are to a cyber attack.

Much as cyber can invert conceptions of power for larger or more technologically sophisticated states, it can also allow smaller states and non-state actors to have greater influence than they might otherwise enjoy. Small countries like Israel and Estonia – whose manufacturing sectors are nowhere near those of larger states – have invested heavily in their technology sectors (Hague, 2017). As well, their relatively small populations allow for easier sharing of technology and techniques (two staples of success in cyberspace), as those working in the cyber security industry in such states often have personal relationships (Segal, 2016: 64). This also means their response time in the event of a cyber attack is reduced; unlike in larger states such as the US, where a number of different agencies and government bodies must coordinate responses (such as the NSA and National Security Council), the links between cyber security experts and practitioners in smaller countries are more direct and more personal (Segal, 2016: 64).

Cyber has also become an avenue of exploration for states which feel besieged by the West: both North Korea and Iran have cyber warfare capabilities and have used them in the past to conduct cyber attacks, such as the North Korean hack of Sony Pictures in 2014 (*The Economist*, 2014). However, despite smaller states gaining a great deal of influence by investing in cyber, the United States still leads the way (Segal, 2016: 14-15); indeed, the NSA was able to attribute the Sony hack to North Korea because they had already hacked Pyongyang's computers (Kaplan, 2016: 269). Less conventionally powerful actors – be they states or non-state actors – have recognised cyber war's potential for both the accumulation of power and for disruptive acts by which they can increase the cost for more materially powerful actors to pursue their goals (National Intelligence Council, 2017: 28).

The proliferation of cyber war techniques in the 21st Century is based largely on the minimal infrastructure necessary to engage in cyber war and the fact that it can asymmetrically target more conventionally powerful states. The abundance of data in the modern world – especially in more technologically advanced and conventionally powerful states – makes investing in cyber war an incredibly cost-effective avenue for targeting the data level of the DIK paradigm. As well as cyber's effectiveness, the benchmark for entering into a cyber war campaign is set incredibly low. Anyone – whether they are a non-state actor or a small state facing US aggression – can pick up a hammer and strike their adversary's glass wall.

The Hardware Store: Cyber Weapons and Exploits

While cyber's asymmetry has contributed to its ubiquity in the 21st Century, the nature of cyber weapons goes a long way towards explaining how and why they are so effective at targeting data. Cyber weapons – code that is designed to threaten or damage anything from a single computer to an entire network (Rid, 2013: 37) – are radically different from most if not all conventional weapons. For the most part, they are cheaper, can be recycled, and often rely on previously unknown flaws in the target's system. These weapons define cyber war and cyber conflict, and by extension, anyone wishing to manipulate the data level of the DIK paradigm.

To gain an understanding of cyber weapons, it is important to distinguish them from conventional weapons. Cyber weapons do not use kinetic force, relying instead on digital means (Singer & Friedman, 2014: 68). As well, they target the data created and stored on computers before physical locations or infrastructure, and they are difficult to attribute (Lin et al., 2012: 24). It is also important to note that their outcome is harder to predict than that of conventional weapons (Singer & Friedman, 2014: 68-69): a cyber weapon can spread beyond its mandate in a number of ways and through no fault of the creators (Lin et al., 2012: 25). Indeed, the malware known as 'Stuxnet' was only discovered because it spread further than its intended target and infected more than 300,000 computers in roughly a hundred countries (Segal, 2016: 3-4).[6] Beyond these obvious differences, however, are a number of aspects which lie at the heart of cyber's capacity to influence data, which explains its prevalence in the 21st Century.

Firstly, cyber weapons are extremely cost-effective. In contrast with conventional weapons – whose life cycle and efficacy are dependent on research to

[6] Stuxnet was a virus created by the US government and used to sabotage Iran's 'Natanz' nuclear reactor.

develop the weapon followed by mass production – cyber weapons essentially skip the ‘mass production’ phase. The majority of expense is devoted to the research and development phase (Singer & Friedman, 2014: 69), after which the malware is ready to go and can simply be copied over and over again. It should be noted, however, that the ease with which actors can develop cyber weapons is proportional to the difficulty of defending against them; as Kim (2012: 325) eloquently surmises, “…today cyber weapons absolutely overwhelm defensive tools and techniques.”

All parties with an interest in cyberspace develop defensive capabilities, however, none have proven impenetrable; the glass wall will always break. Even data stored on ‘air-gapped’ computers is vulnerable to cyber war techniques.[7] In the past, USB thumb drives have been used to circumvent such defensive measures, notably in the case of Stuxnet (Kaplan, 2016: 207) and a 2008 cyberattack dubbed ‘Buckshot Yankee’, which saw thumb drives made in Russia and sold in Afghanistan being loaded onto computers connected to the Pentagon’s classified network (Nakashima, 2011). The Pentagon’s response in the case of Buckshot Yankee is interesting: it banned the use of external hard drives and USB sticks (Zetter, 2011), however, it subsequently allowed thousands of exceptions to this policy in the name of efficiency (Whittaker, 2013). The US military’s capitulation is demonstrative of a prevailing truth of cyberspace: after an actor has digitised their key systems and infrastructure, unplugging their network is simply not a viable option. Once data is stored on a computer it is susceptible to extremely cost-effective cyber war techniques, which can either be deployed in brute force or utilise lapses in security to reach their objective. One way or the other, the hammer will break through.

While cyber weapons are certainly cheaper than conventional weapons, they are not free. There are still resources which must be dedicated to their creation, and often the sophistication or size of the malicious code – as well as its targets – can be indicative of whether a nation-state or non-state actor was responsible for its creation. A cyber attack conducted by a group, for example, will most likely have no specific target, reuse malware available online, and simply try to infect as many machines as possible, stealing important information like credit card numbers or passwords (Player, 2015). In contrast, a cyber attack conducted by a nation-state will

[7] An air gap involves keeping a system disconnected from the Internet or any other network; it is separated by a literal gap of air.

most likely be more focused, more sophisticated, built from scratch, and designed to avoid detection (Player, 2015; Zetter, 2012). The malware known as Flame, for example, was developed by the United States and was roughly 4,000 times larger than the typical hacker tool available at the time (Kaplan, 2016: 204-205).[8] A group – regardless of its dedication – simply would not be capable of creating such a complex and enormous piece of malware, which led many cyber security experts to believe it was the work of a nation-state (*The Economist*, 2010b; Kramer & Perlroth, 2012).

As well as being incredibly cost-effective, cyber weapons are also reusable. This particular facet of cyber weapons can make life incredibly difficult for cyber security researchers, as they will often attempt to determine malware's origins by comparing it to samples of past malicious code (Segal, 2016: 55). During the 2014 Sony hack, for example, the evidence built on malware samples was not sufficient to implicate North Korea, but also not enough to rule out Pyongyang (Segal, 2016: 56). The malware used in the cyber attack was very similar to past hacks perpetrated by 'DarkSeoul', a hacker group working for North Korea which attacked South Korean banks and television stations in June 2013 (Segal, 2016: 55). It is important to note that one cyber weapon's similarity to another is not conclusive proof of origin; as Marc Rogers, director of security for DEF CON (the largest hacker conference in the world) notes, a great deal of malware is publicly available and is commonly circulated among hackers (Rogers, 2014).

There are a number of examples of this trend in effect. 'Poison Ivy' is a breed of malware which is so commonly used it is difficult to distinguish one user from another, and has formed the backbone of a number of cyber attacks in the past (FireEye, 2013: 32). 'BlackEnergy' is a type of malware initially designed for DDoS attacks and sold on the Russian black market, then repurposed to steal passwords and IDs from bank websites and eventually used to conduct espionage against both public and private actors (Kaspersky Lab, 2017; Segal, 2016: 13); a link has also been suggested between BlackEnergy and the 2017 ExPetr ransomware attacks (GReAT, 2017). Flame was repackaged by Iran's cyber war unit and used to wipe

[8] Malicious software which formed the basis of 'Stuxnet', Flame has been found throughout the Middle East and has a broad range of applications from logging keystrokes to monitoring Skype (Zetter, 2012; Kim, 2012: 327).

almost 30,000 hard drives at the joint US-Saudi Arabian oil company, Saudi Aramco (Kaplan, 2016: 213). And, in October 2017, all US government agencies were ordered to remove any antivirus products sold by the Russian cyber security firm Kaspersky from their systems, after Israeli intelligence officers noticed an NSA-created tool contained within the company's products; this tool had been stolen from the Agency after a single NSA employee had improperly kept classified documents on their personal computer (Perlroth & Shane, 2017).

The hammer – whether by flaws in security or human error – will always penetrate the glass wall, yet these incidents are also indicative of a broader trend in the creation and use of weapons in cyberspace. Cyber weapons can be reverse-engineered or repackaged and used to strike a broad range of targets; this facet of malware is also one of the main reasons it is difficult to attribute a cyber attack to a particular actor. Put simply, along with the cost-effectiveness of picking up a hammer to strike an adversary's defences, the field of cyber war is replete with tools which can be bought or stolen from other actors and used off the shelf or repurposed for something completely different. Actors intending to manipulate data will find no shortage of cyber weapons, which contributes to the prevalence of cyber attacks in the 21st Century.

Finally, no discussion of cyber weapons would be complete without an examination of 'zero-day' exploits. For an actor involved in cyber war, zero-day exploits represent pre-existing cracks in the glass wall guarding their target's data. Zero-days are software bugs whose presence and nature is unknown until the point of their discovery, and are an unavoidable aspect of modern information technology (Nakashima, 2016; Singer & Friedman, 2014: 42). The name 'zero-day' is based on the uncertainty inherent in the exploit; as it could not have been known prior to the attack, the day of the attack is the zeroth day that a patch to the issue can be created (Singer & Friedman, 2014: 42).

The transition of zero-days from quirks in an operating system to prized exploits for both tech companies and black marketeers is indicative of broader changes in cyber war over time. Zero-days have become an incredibly important aspect of the cybersecurity industry, with large companies becoming semi-reliant on private actors to discover vulnerabilities in their software (Coleman, 2015: 25). As cyber war has intensified and the cyber industry has grown and expanded, the premium placed on zero-days has increased dramatically; today, those who discover such exploits can sell them to governments, criminals, or tech companies for a small fortune (Kaplan, 2016: 137).

A number of notable past cyberattacks have involved zero-day exploits. In particular, the discovery in 2015 of malware hidden in Kaspersky's servers used three zero-day exploits: one to infect the original machine from an email, one to infect the network from the original machine, and one to install the malware's toolkit in the computer's kernel, the deepest level of its operating system (Zetter, 2015). The use of so many zero-days, coupled with the general sophistication of the code, led many to assume it was created by a nation-state (Zetter, 2015), and given that Kaspersky has been linked with Russian cyber war (Perlroth & Shane, 2017), it is likely the malware discovered in its servers was originally created by the US. While zero-days can appear in a number of contexts, they are certainly used by states to create their own malware (Zetter, 2014); Stuxnet, for example, utilized five zero-day exploits to infect and control the centrifuges at one of Iran's nuclear reactors (Kaplan, 2016: 203-206).

Overall, cyber weapons are far more multi-faceted than their conventional brethren; in addition to striking targets, they can also be created, repackaged and recycled for comparatively little cost (Kramer & Perlroth, 2012). The reusable nature of cyber weapons, coupled with the difficulty in attributing a cyber attack and the prevalence of digitally stored data in the 21st Century, explains why cyber is the information warrior's tool of choice for targeting the data level of knowledge creation. Yet for all the complexity of the cyber weapons themselves – such as creating malware or discovering zero-days – the only feature of cyber weapons which can be used to influence the information level of the DIK paradigm – the context in which data is processed by a human operator – is the fact that a great deal of malware shares a common heritage. This aspect of cyber has been used to deflect blame in the past, particularly by Russia in response to investigations of cyber attacks against Georgia in 2008, during which Russian officials pointed to the public availability of tools used to conduct DDoS attacks to suggest it was the work of private citizens or groups rather than the government (Segal, 2016: 68). Cyber's versatility, cost-effectiveness, and asymmetric nature have made cyber war ubiquitous in the 21st

Century, and while it rarely features in IW campaigns at the information level, its effectiveness at manipulating data means it does not necessarily need to transcend this divide. When an information warrior wants to break down a glass wall, they use a hammer.

Shards of Glass: Cyber War's Accuracy and Unforeseen Consequences

Another important aspect of cyber which has made it the IW tool of choice for targeting data is its pinpoint accuracy, which can sometimes blind its users to its unforeseen consequences. Different actors – including states and non-state actors – have different priorities and different areas which they consider vital to their continued survival and prosperity. Some are the same targets an adversary would consider in a conventional war – industries or locations deemed 'critical infrastructure', such as electrical power, telecommunications, and water supply (The White House, 2013). Other priorities, however, are less tangible; China, for example, wants the Communist Party to have the 'most powerful voice in cyberspace' (Ruwitch, 2016). This is a fairly simple example of an actor's priorities; control in cyberspace is important to Beijing, therefore any attempt to diminish the Party's control could prompt Beijing to escalate. Yet each actor's priorities are different, and despite cyber's accuracy, it can sometimes cause unforeseen consequences (Segal, 2016: 86-87).

The knock-on effects of a cyber attack are difficult to comprehend. For example, a cyber attack turning all the traffic lights in an area red may be considered nothing more than a nuisance in the United States. In Tel Aviv, however – which already experiences prohibitive traffic – such an event could be considered an act of war, as Israel's military strategy in the event of a conflict is reliant on the ability to quickly deploy its reserve forces (Segal, 2016: 97). These unforeseen consequences can also affect cyber attacks which target the information level of the DIK paradigm. Hacking the Associated Press's Twitter account and suggesting that a bomb had injured President Obama – as the Syrian Electronic Army did in April 2013 (Kan, 2013b: 111) – might not seem like grounds for war, yet within a few seconds of the tweet going out the Dow Jones Industrial Average dropped 146 points and $136 billion in market value disappeared (Segal, 2016: 16-17). Financial services are considered by Washington to be critical infrastructure (The White House, 2013);

therefore, the ramifications and unforeseen consequences of the hacking of a Twitter account could justify the position that the hack itself targeted the United States' critical infrastructure. Whether or not the Syrian Electronic Army's actions were intended to cause issues on Wall Street is unclear, however, the end result of a single erroneous tweet demonstrates how cyber can effectively bolster an IW campaign targeting the information level of the DIK paradigm.

The prevalence of data in the 21st Century and cyber's precision in targeting that data have made cyber war techniques a cost-effective endeavour for a number of actors, both state and non-state. Yet cyber's precision can create a false impression in an attacker's mind that their actions will not prompt a response; in such cases they may not consider the unforeseen consequences or ramifications of their actions, or fall prey to 'mirror imaging' – an actor's assumption that their target will react in the same way to a situation as they would (Goldman, 2006: 91-92).

The importance of an actor's priorities also extends to non-state actors. In 2008 the hacker collective Anonymous engaged in a cyber conflict with Los Zetas, a Mexican drug trafficking organisation (Kan, 2013a). After Los Zetas kidnapped a member of Anonymous, the hacker group threatened to 'dox' Los Zetas (Kan, 2013a: 40).[9] 'Doxing' is a common hacker tactic, and Anonymous's resort to it is not atypical for the group (Coleman, 2015: 7), yet in this instance Los Zetas took Anonymous' stated actions as an existential threat. As a criminal organisation, the opacity of Los Zetas' networks and operations was key to the group's efficacy and survival (Kan, 2013a: 46). By threatening to reveal its network and its members Anonymous had, perhaps unwittingly, forced Los Zetas to escalate by attempting to 'reverse hack' Anonymous' members and threaten them (Kan, 2013a: 40).

Cyber's precision and unforeseen consequences are a critical issue for policymakers and heads of non-state organisations in the 21st Century. Cyber is still very much an emergent domain, and one which policymakers have yet to fully come to terms with (Burns & Cohen, 2017). One need look no further than repeated requests from policymakers that corporations provide backdoors to their products -- despite the fact that such backdoors can subsequently be exploited by nefarious actors – for evidence of this (Williams, 2017). This lack of understanding is incredibly

[9] Dox: reveal a target's identity and make their private information public.

problematic, as two of the defining features of cyber attacks are speed and ambiguity (Kaplan, 2016: 272). In the event of a cyber attack, where policymakers' decision time is reduced and leaders are expected to make snap decisions based on limited information, the risk of escalation is high (Segal, 2016: 77-78). Exacerbating this ambiguity is the fact that there is no functional difference between cyber espionage and preparation for an attack; both involve intruding into a network and can easily be mistaken for one another. In such a situation – which are becoming more common – a defender may feel obligated to respond as quickly and forcefully as possible (Segal, 2016: 84).

The aspects of cyber war noted above explain why cyber is so effective at targeting data, and are indicative of the difficulties cyber poses to information systems in the 21st Century. Cyber inverts conceptions of power by making anything connected to a network a liability to a defender (Uchill, 2017); its weapons are cheap and easy to use, reuse, and recycle; it is capable of precise strikes on anything from a single computer to an entire network; and its speed and ambiguity, while beneficial to the attacker, can sometimes create unforeseen consequences. Cyberspace's ubiquity has yielded tremendous gains, however, in terms of IW it has also created tremendous vulnerabilities for anything and everything run by a microchip. Cyber war techniques – as a facet of IW – hold sway in the digital domain, and as that domain has expanded and continues to expand, cyber war will only become more common as actors continuously look for ways to pursue their interests in a cost-effective and largely covert way.

The Hammer Strikes: Destructive and Disruptive Cyber Attacks

This section will examine two eminent trends in cyber attacks – destructive and disruptive – to examine how cyber war has adapted to the prevalence of digital devices, which has increased the number of potential targets from a handful of US military servers to virtually any computer. This section will also outline cyber attacks which have transcended the data level and influenced the information that a human operator has received.

Destructive

Despite a number of policymakers and strategists suggesting that a destructive cyberattack – often invoked as a 'cyber Pearl Harbour' or 'cyber 9/11' in the US – could damage or destroy an actor's infrastructure or harm its citizens, such cyber attacks have been few and far between. One of the earliest known destructive cyber attacks occurred in 1982, when a pipeline in Siberia exploded due to adjustments made by the CIA on the pipeline's computer-control systems (*The Economist*, 2010a; Boot, 2007: 447). Another example was the Aurora Generator Test, which occurred twenty-five years after the Siberian pipeline explosion and involved a group of cyber security researchers destroying an electrical generator to demonstrate such systems' vulnerabilities (Meserve, 2007). The fact that they were able to do so in just three minutes with twenty-one lines of malicious code is proof of the ease and efficacy of shattering an adversary's glass walls (Kaplan, 2016: 167-168). Stuxnet, too, is an example of a destructive cyberattack, as it involved the sabotage of centrifuges at one of Iran's nuclear power plants (Kaplan, 2016: 206; Segal, 2016: 3). All three cases involved physical destruction, and all three achieved their goals by manipulating the data which controlled the operating parameters of infrastructure – a pipeline, a generator, and a nuclear reactor respectively – to make them exceed their design tolerances (*The Economist*, 2010a; Meserve, 2007; Kaplan, 2016: 206). This has been the nature of destructive cyber attacks from their inception to the present.

It is important to note, however, that despite being a destructive cyber attack which targeted data, Stuxnet is also an example of a cyber weapon which influenced the information level of the DIK paradigm. The malware could easily have been programmed to destroy every centrifuge at the Natanz reactor, however, such an action would have aroused the suspicions of the Iranian government (Kaplan, 2016: 208). Instead, it was designed to damage just enough of the infrastructure at the reactor that the scientists or equipment would be blamed for the malfunctions, causing Iran to replace functional people and infrastructure and delay their nuclear program (Kaplan, 2016: 208). As Kaplan (2016: 208) notes, "…the target wasn't just the Iranians' nuclear program but also the Iranians' confidence – in their sensors, their equipment, and themselves." In short, despite its destructive nature, Stuxnet was designed to not just affect data, but also the context in which that data was received by a human operator, i.e., information. It should be noted that transcending this divide can be expensive; Ralph Langner, one of the first cyber security experts to decode parts of the Stuxnet worm, estimated that keeping the attack hidden throughout its operation would have consumed roughly half of the total cost of developing it (Segal, 2016: 2). Overall, Stuxnet represents a rare subset of cyber attacks which is used as a tactic rather than a strategy – in this case, the overall strategic goal was to delay or halt the Iranian nuclear program – yet it also demonstrates that transcending the divide between data and information can incur considerable cost.

Despite their capacity to achieve tangible results, there are a number of reasons for destructive cyber attacks being relatively uncommon in the history of cyber war. Firstly, a destructive cyberattack tends to draw an adversary's attention to their vulnerability; as in the case of Iran – which quickly developed a respectable cyber capability – a destructive cyberattack is a powerful wake-up call, and the malware involved in its execution is often single-use only as the target (and others) will develop patches to counter it (Segal, 2016: 11-12). This is also a reason why cyber war techniques rarely proceed beyond the data level of the DIK paradigm: the constant usage of a particular exploit at the data level makes it more likely that exploit will be removed. Essentially, in breaking the glass wall, the hammer can sometimes be rendered obsolete for future uses (such as in the case of zero-days, which are patched almost instantly after they are discovered). This is not as problematic as it seems, however, as the information warrior can simply find or modify another cyber weapon.

Another important factor is the question of what an actor's overall objective is, and whether or not cyber can achieve that objective. In 2013 and 2014, for example, during its annexation of Crimea, Russia could have waged a much more damaging cyber war against Ukraine if it had so desired by targeting telecommunications or transport networks (Segal, 2016: 72-73). One plausible reason for its restraint is the fact that an all-out cyber war may have alienated the ethnic Russians and Russian speakers in Crimea whom the Kremlin was seeking to influence (Segal, 2016: 72-73). A destructive cyber attack may have fulfilled short-term Russian military objectives, however, it would also have undermined its greater strategy.

Overall, destructive cyberattacks of the 'cyber 9/11' variety are entirely possible; indeed, the fact that all the examples noted above have utilized essentially the same exploit (exceeding the device's design tolerances) is indicative of the vulnerabilities of many actors. Having said this, the fact that they have occurred so infrequently reveals a greater trend in IW in the 21st Century. Despite its destructive capacity, cyber war techniques being used for destructive purposes can potentially undermine a particular actor’s long-term goals, and in terms of broader IW campaigns, can make it more difficult for information warriors to affect the higher levels of the DIK paradigm with active measures.

Disruptive

In contrast with destructive cyber attacks – which have remained fairly consistent albeit infrequent since their inception – disruptive cyber attacks have evolved and changed in line with advances in technology. Most of the earliest cyber attacks targeted the US military, as at the time it was essentially the only actor connected to what would later become the Internet (Boot, 2007: 307). One of the earliest disruptive cyber attacks occurred in 1997 during the US military exercise known as ‘Eligible Receiver’. During the exercise, a group of hackers working for the NSA attempted to penetrate the Pentagon’s command and control systems using software and equipment available commercially (Kaplan, 2016: 57). This case is very similar to the Aurora Generator Test: not only were both designed to make the threat of a cyberattack on critical infrastructure apparent, both were also incredibly efficient, as the NSA employees needed only four days to functionally defang the US military (Kaplan, 2016: 68). Following shortly after Eligible Receiver were ‘Solar Sunrise’ and ‘Moonlight Maze’, which both occurred in 1998 and involved unauthorized access to unclassified US military networks (Kaplan, 2016: 73). In the case of the former, the perpetrators were found to be two American teenagers and an eighteen-year-old Israeli hacker calling himself ‘The Analyser’ (Kaplan, 2016: 74); the latter was traced back to Russia (Kaplan, 2016: 85). These two incidents make 1998 an important year for cyber war: not only was it the first known instance of a state penetrating another’s networks, but it was also the first time a non-state actor was found to be responsible for a cyber attack.

As the Internet became increasingly ubiquitous, and as more data became digitized, corporations also began to acknowledge the threat posed by cyber war. In 2013, the cyber security firm Mandiant published a report naming China’s People’s Liberation Army (PLA) Unit 61398 as an incredibly prodigious hacker responsible for at least 141 intrusions across twenty sectors over seven years (Kaplan, 2016: 222-223; Mandiant, 2013). The targets for these and similar attacks varied greatly, from large tech companies such as Google and Adobe (Operation Aurora) to defence contractors (Titan Rain), oil and petrochemical companies (NightDragon) and even NGOs, such as Tibetan exile centres (GhostNet) (Kim, 2012: 323). The defining characteristic of these attacks is their relative simplicity, as the infamous 'Operation Shady RAT' cyber attacks show. A RAT (Remote Access Trojan) is a piece of malware which is incredibly simple and easy to use, having been described as "…the hacker's equivalent of training wheels." (FireEye, 2013: 2) The RAT will essentially allow an intruder to "…point and click their way through the target's network…" (FireEye, 2013: 2), making it easy for an attacker with no technical knowledge to disrupt or steal from their target. All they need is a delivery system for the malware, which in this instance was a 'spear-phishing' campaign (Kaplan, 2016: 225-226).

'Phishing' describes a slew of emails being sent to random targets hoping one or more of them will open it. This is a highly prevalent strategy in IW in the 21st Century, as an estimated one in every 1,968 emails contain some form of phishing scam as of July 2017 (Symantec Security Response, 2017). This 'low-hanging fruit' tactic is indicative of the broader brute force philosophy which underpins a great deal of modern cyber war. 'Spear-phishing', on the other hand, is a much more sophisticated strategy which combines aspects of active measures with cyber's data-level manipulation. In this instance, the attacker is trying to bait a particular target who is unlikely to fall prey to a simple phishing campaign (Segal, 2016: 7). To do so, information warriors will combine psychological manipulation with cyber weapons to find their mark. The emails sent to the target are crafted to seem as though they come from someone the subject knows, and will more often than not reach their target when their concentration is at its nadir, such as first thing in the morning or just before a long weekend (Segal, 2016: 7). A spear-phishing campaign is dependent on a subject viewing information in a context which is beneficial to the attacker, thereby allowing access to the data contained within their system. This is another example of cyber war techniques influencing information rather than just data, yet in contrast with Stuxnet – where information was manipulated to keep the malware hidden – Operation Shady RAT involved manipulation of information to allow access to the data itself. This shows how cyber war and active measures can supplement each other in the pursuit of a particular goal. Also in contrast with Stuxnet, Operation Shady RAT was an unsophisticated series of cyber attacks; it did not involve any zero-days or other technical exploits, and was, as Singer & Friedman (2014: 92) suggest, “rather unremarkable.” Yet it was able to successfully penetrate 72 targets – including the UN and Olympic Committee (Kim, 2012: 323) – through a clever synthesis of IW techniques targeting both data and information, which suggests that applying the hammer and scalpel in tandem can achieve results which neither could alone.

Conclusion

In conclusion, cyber has in many ways become the ‘war’ aspect of information warfare. So much data is created and stored digitally on computers that IW techniques which target such data – namely cyber war – have become highly sophisticated. Cyber’s asymmetric nature and pinpoint accuracy make it a pernicious aspect of IW in the modern day, and past and present developments in cyber war mean that cyber weapons are extremely cost-effective and can range from sophisticated malware designed to remain hidden at all costs, to programs allowing attackers to operate within a compromised network as if it were their own. Cyber has expanded from being a niche vulnerability of the US military in the late 20th Century to a part of everyday life in the 21st, and with advances such as so-called ‘fileless malware’ and malware specifically designed to target the Internet of Things, cyber attacks will only become more sophisticated and more widespread. [10] [11]

No description of information warfare would be complete without an examination of cyber, however, so too would it be incomplete if it were limited to cyber alone. For all their sophistication, cyber weapons and cyber war techniques are limited in scope. A proliferation of digital data in the 21st Century has made them a lodestar of IW campaigns, yet they are largely limited to targeting the data level of the DIK paradigm. A cyber attack is a precise and effective means of achieving a short-term objective – such as destroying a power plant or stealing data from a

[10] A computer’s anti-virus protection and firewall are designed to protect and scan the computer’s hard drive; fileless malware avoids this area entirely, instead storing itself in the computer’s random-access memory (RAM) or its kernel (the lowest level of its operating system), making it incredibly difficult to detect (Newman, 2017).

[11] The Internet of Things (IoT) refers to the expansion of devices which are connected to the Internet, such as household appliances or ‘smart home’ technology.

corporation or government – yet when paired with techniques targeting the information level of the DIK paradigm, cyber war techniques become a far more powerful tool. Computers are only one part of the information systems which permeate the 21st Century: the other is the human mind, which is capable of taking data and information and synthesizing them into knowledge. This knowledge subsequently affects the subject's view of the world around them – including all future data and information they receive. Cyber has become a high-profile issue the world over as individuals, corporations, and governments realise their dependence on data has left them vulnerable, yet their focus on vulnerability at the data level has blinded them to IW targeting the higher levels of the DIK paradigm.

The Scalpel

Active Measures in the 21st Century

"The strain of anti-intellectualism has been a constant thread winding its way through our political and cultural life, nurtured by the false notion that democracy means that my ignorance is just as good as your knowledge."

– Isaac Asimov (1980)

"I can make them print anything."

– Alt-Right Posterchild Milo Yiannopoulos (Oehmke, 2017)

The previous chapter has argued that cyber war techniques, while immensely effective, are also quite basic in terms of IW's broad capabilities. From its inception, cyber war has been conflated with IW (Williams, 2017), which has limited the attention other forms of IW have received. The term has begun to be expanded as states and non-state actors increasingly realise that hostile foreign powers are capable of bombarding their populations with propaganda more sophisticated than any kind seen before (Zappone, 2017a). The advent of 'fake news' during the 2016 US election does not fall into the category of cyber war, yet it does represent a far more insidious form of IW: the spread of disinformation. This chapter will examine the 'scalpel' of IW in the 21st Century in the form of propaganda and disinformation, referred to as active measures.

Designed to target a population psychologically, active measures are capable of making surgical incisions into political debates surrounding contentious issues and promoting an alternative narrative designed to undermine confidence in the government or bolster a particular agenda. Actors utilising active measures are capable of bombarding their targets with propaganda or disinformation through the

Internet and social media, yet they must ensure the message they propagate is interesting or scandalous enough to be synthesised by the recipient into knowledge, thereby affecting their worldview. This is a pernicious form of IW in the 21st Century and, together with cyber war, allows the information warrior to target all levels of the DIK paradigm. This chapter will outline the effectiveness of propaganda and disinformation at targeting humans as information systems, and argue that such measures have formed an important aspect of IW in the 21st Century and, given their effectiveness, will only become more common and more sophisticated in the future.

Working from the linear conception of the DIK paradigm, this chapter will focus on the information and knowledge phases of this progression to argue that active measures designed to corrupt the knowledge a subject creates have become a priority of information warriors in the 21st Century, facilitated largely by advanced communications technology and social media. Much as cyber is effective at targeting the data and, to an extent, the information levels, so too are active measures effective at targeting the information and knowledge levels; this is because data and information are digitally stored in the 21st Century, while the information itself is synthesized by people into subjective knowledge. Hence, if an information warrior wanted to target a computer system, they would use cyber means; if they wanted to target people, they would use active measures.

This chapter will reference Russian use of propaganda and disinformation extensively. This is because Russia is a prolific user of IW in the 21st Century and, given the effectiveness of its propaganda and disinformation campaigns, is indicative of how IW can be successfully deployed in different arenas and for a number of different purposes, such as provoking social division or exacerbating conflict. As well, the effectiveness of Russia's active measures campaigns means they are likely to be emulated by others in the future, suggesting Moscow's deft use of the scalpel is indicative of future trends in IW targeting information and knowledge (Pomerantsev & Weiss, 2014: 7). The first section will examine propaganda as a form of IW, both historically and in its current iteration, as well as noted Russian use of propaganda. The second section will describe disinformation, in the form of conspiracy theories and support for anti-establishment forces, and cover Russia's use of such tactics. The third and final section will examine the way Russia has combined propaganda and disinformation in a number of theatres, including Ukraine and the United States. Overall, the aim of this chapter is to demonstrate that active measures are widely used, highly effective, and poorly understood by those they target.

This chapter will predominantly focus on the use of IW against civil society and populations, as these are the primary targets for active measures in the 21st Century. Indeed, a number of actors – such as Russia and the Islamic State – have demonstrated an understanding that a state's foreign policy can be shaped by pressures from civil society, which can in turn be influenced externally (Syuntyurenko, 2015: 205). The most obvious and available way to influence a civil society is by manipulating the media – be it traditional or social – and, given the cost-effectiveness of such techniques (Waltzman, 2017: 4; Dean, 2016: 5) this is largely what active measures in the 21st Century have become (Lopatina, 2014: 155).

Routine Surgery: Propaganda and Narrative in the 21st Century

The first set of tactics utilised in an IW campaign can broadly be defined as propaganda. These are the techniques and tools which bolster the image of one party over another, and often involve not just creating a narrative or persuading someone of something, but also crystallising already available information or knowledge within a subject's mind (Welch, 2014: 2). To do so, it uses everything from half-truths to outright lies (Welch, 2014: 2). The salience of the narratives propaganda creates – dependent on factors such as public interest, emotional appeal, and the story's sensational nature – is the key to its successful synthesis into knowledge.

Historically speaking, propaganda is nothing new. Because the Cold War was a conflict of ideology more than of military force, the ability to affect the beliefs of enemy populations was an important area of study for both the US and USSR (Nietzel, 2016: 59-60). As Ellul (1965: xvi) notes, communists believed propaganda was an incredibly potent tool in combating capitalism because the power to influence a person or population's unconscious opinions and biases correlated with the Marxist notion that the individual was less important than the society (Marx, 1972: 117). At the same time, American sociologists downplayed propaganda's effectiveness as they could not fathom that the individual, the most important actor in a capitalist liberal democracy, could be fragile enough to be persuaded by a foreign actor (Ellul, 1965: xvi).

Propaganda in the 21st Century is largely based on ideas and concepts created during the 20th Century. Yet science – particularly neuroscience and psychology – have come a long way since the Cold War. Information warriors today know more about their target audience's mind and thinking patterns than their 20th Century compatriots, and the advent of the Internet and new methods of data storage and collection have made active measures more effective and more widespread in the 21st Century. There are a number of basic understandings of the human mind which can aid the information warrior in creating a narrative or distorting reality (Paul & Matthews, 2016), namely that:

- People can't instantly judge between true and false information.
- Too much information makes people look for the quick and easy way to determine whether a message is trustworthy.
- A particular message or theme becomes more appealing the more it is heard.
- A claim which is supported by evidence – regardless of whether that evidence is true or not – is likely to be accepted by the general public.
- The illusion of objectivity can make propaganda more salient.

All these understandings of individuals' receptivity to new ideas have aided information warriors in the creation and proliferation of active measures. Yet if an actor is engaged in the dissemination of propaganda and wants its target audience to synthesise the information it receives into knowledge – as is the operational goal of any active measures campaign – it must do more than spread its propaganda prolifically and through multiple forms of media. It must also create a narrative which is salient to its target audience and which can, effectively, take on a life of its own. This is a lesson learned by information warriors more by experience than scientific discovery, as there have been a number of active measures campaigns waged in the past which have failed to take hold in the public imagination; in particular, heavy-handed Soviet attempts to influence elections in West Germany in 1983 (Weiss, 2017) and aggressive pro-Russian propaganda targeting Finnish citizens in the 21st Century (Aro, 2016: 125).

This is an example of the difference between cyber war techniques and active measures. Cyber is a blunt tool because, much like a hammer strikes a nail, repeated use of cyber war techniques such as DDoS or phishing attacks will invariably yield results. There are enough lapses in security in computer systems and the people who monitor them that striking a target repeatedly will eventually result in penetration. Active measures, however, are radically different. If a particular narrative or message is too blunt, it will be rejected by the target audience as obvious propaganda or, far more likely, too uninteresting to merit exploration. For active measures to be effective, they must be used like a scalpel: precisely and effectively. The narrative active measures create and perpetuate must be subtle and intelligent, and most importantly, it cannot have an obvious source; as Aro (2016: 126) suggests, if the message cannot be easily recognised as propaganda from a foreign source, then it is more likely to affect people psychologically.

A tactic commonly utilised in conjunction with propaganda is the disruption of narratives which might contradict the propaganda's message, often by attacking telecommunications. This is an example of cyber war being used to facilitate an active measures campaign; the use of cyber to disrupt an adversary's communication is not a strategy in and of itself, but rather a tactic used to ensure the narrative propagated by active measures achieves maximum penetration. Indeed, the Syrian government has been known to shut down Internet access in certain regions as a precursor to an attack, largely to prevent dissemination of information or images relating to the attack which might damage the state's propaganda efforts (Bradbury, 2013: 17). Similarly, during its campaign in Georgia in 2008, Russia utilised its considerable cyber war capabilities to disrupt communications from Georgian news and television channels, as well as the Georgian government (Segal, 2016: 69). This use of cyber was subservient to a greater active measures strategy: by effectively silencing Georgian media, the first images Georgians, Russians and, indeed, the outside world received of the conflict were Russian propaganda (Segal, 2016: 69). This meant that the impression audiences had of the conflict was one skewed towards Russia, and is a tactic the Kremlin has also utilised in its ongoing conflict in Ukraine (Ostrovsky, 2015: 343). Disrupting an adversary's ability to disseminate their propaganda or narrative is a key component of active measures, as such disruption essentially means the information warrior's message is the only one available. In some cases, however, disruption is unnecessary; active measures can instead be used to highlight negative aspects or embarrassing incidents, ensuring they form an inexorable part of a subject's knowledge of a state or actor.

The US's missteps in the Middle East – and subsequent loss of control of the narrative – are a perfect example of this phenomenon in action. The importance of narrative has been a decisive factor in a number of conflicts since Vietnam, where popular support dwindled as images of the brutality of America's campaign in Southeast Asia were beamed back home (Mandelbaum, 1982). Thirty years later, the US again faced a public backlash due to a number of controversies surrounding its campaign in Iraq. After a successful strategy of embedding journalists with coalition forces during the early stages of Operation Iraqi Freedom, a sequence of events which began with the revelation that Iraq had no WMDs, followed by the scandal at Abu Ghraib and the heavy-handedness of the Pentagon's campaign in Fallujah undermined the United States' narrative and tarnished its reputation not just in the global community, but among the people it was trying to influence (Boot, 2007: 413-414).

Unlike other states such as Syria and Russia, who were able to impose a media blackout on their operations and thereby avoid gruesome images or embarrassing incidents being revealed, the US military answered to a democratic government and was held accountable for its actions (Boot, 2007: 414). David Kilcullen, a noted Australian counterterrorism expert, has argued that measures taken by Western states during the Iraq War – most notably the British and American practice of 'extraordinary rendition' – tarnished the reputations of these countries, reduced the salience of their message, and allowed local grievances to fester into violent conflicts (Kilcullen, 2015: 7-8). This is an important concept when it comes to modern iterations of IW: while losing control of the narrative is not necessarily synonymous with defeat, as Max Boot (2007: 367) cannily notes, "…global indignation was one of the few things capable of stopping American air power."

Washington's missteps in the Middle East demonstrate the precise reason why Russia views soft power as zero-sum (Van Herpen, 2016: 272). Not only did the widely publicised issues the US faced in Iraq and Afghanistan – not to mention the trouble it had in justifying the invasion of Iraq based on false intelligence – lead to a devastating loss of soft power and prestige, they also created conditions beneficial for a Russian narrative to take root. An article written by Vladimir Putin for *Russia Today* (RT) in the lead-up to the 2012 Russian election outlined his worldview, which placed emphasis on the creation of trust in the international system and argued that Western actions – "…a string of armed conflicts under the pretext of humanitarian concerns…" (Putin, 2012) – had undermined this trust. This loss of narrative control by the United States has increased the salience of Russia's narrative about Western neo-imperialism disguised as concern for human rights; essentially, loss of prestige for the West makes Russia's propaganda sound more truthful.

Overall, propaganda has come a long way since the Cold War. Not only has social media made it considerably easier to disseminate propaganda to individuals, but understandings of the human mind in the 21st Century have also made it easier for information warriors to create narratives which are salient and tailored to specific audiences, saturating them with information to affect their worldview. Yet just as important as creating a coherent narrative for an active measures campaign is diminishing the salience of counter-narratives; this is either done by disrupting such narratives – possibly through cyber means – or by highlighting the negative aspects of such information. Active measures, however, are not limited to propaganda; disinformation, too, can be used to undercut the mainstream narrative and make an audience more receptive to external propaganda.

Infecting the Wound: Disinformation and Anti-Establishment Forces

Disinformation is the targeted use of half-truths, truths out of context, or outright lies to deceive a target audience, and is a particularly pernicious form of IW used in the 21st Century. Given that Russia is one of the more prolific actors in terms of IW in the 21st Century – and, indeed, the fact that the word 'disinformation' itself comes from the Russian word *dezinformatsiya* (Vershbow, 2017) – this section will focus on the Kremlin's exploitation of the concept of freedom of information to disseminate disinformation (Pomerantsev & Weiss, 2014: 6). This section will begin with an examination of three cases of disinformation causing political action to outline proven instances of active measures' effectiveness. The next subsection will explore the way conspiracy theories can corrupt the DIK paradigm and brainwash their subjects, and the final subsection will examine the ideology of 'Putinism' as it relates to

Russia’s support of anti-establishment forces as a form of IW in the 21st Century. Overall, this section will argue that by virtue of new communications technologies, disinformation has become a common and effective tactic for corrupting the DIK paradigm and infecting a subject’s knowledge creation process. .

Hearts and Minds: The Efficacy of Active Measures

The first example of disinformation at work is related to the ‘White Helmets’, a group of civil first responders in Syria. Despite their 2016 nomination for a Nobel Peace Prize (Ellis, 2017), they are often targeted by Russian and Syrian disinformation campaigns suggesting they are linked to al Qaeda (*Russia Today*, 2017). The White Helmets were initially discredited by a graphic depicting the same girl ostensibly being saved by them three times in three different months, after which the ‘one-finger salute’ they gave in a number of images and videos was erroneously linked to al Qaeda (Worrall, 2016). Interestingly, subsequent conspiracy theories surrounding the group have been propagated not just by Russia, but also by *InfoWars*, which suggested that the group was responsible for sarin gas attacks in Syria (Al-Laham, 2017). The fact that the narrative surrounding White Helmets has become contested is incredibly beneficial for Russia and Syria, as their ‘double tap’ air strike strategy – which involves striking targets twice after a brief respite – means they kill a large number of these first responders (Ellis, 2017). Were the narrative surrounding White Helmets unanimously positive, this double tap strategy could deal a serious blow to Russian and Syrian credibility, yet with the spread of disinformation, the narrative is not unanimously positive and a shred of doubt as to the White Helmets’ true purpose allows both regimes to justify their actions (Ellis, 2017).

Active measures can be used not only to provide cover for one’s actions, but also to foment political action by exploiting known issues in a particular region. In 2017, Qatar became embroiled in a diplomatic crisis with a number of its neighbours, including Saudi Arabia, the United Arab Emirates, Egypt, and Bahrain (*Al Jazeera*, 2017; Herr & Bate, 2017). One of the major causes of heightened tensions was the hack of Qatar’s state-run news agency, which involved the publication of comments made by Qatar’s emir, Sheikh Tamim bin Hamad Al Thani, which glorified Iran, Hezbollah, Hamas, and Israel (*Al Jazeera*, 2017; DeYoung & Nakashima, 2017).

Qatar categorically denied the comments and argued they had been planted as part of a dedicated smear campaign designed to slander its ruler, a position supported by senior US officials (Windrem & Arkin, 2017; DeYoung & Nakashima, 2017). Regardless of their denial, the planted information targeted known issues within the region, and demonstrates how quickly disinformation can spread – particularly when it is incendiary and sensational – and the capacity of false information to prompt political action (Herr & Bate, 2017). This incident happened at the highest levels of government and demonstrates that in the 21st Century, no one is safe from active measures.

The next example deals with controversy surrounding vaccinations, and while there is no evidence of a concerted active measures campaign in this instance, it is indicative of the effects disinformation can potentially have on a population at large. After Andrew Wakefield, a British doctor, had a paper published in the Lancet medical journal which suggested a (subsequently disproven) link between autism and a particular type of vaccination, a number of parents refused to vaccinate their children out of fear (Kelland, 2010). This refusal to vaccinate saw a surge in the number of documented cases of preventable diseases in the US, including measles, mumps, and whooping cough from 2012 to 2014 (Sifferlin, 2014). Interestingly, even after the causal link between unvaccinated children and disease outbreaks was publicised by public health officials, anti-vaccine supporters spoke out against scientists and paediatricians, suggesting they were part of a greater conspiracy (Sun, 2017). This example may not be a deliberate disinformation campaign, however, it is nevertheless indicative of the effect the scalpel can have on a population. By feeding disinformation to a subject population, their knowledge creation process can be corrupted to the point that anything or anyone who opposes it is considered a liar.

Overall, the disinformation aspect of an active measures campaign differs from propaganda; it is designed less to create support for a particular action or viewpoint than it is to cast doubt in a subject's mind as to the authenticity of the mainstream narrative. Disinformation takes data – such as the White Helmets in Syria, comments attributed to the head of Qatar, or the number of autistic children born each year – and alters the context in which they are viewed to suggest to their target audience that White Helmets are terrorists, that Qatar's emir is fond of Israel, and that vaccines cause autism. Disinformation cuts cleanly and precisely, making small incisions into its audience's knowledge of a particular subject and sowing the seeds of doubt in their mind. Yet, much like propaganda, sometimes corrupting a narrative with disinformation is not the best option. Sometimes it is better to spread conspiracies and support anti-establishment forces, thereby heightening or exacerbating social or political divides.

The Unclean Scalpel: Conspiracy Theories in the DIK Paradigm

Conspiracy theories are incredibly corrosive of the DIK paradigm, as once a conspiratorial narrative has been internalised by a subject, they are unlikely to change their views. This is a facet of knowledge creation which has been weaponised by information warriors, and has formed an important part of IW in the 21st Century. At the outset, it is important to note differing opinions on the nature and purpose of IW between Russia and the West. A Russian conceptual document defined 'information war' as, among other things, "…massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party" (NATO CCDCOE, 2011: 5). This quote explicitly links active measures with the failure of institutions and governments, yet it also indicates a fundamental disconnect between perceptions of IW between Russia and the West. As Zappone (2017a) argues, Western countries have a tendency to conflate IW with cyber warfare – focusing on the military aspect of IW – while Russia uses the terminology of the 'information space' and broadens its list of targets to the social and political (Darczewska, 2016: 14). In Russia, cyber serves to supplement active measures, and IW tactics are justified in peace or wartime (Waltzman, 2017: 4; Lucas & Pomeranzev, 2016: 5) because, in the minds of Russian policymakers, their country has been besieged by Western IW since the end of the Cold War (Putin, 2012; Yablokov, 2014: 623; Zappone, 2017a).

This mentality is not limited to obvious cases such as NATO expansion or pro-Western leaders coming to power in Ukraine (National Intelligence Council, 2017: 127). It also extends to the very conception of human rights and international law. Indeed, Vladimir Putin explicitly linked human rights with pernicious attempts at political engineering in the run-up to the 2012 Russian election (Putin, 2012); he wrote that foreign actors were levying criticism at Russia "…in a persistent effort to influence our citizens…", and that the human rights agenda had been 'privatized' by the US and its allies to create a cover for exerting pressure on its opponents (Putin, 2012). This mentality of Russia being the target of a Western conspiracy is a staple of the Russian media diet (Yablokov, 2014: 623) and traces its roots back to Lenin and Stalin, who often bolstered public support by invoking images of a Russia "…besieged by enemies abroad and traitors within" (Lo, 2015: 25).

One of the most valuable weapons Russia has in its campaign to spread disinformation through conspiracy theories is television, and among its numerous propaganda channels, *Russia Today* (RT) stands out. Formed in 2013 after the surprise liquidation by Putin of the state media agency 'RIA Novosti', RT was created as an enormous state-funded multilingual media company designed to improve Russia's image in the world (Yaffa, 2014). RT has been used by the Kremlin not just to promote its own agenda, but also to disseminate conspiracy theories which challenge the mainstream narrative or description of events (Yablokov, 2015: 301). Contrary to its stated aim, RT is designed more to undermine confidence and foster mistrust of foreign governments and media than it is to promote a good image of Russia (Kelly, 2017), and despite having little viewership or impact in the US, it is highly effective in Europe, where its alternate narrative allows the Kremlin to exert influence over its neighbours (Pomerantsev, 2014).

It is important to note that RT is broadly negative of the US, running stories related to chaos in America to contrast with strength and authority in Russia (Berger, 2017). As well, RT is noted for holding interviews with 9/11 'truthers' who argue that the September 11 terrorist attacks were perpetrated by the US government (Pomerantsev, 2014; Van Herpen, 2016: 72). Having such conspiracy theorists on a 'news' network lends their theories an air of credibility; essentially, by being acknowledged by the mainstream, they inch closer to *being* mainstream (Rutenberg, 2017). Indeed, a similar situation has occurred in the US, where the act of Fox News interviewing the head of *InfoWars*, Alex Jones, was criticised as legitimising the narratives he promotes (Rutenberg, 2017).

Conspiracy theories have largely been left by the wayside in terms of academic study (Yablokov, 2015: 301), however, this belief that conspiracies are unimportant or not worthy of attention is misguided. Fenster (2008: 84-90) has described conspiracy theories as a “populist theory of power,” an apt assessment given their role in bringing populist leaders to power in 2016 and 2017. Indeed, Faris et al.'s (2017) study demonstrates that during the 2016 US election, the sources Trump supporters tended to get their news from were generally more biased and more likely conspiratorial than those who voted for Clinton (Faris et al., 2017), and Donald Trump himself is known to have agreed with the conspiracy theories espoused by Alex Jones and *InfoWars* (Rutenberg, 2017).

This dynamic is replicated in countries such as France, Hungary, and Slovakia, where a study by Gyarfasova et al. (2013) showed that far-right party members were more likely to believe conspiracy theories than members of any other party (Pomerantsev, 2014). These conspiracies are becoming more salient because their transmission is becoming more advanced, taking a seemingly objective stance and including a number of citations and references – all of which, it should be noted, link back to other conspiracy theory websites (Aro, 2016: 125). Indeed, as Starbird’s (2017) study into retweets among conspiracy theorists showed, media companies which challenged the mainstream narrative of events – such as *InfoWars*, newsbusters.org and RT – frequently featured links to one another’s reports in an effort to justify or support their own conspiratorial narratives. Conspiracy theories are being repackaged as objective or unbiased information, thereby polluting the DIK paradigm for all those who consume them.

Overall, this suggests an increase in the salience of conspiratorial narratives, which operates in favour of those utilising active measures. Conspiracy theories are incredibly useful to the spread of disinformation; as Sunstein & Vermeule (2008: 7) note in their study, the underlying trend with conspiracy theories is a creeping distrust of any institution which produces knowledge. As the conspiracy theory rejects the mainstream narrative -- by, say, suggesting that the 9/11 terrorist attacks were committed by the US -- then it perceives those who spread the mainstream narrative as either being a party to it or too ignorant to fathom the truth. Dmitry Kiselev, the former head of RT, perfectly summed up this sentiment when he told a co-worker during an argument "...you simply don't understand anything" (Yaffa, 2014). Any attempt to sway them from this belief is considered to be either the response of an ignorant person or a concerted effort by someone who is in on the conspiracy. This skeptical mindset is incredibly valuable to the modern information warrior, as when the conspiracy theory is synthesised from data and information into knowledge, it creates the impression that the subject knows better than everyone else; they become unreceptive to narratives emanating from mainstream media or experts (Sunstein & Vermeule, 2008: 7), which means their beliefs cannot be disproven. Information warriors spreading disinformation operate with unclean scalpels, infecting their targets with disinformation to corrupt the DIK paradigm and make them internalise a false narrative.

Conspiracy theories are an important aspect of IW in the 21st Century, and Russia's focus on this particular brand of disinformation makes it a valuable case study. The Russian state does not simply lie or cheat, it actively recreates its version of reality which is filtered through 'news' agencies such as RT, creating "mass hallucinations" which then correlate with political action (Pomerantsev, 2014). Moscow's experience with half-truths and truths bereft of context has allowed it to perpetrate an incredibly sophisticated disinformation campaign (Fattibene, 2016: 134) which Western countries are woefully unprepared to combat (Czuperski, 2016: 9). With a tremendous increase in the amount and variety of information available, it can be difficult for individuals and groups alike to judge what information is trustworthy (Paul & Matthews, 2016). This is a fundamental flaw in the DIK paradigm which information warriors exploit. Disinformation – especially when fed to a subject by social media and search engine algorithms designed to show them only what they want to see – can poison the subject's mind and not only make them believe things which are not true, but cause them to rally (sometimes violently) for political action based on erroneous claims.

Multiple Incisions: Putinism and Anti-Establishment Forces

During the 2016 US election, Russian-purchased advertisements appearing on Facebook and Twitter played both sides of socially or politically divisive issues such as Black Lives Matter (Entous et al., 2017; Romm & Molla, 2017). These ads were designed to exaggerate social divisions, exacerbate tensions between politically opposed groups, and, as Senator Mark R. Warner (D-VA.) suggests, to "…sow chaos" (Entous et al., 2017). Not only is this perfectly in line with Russia's conception of IW as a tool to destabilise societies (NATO CCDCOE, 2011: 5), but it also echoes the narrative that RT perpetuates of a United States tearing itself apart at the seams (Berger, 2017).

Support for anti-establishment forces is not a new phenomenon by any means – the Cold War is replete with examples of the USSR supporting Leftist groups and the US supporting their capitalist opponents – yet what has changed in the 21st Century is the idea of one party playing both sides of the political divide for no other reason than to create division. In the past the goal of such actions was to install a party or candidate favourable to a particular side of the ideological divide, yet today Russia supports anti-establishment forces simply to undermine confidence in the society and the government of which they are a part. This corrupts the DIK paradigm by making people internalise division within their society as part of everyday life; in short, citizens of the US believe their country is tearing itself apart because the impact of anti-establishment forces is embellished. In order to understand how Russian support for anti-establishment forces operates – and in keeping with the notion that the Kremlin’s use of active measures is indicative of the future of IW (Pomerantsev & Weiss, 2014: 7) – it is important to examine the ideology of ‘Putinism’.

The ideology of Putinism is simultaneously fluid and solid. It is best conceptualised as Vladimir Putin’s attempt to solidify his control over Russia, which began in the wake of protests against his rule in 2011 (Zakaria, 2014). It is not an ideology per se, but more a collection of values which are hallmarks of Putin’s view of the world, such as nationalism, social conservatism, religion, Russian exceptionalism, and a belief that the West is steadily encroaching on Russia (Yaffa, 2014; Zakaria, 2014). Most importantly, one of Putinism’s key tenets is the idea that ‘human rights’ and ‘democracy’ are fraudulent and that the West has fallen into a liberal decadence of its own making (Eltchaninoff, 2017), a line echoed by anti-establishment groups throughout the Western world (Oehmke, 2017). In contrast with the USSR, which hijacked ideas of ‘democracy’ and ‘human rights’ to justify their polar opposites, Putinists in modern Russia make no such efforts, instead implying that not even the West truly believes in these values (Pomerantsev & Weiss, 2014: 5). This is why the United States’ mistakes in the Middle East – including its enhanced interrogation and extraordinary rendition programs, both of which are violations of human rights – have proven so costly. Not only has Washington’s soft power been diminished, but it has increased the salience of Putinism as a way of viewing the international order.

Putinism presents a unique challenge to any attempting to combat it precisely because it simultaneously stands for nothing and everything. Putinism as it exists in Russia is authoritarianism disguised as democracy; it involves the creation of fake political parties which represent paragons of a particular ideology or belief, and then having these ‘parties’ conflict with one another, presenting the illusion of choice. Or, as Pomerantsev (2014) suggests, “…instead of simply oppressing opposition…it climbs inside all ideologies and movements, exploiting them and rendering them absurd.” It is the same logic which allowed a former Kremlin elite, Vladislav Surkov, to sponsor festivals dedicated to cutting-edge and provocative art in Moscow, then support Orthodox fundamentalists who attacked the exhibitions (Pomerantsev, 2014). The goal here was not to see one or other side victorious, but simply to ensure any and all political movements were created under the watchful eye of Russian elites; by owning all political discourse, no matter how extreme, the Kremlin ensures it cannot lose control.

As an approach to public diplomacy, Putinism allows a great deal more freedom than older Cold War techniques. Unlike communism or capitalism, Putinism has no overriding ideology to govern it (Yablokov, 2015: 312); this allows it to support not just leftists, but anti-establishment forces on both sides of the political divide (Pomerantsev & Weiss, 2014: 6). Putinism is essentially a lesson in contradiction; everything which falls under Putinism's umbrella – from censoring information online but providing the founder of WikiLeaks free reign, to siding with the Occupy movement and lambasting corporate greed while simultaneously running one of the most corrupt countries in the world – is a paradox, and this is exactly why it is popular with anti-establishment groups on both sides of the political divide, from anarchists to neo-Nazis (Pomerantsev & Weiss, 2014: 6). As Michael Weiss so eloquently puts it, "Putinism is whatever they want it to be" (Pomerantsev & Weiss, 2014: 5). As a form of IW, Putinism has proven very successful; one need look no further than the rise of the alt-right and anti-globalists or the current backlash against ‘elites’ which, in true Putinist form, is paradoxically led by some of the wealthiest and most highly-educated people in the world (*The Economist*, 2016).

Yet Putinism, anti-establishment forces, and active measures more broadly do have a natural counter, in the form of journalists and experts. Despite social media's decrease of the influence of experts and journalists (Faris et al., 2017: 17; Ojala et al., 2016: 3; Waltzman, 2017: 1-2) these groups are still pivotal to countering disinformation campaigns. They are the members of a society most likely to uncover an active measures campaign, as they are trained to think critically. As well, they will do their utmost to publicly oppose and debunk disinformation. Propaganda and disinformation cannot operate in the light, as the DIK paradigm cannot be influenced if the subject is aware they are being manipulated (Aro, 2016: 126). This is likely why journalists and experts who discover active measures campaigns quickly become the targets of another incredibly successful 21st Century IW tactic: trolling (Aro, 2016: 123; Nimmo et al., 2017).

Trolls fall into the category of 'anti-establishment forces', as they are often utilised to spread a false narrative widely (Aro, 2016: 123). Yet their true value lies in their ability to harangue and harass those who oppose the Kremlin's narrative (Pomerantsev & Weiss, 2014: 6). Jessikka Aro is one case of such activities: a Finnish journalist who publicised the existence of a Russian-backed troll factory, she immediately faced a concerted backlash and hate campaign spawned by Internet trolls (Aro, 2015). As well, the Atlantic Council's Digital Forensic Research (DFR) Lab, designed to combat disinformation online, was targeted by what a number of its correspondents concluded was a pro-Russian botnet of trolls designed to discredit and intimidate the staff at the organisation (Nimmo et al., 2017). Even the crude and crass remarks which are hallmarks of Internet trolling are used succinctly and effectively by 21st Century information warriors. In this case, the scalpel is designed to reduce the salience of journalists and experts in society, discrediting reliable sources of information by sowing doubts about their loyalties and personal lives.

Overall, disinformation in 21st Century IW can affect every level of the society and state, and can take multiple forms including conspiracy theories and anti-establishment forces. Yet regardless of the level it influences or the form it takes, disinformation has proven incredibly effective at corrupting the DIK paradigm. The normal progression from information to knowledge can be hijacked by a skilled information warrior, who plants seeds of doubt in a subject's mind and then repeatedly reinforces this new narrative by recycling it through different television programs, social media feeds, and websites. Russia – based on the capability and effectiveness of its active measures campaigns – can be considered a progenitor of future trends in IW in the 21st Century (Pomerantsev & Weiss, 2014: 7), and the ideology of Putinism is a useful basis to understand how disinformation operates in the modern world.

The Operating Theatre: Russian IW in Action

To demonstrate how dangerous and effective propaganda and disinformation can be when used in concert, this section will examine Russian active measures campaigns centring on Russian speakers outside Russia, the conflict in Ukraine, and Donald Trump Jr.'s supposed meeting with Russian agents during the 2016 US election. Through this examination, it becomes apparent that active measures are an incredibly potent form of IW in the 21st Century, and unlike cyber war – whose effectiveness is unparalleled but within a limited scope – active measures can be applied in more diverse ways, affecting the higher levels of the DIK paradigm to stoke social divisions, promote nationalist sentiment, or even encourage distrust of and violence against governments.

A common theme in Russian active measures campaigns is the decline of Russian speakers outside of Russia. This is a tactic used by Russia to invoke nationalistic and patriotic sentiments in Russians and create the impression that Russian speakers are persecuted by foreign governments (Putin, 2012). Interestingly, the Russian government's actions in relation to these diasporas – including in Ukraine – are not designed to promote integration or present Russia as a cooperative member of the international community, but rather to sow distrust and publicise Russia's expansionary ambition (Kivirahk, 2010). This prompts suspicion of Russian-speaking groups by their governments, which makes these disaporas feel persecuted and solidifies their ties to a Russia which portrays itself as their defender (Kivirahk, 2010). This promotion of persecution is an IW tactic Russia shares with ISIS, which prompts lone wolves to attack their home countries in an effort to make Muslims feel persecuted, thereby prompting them to support the Islamic State (Dearden, 2017).

As well as bolstering support for Russia among such communities, narratives focusing on Russian speakers can often undermine confidence and promote distrust of governments. In one instance, after Russian-language channels broke the story that a 13-year old Russian-German girl named Lisa had been raped by migrants in Germany, the narrative was picked up by mainstream German media before it could be debunked by authorities (Standish, 2017). After it was eventually disproven, the narrative shifted from ‘young Russian speaker raped’ to ‘German government covers up rape’, perpetuated both by the Russian media and Sergey Lavrov, Russia’s Foreign Minister (Nechepurenko & Smale, 2016). Not only did this promote conspiratorial thinking, it also bolstered anti-establishment forces in the form of anti-immigrant groups, who quickly protested in large numbers (Standish, 2017). The ‘Lisa Story’ is considered to be a paragon of Russian disinformation in action; it spread quickly, targeted a known issue in the region, and was synthesised into knowledge by its recipients faster than it could be debunked.

Focusing the narrative on a Russian speaker is a common tactic for the Kremlin, as in addition to undermining confidence in the country it has targeted, it is also guaranteed to stoke nationalist sentiment within Russia. In 2012, in an article for RT, Vladimir Putin explicitly linked protection of the rights of citizens abroad with respect for one’s country (Putin, 2012). The protection of Russian speakers outside Russia has formed a lodestar of Russian IW and disinformation, and the ‘Lisa Story’ in Germany was also mirrored in Finland, where Finnish forces were accused by Russian media of discriminating against Russian-Finnish citizens and abducting Russian-speaking Finnish children (Rosendahl & Forsell, 2016). Again, as well as promoting a conspiratorial narrative and promoting distrust of governments, these disinformation operations also stoke nationalist sentiment in Russia and faith in the Russian government. Russian people synthesise this disinformation into a worldview where Moscow fights for the rights of institutionally persecuted Russian-speakers abroad.

This focus on Russian speakers is a tactic the Kremlin has brought to its ongoing involvement in Ukraine, which has become a litmus test for a new and incredibly effective kind of IW in the 21st Century (Ojala et al., 2016: 2). Indeed, the Ukraine conflict was referred to in 2014 by US Gen. Philip Breedlove, formerly NATO’s top commander, as “the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare” (Pomerantsev, 2014; Peterson, 2017). Arkady Ostrovsky, the former Russia and Eastern Europe editor for *The Economist*, characterises the war in Ukraine as the first which was waged purely for narrative purposes (Ostrovsky, 2015, 343). The author notes that "…never before have wars been conducted and territory gained primarily by means of television and propaganda. The role of the military was to support the picture" (Ostrovsky, 2015: 343).

Russian IW in Ukraine represents one of the most concise and successful uses of the scalpel in operation in the 21st Century. During the war, Russian television and news programs provided on-the-ground coverage double the length of their usual programming, with Ukrainian forces portrayed as fascists and Russians as heroes (*Reuters*, 2014; Ostrovsky, 2015: 345). Indeed, a Ukrainian woman who appeared on Russian television and told the harrowing story of how her young son was brutally crucified by Ukrainian soldiers created an uproar in Russia, despite the fact that it was fake (Van Herpen, 2016: 4-5). Similarly, the marching of Ukrainian prisoners of war (POWs) – aggressively referred to as 'fascists' or 'Nazis' – through separatist strongholds in 2015 was designed to be reminiscent of the end of WWII, when German prisoners were marched through Red Square in Moscow (Peterson, 2017). Instances such as this are designed to create and support a narrative of pro-Ukraine forces as fascists and pro-Russia forces as heroes.

Demonisation of enemies and lionisation of friendly forces has a long history in warfare, however, the new ways in which this tactic is employed are indicative of the state of IW in the 21st Century. Labelling one's adversaries as 'fascists', in addition to being a useful propaganda tool, is also a helpful distraction (Yuhas, 2014). Exploring the truth behind claims that Ukrainian pro-government forces are 'fascist' still requires engagement with this disinformation, and, as Yuhas (2014) suggests, "…any discussion of fascists at all is a Kremlin win." As noted above, conspiracy theories become more dangerous the more they are discussed (Rutenberg, 2017), as by engaging with such narratives they slowly become more mainstream and influence more people, corrupting the DIK paradigm.

As well as acting as a distraction, demonisation of enemies through television and social media has allowed the Russian government to target the Ukrainian public directly and involve them in the conflict (Ostrovsky, 2015: 343). As Timothy Snyder (2014) suggests, "Propaganda is…not a flawed description, but a script for action."

Russian propaganda convinced many disenfranchised people in Ukraine – from poorly paid coal miners to former Soviet soldiers – that they could be heroes, while disinformation was used to promote the image of the Ukrainians as 'fascists' who had to be opposed (Ostrovsky, 2015: 344). A large number of native Ukrainians -- many of whom were unable to access Ukrainian TV and news, relying on Russian television for information – became separatists and fought against the Ukrainian army, thoroughly convinced by Russian propaganda that they were fighting for the right cause (Peterson, 2017). In Ukraine, Russia has brought propaganda and disinformation into the 21st Century and wielded them with tremendous effectiveness, using the two in tandem to convince disenfranchised Ukrainians to oppose their own government.

While narratives regarding the persecution of Russian speakers have proven effective in Eastern Europe, in targeting Western countries – such as the United States – a far more precise and insidious narrative is necessary. The situation, as described by American media, involves Donald Trump's son, Donald Trump Jr., meeting with a 'Russian government attorney' who promised him disparaging information on his father's political opponent, Hillary Clinton (Helderman & Wagner, 2017). Daniel Hoffman, a retired CIA case officer who covered Russia, argued that sophisticated Russian intelligence tradecraft would never have allowed communication over a medium as insecure as email and a meeting with agents with such obvious links to the Kremlin (Kelly, 2017). Rather, Hoffman argues, this would fall under the purview of an 'influence operation', a form of psychological warfare designed to influence a population's thinking (Armstead, 2004: 148-149). In this case, the influence operation was one that was designed to be discovered (Hoffman, 2017).

Current trends in Russian IW – including the synthesis of propaganda and disinformation – lend credence to Hoffman's narrative. Acting overtly is not the Russian way, but creating a narrative involving half-truths which is designed to spread quickly and cast doubt on a government's ability to serve its citizens is textbook Russian IW. In this regard, the influence operation has already achieved its goal; the Donald Trump Jr. meeting has caused chaos within the American political system, involving the media, FBI, and Congress, and most importantly, has fomented distrust of and undermined confidence in the US government (Hoffman, 2017).

Conclusion

Information warfare in the 21st Century is defined not just by cyber war, but also by active measures in the form of propaganda and disinformation. While cyber war is an incredibly effective tool, it is nevertheless relegated to the data level, as a cyberattack will rarely, if ever, change the way people perceive the world. Active measures, on the other hand, target the information and knowledge levels of the DIK paradigm, altering the way people understand the world. As such, they pose a far greater and more complex threat than cyber war. This chapter has argued that active measures are very much indicative of future trends in information warfare, with Russian use of propaganda and disinformation providing an insight into expansions in the field of active measures in the 21st Century and providing a template of how such measures might be used in the future.

These active measures are only set to become more complex and more widespread. As more revelations about the 2016 US election surface – such as Russian agents' use of social media networks to organise anti-immigrant rallies (Gilbert, 2017) or fake news in the form of conspiracy theories and support of anti-establishment forces (Starbird, 2017) – it becomes apparent that democratic Western states face a unique threat in active measures. As technology outpaces human understanding, and as advances in telecommunications increase connectivity, it becomes easier for messages propagated by external actors to be synthesised from information into knowledge. Henry Kissinger has argued that the more information we have access to, the less likely we are to create usable knowledge from it (Kissinger, 2014, 349-351); when every problem has a solution online, nothing needs to be scrutinised or placed into its proper context. Against this backdrop, with two thirds of Americans now getting their news from social media (Wagner, 2017), information warriors take up their scalpels and go to work.

Conclusion

"The orator need have no knowledge of the truth about things; it is enough for him to have discovered a knack of convincing the ignorant that he knows more than the experts."

– Socrates (Plato, 1960: 287)

"[Information warfare] is a war without shadows."

– Floridi, 2014: 318

This thesis has argued that IW in the 21st Century manifests in one of two ways: as the hammer or the scalpel. The hammer is cyber war, which bluntly and repeatedly strikes the data upon which our modern world is based. The scalpel is active measures, which deftly and precisely create and undermine narratives through propaganda while simultaneously corrupting the information and knowledge of a particular society through disinformation. The first chapter of this thesis has delved into cyber war, exploring conceptions of and actors in cyberspace, the nature of cyber weapons, and trends in destructive and disruptive cyber attacks. Overall, while immensely effective, cyber war is also limited in terms of its influence on the DIK paradigm; while data is an important aspect of the paradigm, and cyber is incredibly effective at targeting the data level, it will rarely venture beyond cyberspace and begin to influence users in the real world.

The second chapter has explored the combination of propaganda and disinformation – referred to as active measures – which present fundamental challenges to the information and knowledge levels of the DIK paradigm. Active measures are used by skilful operators to corrupt the knowledge creation process, either creating a narrative conducive to a particular actor or spreading disinformation to sow distrust of governments and exacerbate social divides. Overall, this thesis is simply a piece of information; it has collated data collected and contextualised by others into one cohesive source, whose aim is to assist the reader’s creation of knowledge, thereby influencing their worldview in some small way. This is a necessity in the modern world, as too few people understand the data-driven underpinnings of information they receive, and even fewer are prepared to critically examine that information when creating knowledge from it.

A noted limitation of this thesis, given its asides and references to the 2016 US election, is that this event was not explored further. While it has touched upon the election of Donald Trump as President, this thesis has generally mentioned it in passing and given it little attention (despite calling it a ‘benchmark’ of IW in the 21st Century in the introduction). At the time of submission of this thesis, ongoing investigations into the 2016 US election are continually unearthing new details of Russia’s involvement (Boot, 2017; Entous et al., 2017; Romm & Molla, 2017). Rather than attempt to remain ahead of such revelations, this thesis has instead attempted to outline how Russian active measures operate, thereby helping the reader better understand how the DIK paradigm can be manipulated or corrupted in the information age.

Together, cyber war and active measures define IW in the 21st Century, as they affect every level of the DIK paradigm. Cyber war is wielded as a hammer against data by individuals and organisations the world over, smashing against each other’s security in the knowledge they will eventually break through. Active measures are wielded as a scalpel against information and knowledge by skilled operators, making small, calculated incisions hoping to subtly influence their subject’s mind or poison their worldview. Which of the two is more dangerous is entirely in the eye of the beholder, as it depends on what individuals, groups, and entire nations now and in the future value more: data, information, or knowledge.

References

'A cyber-missile aimed at Iran?', (2010b) *The Economist*, published online September 24 2010, accessed July 26 2017, <https://www.economist.com/blogs/babbage/2010/09/stuxnet_worm>.

Al-Laham, M., (2017) ‘Report: Soros-linked group behind chemical attack in Syria’, *InfoWars*, published online April 5 2017, accessed September 28 2017, <https://www.infowars.com/report-soros-linked-group-behind-chemical-attack-in-syria/>.

Alexander, A., (2017) 'How to fight ISIS online', *Foreign Affairs*, published online April 7 2017, accessed August 8 2017, <https://www.foreignaffairs.com/articles/middle-east/2017-04-07/how-fight-isis-online>.

Armstead, L., (2004) *Information Operations: Warfare and the Hard Reality of Soft Power*, Washington DC: Brassey's Inc.

Aro, J., (2015) 'My year as a pro-Russia troll magnet: international shaming campaign and an SMS from dead father', *Kioski*, published online November 9 2015, accessed August 17 2017, <http://kioski.yle.fi/omat/my-year-as-a-pro-russia-troll-magnet>.

Aro, J., (2016) 'The cyberspace war: propaganda and trolling as warfare tools', *European View*, Vol. 15, pp. 121-132.

Arquilla, J., & Ronfeldt, D., (1993) 'Cyberwar is coming!', *Comparative Strategy*, Vol. 12, No. 2, pp. 141-165.

Asimov, I., (1980) ‘A cult of ignorance’, *Newsweek*, Vol. 19, available at <http://aphelis.net/wp-content/uploads/2012/04/ASIMOV_1980_Cult_of_Ignorance.pdf>.

‘Assad: Oscar-feted White Helmets are part of Al-Qaeda’, (2017) *Russia Today*, published online March 20 2017, accessed September 27 2017, <https://www.rt.com/news/381542-white-helmets-al-qaeda-members/>.

Barojan, D., (2017) ‘Hoax hits tragedy in Las Vegas’, *Medium: Digital Forensic Research (DFR) Lab*, published online October 6 2017, accessed October 12 2017, <https://medium.com/dfrlab/hoax-hits-tragedy-in-las-vegas-200390c64b0f>.

Berger, J.M., (2017) 'Here's what Russia's propaganda network wants you to read', *Politico*, published online August 23 2017, accessed September 11 2017, <http://www.politico.com/magazine/story/2017/08/23/russia-propaganda-network-kremlin-bots-215520?cmpid=sf>.

‘BlackEnergy APT attacks in Ukraine’, *Kaspersky Lab*, accessed August 10 2017, <https://www.kaspersky.com.au/resource-center/threats/blackenergy>.

Boisot, M., & Canals, A., (2004) ‘Data, information and knowledge: have we got it right?’, *Journal of Evolutionary Economics*, Vol. 14, pp. 43-67.

Boot, M., (2007) *War Made New: Weapons, Warriors, and the Making of the Modern World*, London: Gotham Books.

Boot, M., (2017) ‘Russia has invented social media blitzkrieg’, *Foreign Policy*, published online October 13 2017, accessed October 16 2017, <http://foreignpolicy.com/2017/10/13/russia-has-invented-social-media-blitzkrieg/>.

Bradbury, D., (2013) 'Information warfare: a battle waged in public', *Computer Fraud and Security*, June 2013, pp. 15-18.

Bradley, O.M., (1948) *An Armistice Day Address*, delivered November 10 1948, Boston, Massachusetts, transcript available at <http://www.opinionbug.com/2109/armistice-day-1948-address-general-omar-n-bradley/>.

'Brainwashing', (1976) *Psychological Perspectives*, Vol. 7, No. 1, pp. 5-8.

Brooking, E.T., (2015) 'Anonymous vs the Islamic State', *Foreign Policy*, published online November 13 2015, accessed August 8 2017, <http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/>.

Burns, W.J., & Cohen, J., (2017) 'The rules of the brave new cyberworld', *Foreign Policy*, published online February 16 2017, accessed July 4 2017, <https://foreignpolicy.com/2017/02/16/the-rules-of-the-brave-new-cyberworld/?utm_content=buffer94c61&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer>.

Byman, D., (2016) ''Death solves all problems': the authoritarian model of counterinsurgency', *Journal of Strategic Studies*, Vol. 39, No. 1, pp. 62-93.

Chuanying, L., (2016) ‘China’s emerging cyberspace strategy’, *The Diplomat*, published online May 24 2016, accessed August 9 2017, <http://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/>.

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

Coleman, G., (2015) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, London: Verso Press.

'Cyberwarfare: war in the fifth dimension', (2010a) *The Economist*, published online July 1 2010, accessed July 19 2017, available at <http://www.economist.com/node/16478792/>.

Czuperski, M., (2016) 'Confronting Putin's hybrid wars in an engagement age', *Hampton Roads International Security Quarterly*, Vol. 16, No. 1, pp. 9-13.

Darczewska, J., (2016) *Russia’s Armed Forces on the Information War Front*, Centre for Eastern Studies, No. 57, accessed September 27 2017, available at <https://www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf>.

Dean, S.E., (2016) '(Dis-)Information age warfare: countering ISIS, Putin & Co.', *Hampton Roads International Security Quarterly*, Vol. 16, No. 1: 5.

Dearden, L., (2017) 'Donald Trump immigration ban: most ISIS victims are Muslims despite President's planned exemption for Christians', *The Independent*, published online January 28 2017, accessed September 4 2017, <https://www.independent.co.uk/news/world/americas/donald-trump-muslim-ban-immigration-visas-refugees-syria-iraq-terrorism-isis-attacks-most-victims-a7550936.html>.

Denning, D.E., (1999) *Information Warfare and Security*, New York: Addison-Wesley.

DeYoung, K., & Nakashima, E., (2017) 'UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence officials', *The Washington Post*, published online July 16 2017, accessed September 12 2017, <https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.6b6a86edde3d>.

Ellis, E.G., (2017) 'Inside the conspiracy theory that turned Syria's first responders into terrorists', *WIRED Magazine*, published online April 30 2017, accessed September 28 2017, <https://www.wired.com/2017/04/white-helmets-conspiracy-theory/>.

Ellul, J., (1965) *Propaganda: The Formation of Men's Attitudes*, New York: Vintage Books.

Eltchaninoff, M., (2017) 'What is Putinism?', *The Huffington Post*, accessed September 17 2017, <http://www.huffingtonpost.com/entry/what-is-putinism_b_8624088.html#>.

Entous, A., Nakashima, E., & Miller, G., (2016) 'Secret CIA assessment says Russia was trying to help Trump win White House', *The Washington Post*, published online December 9 2016, accessed July 9 2017, <https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.baeba6757abf>.

Entous, A., Timberg, C., & Dwoskin, E., (2017) ‘Russian operatives used Facebook ads to exploit America’s racial and religious divisions’, *The Washington Post*, published online September 25 2017, accessed September 28 2017, <https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html?tid=sm_tw&utm_term=.35b6c20c9201>.

Faiola, A., (2017) 'As Cold War turns to Information War, a new fake news police combats disinformation', *The Washington Post*, published online January 22 2017, accessed August 17 2017, <https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html?utm_term=.d64a6660733a&wpisrc=nl_draw&wpmm=1>.

Faris, R.M., Roberts, H., Etling, B., Bourassa, N., Zuckerman, E., & Benkler, Y., (2017) *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 US Presidential Election*, Berkman Klein Center for Internet & Society Research Paper, accessed August 24 2017, available at <https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf?sequence=5>.

Fattibene, D., (2016) 'Information warfare: a new pillar of Russia's foreign policy', *The International Spectator*, Vol. 51, No. 4, pp. 134-136.

Fenster, M., (2008) *Conspiracy Theories: Secrecy and Power in American Culture*, Minneapolis, MN: University of Minnesota Press.

FireEye, (2013) *Poison Ivy: Assessing Damage and Extracting Intelligence*, published online August 21 2013, accessed July 27 2017, available at <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf>.

Galula, D., (1964) *Counterinsurgency Warfare: Theory and Practice*, New York: Praeger.

Gibbs, S., (2016) 'Facebook developed secret software to censor user posts in China, report says', *The Guardian*, published online November 24 2016, accessed August 8 2017, <https://www.theguardian.com/technology/2016/nov/23/facebook-secret-software-censor-user-posts-china>.

Gilbert, D., (2017) 'Russia used Facebook to organize anti-immigrant rallies in US', *Vice News*, published online September 12 2017, accessed September 15 2017, <https://news.vice.com/story/russia-used-facebook-to-organize-anti-immigrant-rallies-in-u-s?utm_source=vicenewsfb>.

Goldman, J., (2006) *Words of Intelligence: A Dictionary*, Maryland: Scarecrow Press, : 91-92.

Goodin, R.E., (2010) *The Oxford Handbook of International Relations*, Oxford: Oxford University Press.

GReAT (Kaspersky Lab's Global Research and Analysis Team), (2017) 'From BlackEnergy to ExPetr', *Securelist*, published online June 30 2017, accessed August 10 2017, <https://securelist.com/from-blackenergy-to-expetr/78937/>.

Gyarfasova, O., Kreko, P., Meseznikov, G., Molnar, C., & Morris, M., (2013) *The Conspiratorial Mindset in an Age of Transition: Conspiracy Theories in France, Hungary and Slovakia - Survey Results*, Combating Anti-Semitic Conspiracy Theories as Tools for Extremist Political Mobilization (Research, Awareness Raising and Education), available at <http://www.ivo.sk/7296/en/news/conspiratorial-mindset-in-the-age-of-transition>.

Hague, B., (2017) ''Every country should have a cyber war': what Estonia learned from Russian hacking', *Defense One*, published online August 14 2017, accessed August 16 2017, <http://www.defenseone.com/technology/2017/08/every-country-should-have-cyber-war-what-estonia-learned-russian-hacking/140217/?oref=DefenseOneFB&utm_content=buffer73a2c&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer>.

Healey, J., (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, USA.

Helderman, R.S., & Wagner, J., (2017) 'Donald Trump Jr. Was told campaign meeting would be with 'Russian government attorney,' according to emails', *The Washington Post*, published online July 11 2017, accessed September 10 2017, <https://www.washingtonpost.com/politics/donald-trump-jr-was-told-campaign-meeting-would-be-with-russian-government-lawyer-according-to-emails/2017/07/11/70b957e2-664c-11e7-9928-22d00a47778f_story.html?hpid=hp_hp-top-table-main_russiatrump-1135am%3Ahomepage%2Fstory&tid=a_inl&utm_term=.b44cac6490b6>.

Herr, T., & Bate, L.K., (2017) 'The Iranian cyberthreat is real', *Foreign Policy*, published online July 26 2017, accessed July 31 2017, <https://foreignpolicy.com/2017/07/26/the-iranian-cyberthreat-is-real/>.

Hey, J., (2004) ‘The data, information, knowledge, wisdom chain: the metaphorical link’, *Intergovernmental Oceanographic Commission Paper 26*, available at <http://inls151f14.web.unc.edu/files/2014/08/hey2004-DIKWchain.pdf>.

Higgins, K.J., (2017) 'Hacking the state of the ISIS cyber caliphate', *Dark Reading*, published online July 6 2017, accessed August 8 2017, <http://www.darkreading.com/perimeter/hacking-the-state-of-the-isis-cyber-caliphate-/d/d-id/1329293>.

Hoffman, D., (2017) 'The Russians were involved. But it wasn't about collusion.', *The New York Times*, published online July 28 2017, accessed August 19 2017, <https://www.nytimes.com/2017/07/28/opinion/the-russians-were-involved-but-it-wasnt-about-collusion.html>.

Hutchinson, W., & Warner, M., (2001) 'Principles of information warfare', *Journal of Information Warfare*, Vol. 1, No. 1, pp. 1-7.

'Is North Korea innocent?', (2014) *The Economist*, published online December 30 2014, accessed August 8 2017, <https://www.economist.com/news/united-states/21637402-america-was-too-quick-blame-north-korea-hack-attack-sony-kim-jong-un>.

Kan, P.R., (2013a) 'Cyberwar in the underworld: Anonymous versus Los Zetas in Mexico', *Yale Journal of International Affairs*, Vol. 8, No. 1, pp. 40-51.

Kan, P.R., (2013b) 'Cyberwar to wikiwar: battles for cyberspace', *Parameters*, Vol. 43, No. 3, pp. 111-118.

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

Kaplan, R.D., (2007) 'A historian for our time', *The Atlantic*, accessed 8/05/17, available at <https://www.theatlantic.com/magazine/archive/2007/01/a-historian-for-our-time/305562/>.

Kelland, K., (2010) ‘Lancet retracts paper linking vaccine to autism’, *The Washington Post*, published online February 3 2010, accessed October 13 2017, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/02/AR2010020203480.html?hpid=moreheadlines&tid=a_inl>.

Kelly, M.L., (2017) 'Cover lifted, a CIA spy offers his take on Trump and Russia', *NPR*, published online August 8 2017, accessed August 19 2017, <http://www.npr.org/2017/08/08/542106975/cover-lifted-a-cia-spy-offers-his-take-on-trump-and-russia>.

Kilcullen, D., (2015) ‘Blood year: terror and the Islamic State’, *Quarterly Essay*, Issue 58, pp. 1-99.

Kim, W., (2012) 'On cyberwarfare', *International Journal of Web and Grid Services*, Vol. 8, No. 4, pp. 321-334.

Kissinger, H., (2014) *World Order*, New York: Penguin Press.

Kivirahk, J., (2010) 'How to address the 'humanitarian dimension' of Russian foreign policy?', *Diplomaatia*, No. 90, International Centre for Defence Studies, Tallinn.

Kramer, A.E., & Perlroth, N., (2012) 'Expert issues a cyberwar warning', *The New York Times*, published online June 3 2012, accessed July 20 2012, <http://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html>.

Kshteri, N., (2014) 'Cyberwarfare in the Korean Peninsula: asymmetries and strategic responses', *East Asia*, Vol. 31, pp. 183-201.

Leslie, I., (2012) 'The uses of difficulty', *1843 Magazine*, published online November/December 2012, accessed September 20 2017, <https://www.1843magazine.com/content/ideas/ian-leslie/uses-difficulty>.

Lin, P., Allhoff, F., & Rowe, N.C., (2012) 'War 2.0: cyberweapons and ethics', *Communications of the ACM*, Vol. 55, No. 3, pp. 24-26.

Liff, A.P., (2012) 'Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war', *Journal of Strategic Studies*, Vol. 35, No. 3, pp. 401-428.

Lo, B., (2015) *Russia and the New World Disorder*, London: Chatham House.

Lopatina, N.V., (2014) 'The modern information culture and information warfare', *Scientific and Technical Information Processing*, Vol. 41, No. 3, pp. 155-158.

Lovejoy, B., (2017) ‘Former UK security service head says weakening encryption would be too dangerous’, *9 to 5 Mac*, published online August 11 2017, accessed August 15 2017, <https://9to5mac.com/2017/08/11/encryption-mi5-uk-security-services/>.

Lucas, E., & Pomeranzev, P., (2016) *Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*, Center for European Policy Analysis, published August 2016.

Mandelbaum, M., (1982) 'Vietnam: the television war', *Daedalus*, Vol. 111, No. 4, pp. 157-169.

Mandiant, (2013) *APT1: Exposing One of China’s Cyber Espionage Units*, Feb. 18, 2013, <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

Marx, K., (1972) *Critique of Hegel's 'Philosophy of Right'*, edited and translated by O'Malley, J., Cambridge: Cambridge University Press.

Matsakis, L., (2017) 'It looks like Facebook bought Google ads to combat its Russian ad scandal', *Vice: Motherboard*, published online October 11 2017, accessed October 12 2017, <https://motherboard.vice.com/en_us/article/9k34w8/it-looks-like-facebook-bought-google-ads-to-combat-its-russian-ad-scandal>.

Meserve, J., (2007) 'Mouse click could plunge city into darkness, experts say', *CNN*, published online September 27 2007, accessed August 6 2017, <http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html>.

Mitrokhin, V., & Andrew, C., (2000) *The Mitrokhin Archive: The KGB in Europe and the West*, London: Gardners Books.

Nakashima, E., (2011) 'Cyber-intruder sparks massive federal response – and debate over dealing with threats', *The Washington Post*, published online December 9 2011, accessed August 10 2017, <https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_print.html>.

Nakashima, E., (2016) 'Russian government hackers penetrated DNC, stole opposition research on Trump', *The Washington Post*, published online June 14 2016, accessed July 7 2017, <https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.5479216336ae>.

National Intelligence Council, (2017) *Global Trends: Paradox of Progress*, accessed July 26 2017, <https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf>.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), (2014) 'Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space,' accessed May 23 2017, available at <https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf>.

Nechepurenko, I., & Smale, A., (2016) 'Russia dismisses German warnings about exploiting teen rape claim', *The New York Times*, published online January 28 2016, accessed August 17 2017, <https://www.nytimes.com/2016/01/29/world/europe/russia-dismisses-german-claims-of-exploiting-teen-rape-case.html>.

Newman, L.H., (2017) 'Say hello to the super-stealthy malware that's going mainstream', *WIRED Magazine*, published online February 9 2017, accessed July 5 2017, <https://www.wired.com/2017/02/say-hello-super-stealthy-malware-thats-going-mainstream/>.

Nietzel, B., (2016) 'Propaganda, psychological warfare and communication research in the USA and the Soviet Union during the Cold War', *History of the Human Sciences*, Vol. 29, No. 4-5, pp. 59-76.

Nimmo, B., Czuperski, M., & Brookie, G., (2017) '#Botspot: the intimidators', *Medium: Digital Forensic Research (DFR) Lab*, published online August 31 2017, accessed October 12 2017, <https://medium.com/dfrlab/botspot-the-intimidators-135244bfe46b>.

Oehmke, P., (2017) 'Milo Yiannopoulos, Bret Easton Ellis and the rise of the hipster alt-right', *Australian Financial Review*, published online August 3 2017, accessed August 19 2017, <http://www.afr.com/news/politics/hipster-altright-declares-were-at-the-beginning-of-the-information-war-20170731-gxm084>.

Ojala, M., Pantti, M., & Kangas, J., (2016) 'Professional role enactment amid information warfare: war correspondents tweeting on the Ukraine conflict', *Journalism* (online publication before print), pp. 1-17.

Ostrovsky, A., (2015) *The Invention of Russia: The Journey from Gorbachev's Freedom to Putin's War*, Great Britain: Atlantic Books.

Panzarino, M., (2017) 'Apple issues statement regarding removal of unlicensed VPN apps in China', *TechCrunch*, published online July 31 2017, accessed August 1 2017, <https://techcrunch.com/2017/07/30/apple-issues-statement-regarding-removal-of-unlicensed-vpn-apps-in-china/>.

Paul, C., & Matthews, M., (2016) *The Russian 'Firehose of Falsehood' Propaganda Model*, RAND Corporation: Santa Monica, California.

'People have become obsessed with elites', (2016) *The Economist*, published online December 15 2016, accessed August 24 2017, <https://www.economist.com/news/books-and-arts/21711859-obsession-meaningless-without-proper-focus-world-has-become-obsessed>.

Perlroth, N., & Shane, S., (2017) 'How Israel caught Russian hackers scouring the world for US secrets', *The New York Times*, published online October 10 2017, accessed October 13 2017, <https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html>.

Peterson, N., (2017) 'In Ukraine, Russia weaponizes fake news to fight real war', *The Daily Signal*, published online March 30 2017, accessed October 12 2017, <http://dailysignal.com/2017/03/30/in-ukraine-russia-weaponizes-fake-news-to-fight-a-real-war/>.

Plato, (1960) *Gorgias*, translated by W. Hamilton, London: Penguin Press.

Player, C., (2015) 'State sponsored malware becoming more sophisticated: Kaspersky', *ARN (from IDG)*, published online March 13 2015, accessed August 10 2017, <https://www.arnnet.com.au/article/570306/state-sponsored-malware-becoming-more-sophisticated-kaspersky/>.

Pomerantsev, P., (2014) 'Russia and the menace of unreality', *The Atlantic*, published online September 9 2014, accessed August 24 2017, <https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/>.

Pomerantsev, P., & Weiss, M., (2014) *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Institute for Modern Russia, accessed April 8 2017, available at <http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf>.

Putin, V., (2012) 'Russia and the changing world', *Russia Today*, published online February 27 2012, accessed August 17 2017, <https://www.rt.com/politics/official-word/putin-russia-changing-world-263/>.

Rid, T., (2013) *Cyber War Will Not Take Place*, London: Hurst & Company.

Rogers, M., (2014) 'Why I *still* don't think it's likely that North Korea hacked Sony', *Marc's Security Ramblings*, published online December 21 2014, accessed August 10 2017, <https://marcrogers.org/2014/12/21/why-i-still-dont-think-its-likely-that-north-korea-hacked-sony/>.

Romm, T., & Molla, R., (2017) 'Junk news and Russian misinformation flooded Twitter during the 2016 election', *Recode*, published online September 28 2017, accessed October 1 2017, <https://www.recode.net/2017/9/28/16378186/twitter-fake-news-misinformation-russia-oxford-swing-states>.

Rosendahl, J., & Forsell, T., (2016) 'Finland sees propaganda attack from former master Russia', *Reuters*, published online October 20 2016, accessed August 17 2017, <https://www.reuters.com/article/us-finland-russia-informationattacks-idUSKCN12J197?feedType=RSS&feedName=topNews>.

Rutenberg, J., (2017) 'Megyn Kelly, Alex Jones and a fine line between news and promotion', *The New York Times*, published online June 14 2017, accessed September 10 2017, <https://www.nytimes.com/2017/06/14/business/nbc-megyn-kelly-alex-jones-sandy-hook.html>.

Ruwitch, J., (2016) 'China wants Party's voice 'strongest in cyberspace'', *Reuters*, published online January 7 2016, accessed August 9 2017, <https://www.reuters.com/article/china-cyberspace-idUSL3N14R1T120160107>.

'Saudi Arabia, UAE, Egypt, Bahrain cut ties to Qatar', (2017) *Al Jazeera*, published online June 5 2017, accessed September 12 2017, <http://www.aljazeera.com/news/2017/06/saudi-arabia-uae-egypt-bahrain-cut-ties-qatar-170605031700062.html>.

Segal, A., (2016) *The Hacked World Order*, PublicAffairs: New York.

Sheldon, J.B., (2014) 'Geopolitics and cyber power: why geography still matters', *American foreign Policy Interests*, Vol. 36, pp. 286-293.

Sifferlin, A., (2014) ‘4 diseases making a comeback thanks to anti-vaxxers’, *Time*, published online March 18 2014, accessed October 12 2017, <http://time.com/27308/4-diseases-making-a-comeback-thanks-to-anti-vaxxers/?iid=sr-link8>.

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

Snyder, T., ‘Crimea: Putin vs Reality’, *New York Review of Books Daily*, published online March 7 2014, accessed October 12 2017, <http://www.nybooks.com/daily/2014/03/07/crimea-putin-vs-reality/>.

Standish, R., (2017) 'Why is Finland able to fend off Putin's information war?', *Foreign Policy*, published online March 1 2017, accessed August 17 2017, <https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/>.

Starbird, K., (2017) 'Information wars: a window into the alternative media ecosystem', *Medium*, published online March 15 2017, accessed September 10 2017, <https://medium.com/hci-design-at-uw/information-wars-a-window-into-the-alternative-media-ecosystem-a1347f32fd8f>.

Stevens, T., (2015) 'Roar of China's 'Great Cannon' heard across the internet', *The Conversation*, published online April 15 2015, accessed August 8 2017, <https://theconversation.com/roar-of-chinas-great-cannon-heard-across-the-internet-40201>.

Sun, L.H., (2017) ‘Despite measles outbreak, anti-vaccine activists in Minnesota refuse to back down’, *The Washington Post*, published online August 21 2017, accessed October 12 2017, <https://www.washingtonpost.com/national/health-science/despite-measles-outbreak-anti-vaccine-activists-in-minnesota-refuse-to-back-down/2017/08/21/886cca3e-820a-11e7-ab27-1a21a8e006ab_story.html?utm_term=.31c284ccc1db>.

Sunstein, C.R., & Vermeule, A., (2008) 'Conspiracy theories', *University of Chicago Law School Public Law & Legal Theory Research Paper Series*, Paper No. 199.

Symantec Security Response, (2017) *Latest Intelligence for July 2017*, published online August 4 2017, accessed August 15 2017, <https://www.symantec.com/connect/blogs/latest-intelligence-july-2017?om_ext_cid=biz_social_EMEA_facebook_ConnectBlog,EMEA>.

Syuntyurenko, O.V., (2015) 'Network technologies for information warfare and manipulation of public opinion', *Scientific and Technical Information Processing*, Vol. 42, No. 4, pp. 205-210.

The White House, (2013) *Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21)*, published online February 12 2013, accessed August 13 2017, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Thucydides, (1954) *History of the Peloponnesian War*, edited by R.I. Finley, translated by R. Warner, London: Penguin Publishing.

Uchill, J., (2017) 'Hackers accidentally create network-busting malware', *The Hill*, published online July 30 2017, accessed August 15 2017, <http://thehill.com/policy/cybersecurity/344555-hackers-accidentally-create-network-busting-malware>.

'Ukraine bans Russian TV channels for airing war 'propaganda'', (2014) *Reuters*, published online August 20 2014, accessed September 7 2017, < https://www.reuters.com/article/us-ukraine-crisis-television/ukraine-bans-russian-tv-channels-for-airing-war-propaganda-idUSKBN0GJ1QM20140819>.

United States Army, (2015) *Techniques for Effective Knowledge Management*, published March 6 2015, accessed September 22, 2017, <http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp6_01x1.pdf>.

United States National Intelligence Council, (2017) *Global Trends: Paradox of Progress*, accessed July 26 2017, available at <https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf>.

Van Herpen, M.H., (2016) *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*, New York: Rowman & Littlefield.

Vershbow, A., (2017) 'NATO, the US, and the EU need a transatlantic response to Russian disinformation and political warfare. Former US Ambassador to Russia and Deputy Secretary General of NATO Alexander Vershbow explains why.' *Atlantic Council*, posted September 8 2017, <https://www.facebook.com/AtlanticCouncil/videos/1477153005671578/>.

Wagner, K., (2017) 'Two-thirds of Americans are now getting news from social media', *Recode*, published online September 7 2017, accessed September 17 2017, <https://www.recode.net/2017/9/7/16270900/social-media-news-americans-facebook-twitter>.

Waltzman, R., (2017) 'The weaponization of information: the need for cognitive security', *Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity*, April 27 2017, accessed August 27 2017, <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf>.

Weiss, A., (2017) 'Vladimir Putin's political meddling revives old KGB tactics; Russia is returning to the playbook of the Cold War in its covert efforts to interfere with elections in the West', *Wall Street Journal*, published online February 17 2017, accessed August 25 2017, <https://www.wsj.com/articles/vladimir-putins-political-meddling-revives-old-kgb-tactics-1487368678>.

Welch, D., (2014) 'Introduction',' in *Nazi Propaganda: The Power and the Limitations*, ed. David Welch, London: Routledge.

Whittaker, Z., (2013) ‘Pentagon’s failed flash drive ban policy: a lesson for every CIO’, *ZDNet*, published online June 24 2013, accessed August 10 2017, < http://www.zdnet.com/article/pentagons-failed-flash-drive-ban-policy-a-lesson-for-every-cio/>.

'Why China's AI push is worrying', (2017) *The Economist*, published online July 27 2017, accessed August 1 2017, <https://www.economist.com/news/leaders/21725561-state-controlled-corporations-are-developing-powerful-artificial-intelligence-why-chinas-ai-push>.

WikiLeaks, (2017) 'Vault 7: CIA hacking tools revealed', published online March 7 2017, accessed August 8 2017, <https://wikileaks.org/ciav7p1/>.

Williams, R., (2017) 'We need to stop acting as if encryption initiated terrorism', *iNews*, published online July 24 2017, accessed July 31 2017, <https://inews.co.uk/essentials/news/technology/we-need-to-stop-acting-as-if-encryption-initiated-terrorism/>.

Windrem, R., & Arkin, W.M., (2017) 'Who planted the fake news at the center of Qatar crisis?', *NBC News*, published online July 18 2017, accessed September 12 2017, <https://www.nbcnews.com/news/world/who-planted-fake-news-center-qatar-crisis-n784056>.

Worrall, P., (2016) ‘Eva Bartlett’s claims about Syrian children’, *Channel 4 FactCheck*, published online December 20 2016, accessed September 28 2017, <https://www.channel4.com/news/factcheck/factcheck-eva-bartletts-claims-about-syrian-children>.

Yablokov, I., (2014) ‘Pussy Riot as agent provocateur: conspiracy theories and the media construction of nation in Putin’s Russia’, *Nationalities Papers*, Vol. 42, No. 4, pp. 622-636.

Yablokov, I., (2015) 'Conspiracy theories as a Russian public diplomacy tool: the case of *Russia Today (RT)*', *Politics*, Vol. 35, No. 3-4, pp. 301-315.

Yaffa, J. (2014) 'Dmitry Kiselev is redefining the art of Russian propaganda', *New Republic*, published online July 2 2014, accessed August 27 2017, <https://newrepublic.com/article/118438/dmitry-kiselev-putins-favorite-tv-host-russias-top-propogandist>.

Yuhas, A., (2014) ‘Russian propaganda over Crimea and the Ukraine: how does it work?’, *The Guardian*, published online March 18 2014, accessed October 12 2017, <https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media>.

Zakaria, F., (2014) 'The rise of Putinism', *The Washington Post*, published online July 31 2014, accessed September 16 2017, <https://www.washingtonpost.com/opinions/fareed-zakaria-the-rise-of-putinism/2014/07/31/2c9711d6-18e7-11e4-9e3b-7f2f110c6265_story.html?utm_term=.a6cb6892f2c1>.

Zappone, C., (2017a) ‘Fake news fight: cyber security is little defence against information war’, *The Sydney Morning Herald*, published online May 3 2017, accessed September 26 2017, <http://www.smh.com.au/world/fake-news-fight-good-cybersecurity-little-defence-against-information-war-20170501-gvw55m>.

Zappone, C., (2017b) ‘Hillary Clinton calls Russian information war a ‘clear and present danger’ to Western democracy’, *The Sydney Morning Herald*, published online October 8 2017, accessed October 10 2017, <http://www.smh.com.au/world/hillary-clinton-calls-russian-information-war-a-clear-and-present-danger-to-western-democracy-20171008-gywfrj.html>.

Zetter, K., (2011) ‘The return of the worm that ate the Pentagon’, *WIRED Magazine*, published online December 9 2011, accessed August 10 2017, <https://www.wired.com/2011/12/worm-pentagon/>.

Zetter, K., (2012) ‘Meet ‘Flame’, the massive spy malware infiltrating Iranian computers’, *WIRED Magazine*, published online May 28 2012, accessed August 10 2017, <https://www.wired.com/2012/05/flame/>.

Zetter, K., (2014) ‘Hacker lexicon: what is a zero day?’, *WIRED Magazine*, published online November 11 2014, accessed August 10 2017, <https://www.wired.com/2014/11/what-is-a-zero-day/>.

Zetter, K., (2015) 'The NSA acknowledges what we all feared: Iran learns from US cyberattacks', *WIRED Magazine*, published online February 10 2015, accessed July 31 2017, <https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/>.

Zins, C., (2007) 'Conceptual approaches for defining data, information, and knowledge', *Journal of the American Society for Information Science and Technology*, Vol. 58, No. 4, pp. 479-493.