Department of Political Science and International Relations

Will Cyber War Happen?

Conceptualising cyber warfare as acts of war

Conor McKenna

UNIVERSITY OF BIRMINGHAM

Supervisor: Dr Adam Quinn

Secondary Supervisor: Professor Scott Lucas

Abstract

Cyber attacks are becoming increasingly common as a tool for conducting foreign and security policy. Despite cases of real damage inflicted on states by such attacks, however, a cyber-only attack has never triggered a conventional military response. This may lead observers to assume that a robust norm exists to the effect that a cyber-only attack cannot clear the threshold to qualify as an act of war rendering conventional military response legitimate. This thesis seeks to question the robustness of any such assumption. It proposes a framework for understanding inter-state actions that highlights the scope for divergent state interpretations regarding the parameters of legitimate response to a cyber-attack, and consequent risk of inadvertent provocation of conventional response. Using two historical cases as illustrative examples, the thesis examines the expectations of states in deploying cyber attacks, especially that of contained risk, as well as how the attack was interpreted by the state that has been acted upon. It then discusses the range of potential modes of response open to the victim government in the aftermath of the attack's discovery. In critically assessing these, the thesis judges that the factors inhibiting the response were contingent and primarily prudential. In alternate circumstances, it is quite conceivable that a state might consider conventional military action as falling within the scope of its legitimate response to a cyber attack, if the attack were of sufficient severity, and prudential calculations permitted. We should be cognisant that the threshold for judging an 'act of war' to have been committed is a construction based upon states' respective, and potentially divergent, interpretations of actions taken by and against them. As such, prevalent understandings regarding the thresholds for war and the parameters of legitimate response may be subject to change in light of advancing technology and the resulting scope for forms of aggression without precedent.

Acknowledgements

My thanks especially to my supervisors, Adam Quinn and Scott Lucas. I have not been the easiest of PhD students to supervise, but their advice and support throughout the process has been invaluable. I would not have reached this point without them.

I cannot even begin to express my gratitude to my long-suffering parents who helped me every step of the way. Also, to my brother, whose trip to take me back to Birmingham in 2015 meant more to me than he'll ever know. This thesis would not have been possible without the support my late-grandparents, aunts and uncles.

To my wife, Sheena - who has seen the long days, nights and sat up with me when it all seemed to be going nowhere - I would not have been able to do this without your constant love, care and advice. Also, to my in-laws, Pat and Terry, who have supported us both throughout my PhD.

This thesis would not have been possible without Colin Thain, who gave me a job and taught me the ins and outs of British Politics.

I am deeply grateful to Sam Warner for putting up with my interruptions as we sat together on the 10th floor. An especially big thanks to Chris Featherstone, for cheering me on and racing me to the finish line. Also, to John Evemy, Eva, Manu Padda, Timea Nochta, Elio Di Mucchio and Maren Rohe whose DnD sessions kept me sane this past year. My thanks to senior researcher Mattias Hjort for his witticisms and friendly advice. Mel Cruz and Darcy Luke, special thanks for challenging me to be better. I am grateful to Tom Jarvis, lunchtime discussions would not have

been the same without his insight and critically his use of statistics and Bruno Dalponte for being the big brother I needed. My thanks to Shardia Briscoe-Palmer for being the calming influence on the 10th floor when it all seemed hectic.

I've been lucky to spend my time with some incredible academics at Birmingham. I am indebted to all the staff of the School of Government for assuring me that the PhD is just a step in the journey.

Contents

Chapter 1 Introduction

This thesis examines war, acts of war and the threshold between peace and war. Furthermore, we will analyse the possibility of cyber attacks as a means for crossing that threshold. This thesis will show that our understanding of the threshold for war is constantly changing and that conceptualisations of legitimate responses to cyber attacks as necessarily excluding traditional military responses are short-sighted. In the first chapter, we will examine war from the perspective of Clausewitz and analyse this with literature from the English School as well as Social Constructivism to show that there are significant problems with Clausewitzian notions of what determines war. The second chapter will focus on cyber war, analysing the literature and debates surrounding how cyber attacks are understood. The third chapter will propose a theoretical framework through which we can assess how states determine acts of war. This will examine notions of intention, perception as well as retaliation under a new model termed: Action Phase-Reception Phase (APRP). This framework will then form the basis for analysis in three case studies: firstly, we will use the framework to examine Stuxnet, the US-Israeli cyber attack that was designed to damage the Iranian nuclear programme in 2009; secondly, we will look at the Distributed Denial of Service (DDoS) attack that took place in Estonia in 2007 as a reaction to the moving of a Soviet War Memorial; finally, we will posit a series of hypothetical cases that will further illustrate the utility of the proposed framework. This introductory chapter will explain the significance of each of these chapters to the overall argument and the contribution to the literature made by this thesis.

The research question that this thesis addresses is whether cyber war has the potential to occcur and examines areas where prudential calculations and misalignments provide scope for this to take place. This is a direct response to Rid's (2012) *Cyber War Will Not Take Place* article and subsequent monograph. By cyber war, we refer to a potential event where a cyber attack

can be responded to with the full range of conventional military force and changes the relationship between the principal actors such that a state of war exists. Cyber war, as used in this thesis, does not refer specifically to a conflict that takes place solely in the cyber sphere but where cross-domain warfare occurs. Importantly, this thesis argues that the factors that have restrained reactions to cyber attacks in recent history are contingent and prudential rather than an accepted set of norms.

1.1 War

Chapter two focuses on the literature of war and warfare to understand how states make the transition between peace and war. In order to assess this, we turn to more recent interpretations of war that help to explain what is meant by 'force'. It will be made clear that acts of war are typically synonymous with kinetic attacks, i.e. it is assumed that an act of war must be one in which there is an element of direct lethality or at least potential for lethality. However, there will also be discussion of the problems associated with assumption. For example, there are historical cases that do not necessarily fit within the realms of kinetic attacks. This chapter also deals with the issue of escalation, which is critical to understanding acts of war and how they are determined to be such. This section examines how states determine whether to escalate, and the miscalculation problem that can occur leading up to this. Understanding miscalculation becomes a critical part of the APRP framework discussed later.

War is defined legally in many states and there are specific laws that govern what occurs within a state when it transitions from peace to war. This can be a useful method of examining how states make the transition, but it explains little about why that transition took place, nor does it account for the fact that some states act as though they are at war in a practical sense without issuing a legal declaration. Therefore, it is necessary to break down war into two constituent

elements: war de jure, war that is legal and therefore uses specific mechanisms of state; and de facto war, conflict that resembles war in all or most characteristics without triggering the legal mechanisms. This allows this thesis to consider conflicts that have not proceeded via formal legal pathways. For example, the US has not been legally at war since 1945, though it has been at war in a de facto sense many times since then.

The transition between peace and war is marked by an 'act of war'. Much of this chapter is devoted to better understanding what characterises acts of war and how they are framed, looking at several historical examples for an insight. The analysis is broken down into three subsections: violence against persons or property; violation of sovereignty; and allegiance to ideology or ideologies that are considered unacceptable or illegitimate and or honour-related offences. Discussion of violence against persons or property includes all aspects of traditional kinetic attacks as well as examining some of the issues surrounding what constitutes violence. Discussion of violation of sovereignty covers definitions of sovereignty and potential violations such as invasions and interventions.

Allegiance to considered unacceptable or illegitimate ideology or honour related offences concern the least tangible potential grounds for war. For example, an attack on the honour of the nation was considered grounds for going to war in the past. Historical perspective indicates that our notions of what war is and how acts of war are determined, has shifted through history and will likely continue to do so. This points to a danger that states might be insufficiently reflective about the continuing possibility of evolution in norms in the area of what it means to conduct war and commit acts of war. This danger is evident when we turn to the next chapter, which examines whether a cyber attack could be considered an act of war.

1.2 Cyber War

Chapter three introduces the themes of cyber attack and cyber war. The aim of this chapter is to clarify some misconceptions surrounding cyber attacks and review the relevant literature and debates regarding the status of cyber attacks in foreign policy. There is also examination of the reliance of society on the internet (KPMG, 2015: 2). Understanding the militarised nature of offensive cyber attacks proves critical to advancing our understanding of changing conceptions of acts of war.

The militarisation of cyber attacks presents some useful areas for discussion when it comes to violations of sovereignty and ideology/identity that as discussed in the previous chapter. This chapter shows that states are changing their conceptions of where cyber fits within a framework of national security. For example, while there are different government agency divisions within the US that focus on cyber attacks, the highest tier of responsibility lies with the military rather than with law enforcement agencies. This indicates, and normalises the idea that cyber attacks are to be dealt with within the military sphere rather than the civilian. This chapter focusses heavily on the United States and its national cyber security policy. However it draws on several other examples that indicate similar practice is taking place in other states.

This chapter examines how cyber attacks fit within the conceptual frameworks governing war and acts of war. This primarily focuses on the arguments brought forward by Thomas Rid (2012) in his seminal piece "*Cyber war will not happen"*, which brings together much of the literature at the time on cyber attacks and their relationship with war. But it also provides the context of the wider academic debate that cyber attacks have created. This chapter argues that there is need for better understanding of the concept of force and, of the lack of clarity as to where states consider the threshold for war to lie. The chapter argues that we need to reflect on

how states make calculations regarding the decision to take cyber action, and the expectations they have in doing so. Furthermore, it is important to consider the scope for interpretation by the state that has been acted upon, what factors determine their perception of what took place, and the constraints that can limit their reaction.

This chapter also serves as an introduction to concepts that will be covered later in the thesis such as cross-domain escalation and attribution. The cross-domain issue is important; some scholars believe that cyber attacks will only be responded to by attacks also within the cyber 'domain'. However literature suggests states have engaged in cross-domain escalation previously. Attribution of cyber attacks is critical for understanding how the state that has been acted upon responds to cyber attacks. If the state cannot attribute an attack then its means for response are limited. This chapter reviews literature that suggests that attribution is possible in most cases.

Finally this chapter prposes a new analytical framework for analysing the dynamics of interest here. The proposed 'APRP' model breaks down the inter-state interaction into three constituent elements: calculation of the acting state, which is determined by intention and framed by expectation; the interpretation of the state that is being acted upon; and the reaction of that second state. This provides a framework for discussion and analysis of the case studies previously mentioned.

1.3 Action Phase Reception Phase

Chapter four puts forward a new analytical framework for understanding miscalculation between states. To do this, it breaks down how action is interpreted into a series of constituent elements to better understand the role that each has in the creation of an outcome.

Calculations are best understood by elaborating on two elements: intention and expectation. These form the basis for analysis of an initial action. Understanding intention means having insight into the motivations behind a decision and this further leads to an analysis of the factors that shape this. The argument presented is that intention, meaning the aims underlying a calculated action are shaped by notions of gain, political pressure both internal and external, and public opinion. These influence the specific goals a state selects. For example, public opinion might limit a state from aiming to overthrow another's government with military force, however a cyber attack might be deemed acceptable.

States who are acting also consider the potential reaction of the state that is being acted upon. Particularly important to considering is the interpretation that state is likely to place upon an action once it has taken place. Therefore, the acting state makes a calculation regarding the types of interpretations and subsequent reactions that might be possible and probable. The term used for this is expectation: what the acting state determines are the likely expected outcomes as a result of the action. Intention and expectations combine to set limits for action, I.e. if the intention is not to go to war then the expectation will be to avoid actions that might be expected to provoke a conventional military response. States rely on previous experience with the state to be acted upon in order to make calculations about the types of responses that should be expected.

In terms of avoiding escalation , the expectations of the state guide the choice of action, because a calculating state will only commit acts where the spectrum of anticipated possible response is limited to what it considers acceptable. In simple terms, Intention is the desired outcome of an action; Expectation is the anticipated response to that action within limits of possibility and

probability; and calculation is the process of coming to a decision about what action to take (or not) based on these two. For example, Stuxnet was chosen as a means for dealing with the Iranian nuclear issue on the basis that an Iranian bomb would trigger another war in the Middle East and Stuxnet could help avert this outcome while also avoiding war. The first section of the APRP framework involves understanding such calculations and the types of factors that might lead to a miscalculation of outcome.

Once the action has taken place our analysis shifts from the action phase to the reception phase. This element of the study examines first how the state acted upon perceives and interprets the action. This requires a critical examination of societal and political value attribution, as these are vital factors in understanding how the state that has been acted upon decides to react.

The process of calculating interpretation is vital to reaction but is distinct from the reaction itself. A state might interpret an action against it as legitimate grounds for war, yet nevertheless react in a way that does not further escalate the conflict. Likewise, the state may choose to react by escalating the conflict – especially if they interpret the initial action as having escalated the conflict in the first instance.

Distinguishing between the intentions and expectations of the acting state and the interpretation of the state that has been acted upon lets us see where possible divergences might occur. It is this miscalculation that can lead to escalation and potential war.

We can posit two distinct sets of problems of misinterpretation: firstly, the misinterpretation of intention; and secondly a divergence of interpretation of outcome. With the misinterpretation of

intention, the acting state is misinterpreted as having intended more harm than it did in fact intend. There is a disparity between what the acting state intended and what the state acted upon perceives as the intention. The gravest instance of this occurs when the state that has been acted upon interprets the action as a deliberate desire on behalf of the acting state to cross the threshold between peace and war. If the acting state did not intend to cross that threshold, then there is a dangerous disparity in the interpretations. The divergence of interpretation of outcome between the acting state and the state acted upon, meanwhile, provides an area for miscalculation on both sides, rooted in differences of social and political value attribution. For example, societies place certain intangible value on specific institutions. This creates a situation whereby the acting state can misinterpret the importance of a target to the society and thus attacking it could have differently interpreted outcomes the parties. Examining misinterpretation therefore can be key to understanding a perceived gap in porportion between the action and the outcome.

Next and finally, there is the reaction itself. Initially it is important to understand the different types of reactions: kinetic or other potentially harm-inflicting reactions, as well as restrained reactions, meaning a response not necessarily taken with a view to damaging the other. This might include verbal responses, press conferences and interviews. The form of reaction often determines the direction of the relationship going forward: i.e. a retaliatory strike might be seen to escalate in certain circumstances while merely giving a press conference regarding an attack conveys different meaning.

This chapter categorises reactions into a series of different types. To do this, it breaks down the options of the state that is reacting, into categories of proportionality. It looks at reactions that are: restrained by comparison to the initial action, i.e. where the intended impact and damage is considered by both parties to be less than the initial action; in proportion to the initial action,

when states respond in kind to an attack with a similar type of attack with no expectation on the part of the reacting state that there will be an escalation of the conflict; and finally, those reactions that are out of proportion to the initial attack. This last category means the reacting state choses a retaliatory attack designed to cause significantly more harm than the initial attack. It may also be an attempt by the state to escalate to war. We typically determine proportion based on the expectation of the initial actor; this provides the basis against which subsequent reaction is judged. But importantly an attacked state may face a difficult choice between its prudential calculation of perceived cost to itself of a warlike response and its self-perceived legitimacy were it to respond in that manner. Reaction adds its own nuance to arguments surrounding miscalculation regarding the threshold for war and acts of war. States' reactions are influenced by similar restraining and motivating factors as the calculation phase of the initial action. Understanding that reaction is shaped by interpretation helps to explain what states think they would be entitled to do. But this is only part of understanding a reaction, which is influenced by wider context and prudential calculation.

1.4 Case I: Stuxnet

This is the first of three chapters that apply the conceptual framework to a case study focussing on Stuxnet. As Thomas Rid (2013) notes, Stuxnet presents one of the best cases for study of cyber warfare as it is the case that may have come closest to what he considers an act of war under his definitions. The manner of the attack (a worm that was designed to physically break uranium enrichment centrifuges), as well as the timing of the attack make it suitable for study. The nature of the Stuxnet attack at the outset in 2009, was covert/anonymous, which is significant for the APRP process. The Stuxnet 'worm' is considered one of the most dangerous cyber weapons ever built (Zetter, 2014) and therefore is an important case for our understanding of cyber attacks' relationship to the concept of an act of war.

The chapter relies substantially on the work of Sanger (2012) and Zetter (2014) for understanding the context of the cyber attack. Sanger's insights into the case are unparalleled as he had access to sources in the US government that no one else had, some of whom have since come to light including General James Cartwright. Zetter's work focuses on interviewing the various private contractors that surrounded the Stuxnet case, including conducting interviews with various malware groups and specialists such as Ralph Langner. These help to piece together the various expert opinions on what Stuxnet was and how it worked in practice. These interviews also shed light on the potential that Stuxnet brings to cyber warfare and what it means we can expect going forward.

The analysis of Stuxnet applies the framework outlined in Chapter 4. It concludes that there is a potential gap between US calculations and execution of the attack and the Iranian interpretation of it. This disparity could have proven costly had the Iranian government chosen differently when it came to reaction. The importance of the nuclear programme to the Iranian people and the government meant that the US took a significant risk in assuming that Stuxnet would not be interpreted and acted upon as grounds for war. Though Stuxnet did not lead to war between the two countries, it serves as a useful case for illustrating the potential for misalignment between expectations regarding the outcome of an action and its interpretation by those on the receiving end.

1.5 Case II: Estonia

The second case is a series of cyber attacks that took place in Estonia in 2007. The Estonian case presents different parameters to the Stuxnet case which is useful for understanding the variety of cyber attacks that are possible and of the methods of response at the state level. The case is fundamentally different from Stuxnet in that there was no kinetic effect or attempt to produce

one. One of the main reasons that Rid argued for the importance of Stuxnet was based on its kinetic abilities. The Estonian case provides a contrast. This cyber attack was primarily an effort to take down critical websites including those pertaining to government, media and banking sectors. In this manner the Estonian case is critically different to Stuxnet. Stuxnet was a targeted attack with a very specific aim in mind, to damage the Iranian nuclear programme. The Estonian case is an example of the damage of a more dispersed large scale cyber attack that hits multiple targets at once. Notwithstanding these differences, and perhaps because of them, the case also serves to illustrate the potential for miscalculation and misinterpretation between states.

This case examines the context surrounding the Distributed Denial of Service (DDoS) attack on critical infrastructure in Estonia in 2007 in the wake of controversy surrounding the potential destruction of a Soviet era memorial Bronze Soldier in Tallinn. As the motivations behind the attack are clear, it is possible to make informed inferences regarding Russian cyber policy and military policy leading it, as well as regarding why Russia chose this method of attack rather than using military or direct economic means to achieve the same end.

Cyber attacks can be challenging to address within the literature on war because of the problem of attribution, and the Estonian case is no different in this respect. As with the Stuxnet case, however, a number of experts that have attested to the perpetrator being Russia (Mastriana, 2017; Roscini, 2015; Singer and Friedman, 2014). The nature of the relationship between Estonia and Russia provides an interesting insight into the significance of political and social value attribution. Estonia takes great pride in having one of the most internet integrated societies anywhere in the world. An attack from a previous imperial power on Estonian websites, in what might reasonably interpreted as an attempt to reassert dominance in a former sphere of influence, brings forth a number of hazards that are discussed in this chapter. This forms the bulk of the interpretation section of this chapter.

The analysis of the reaction phase here focuses on the efforts of the Estonian government to come to terms with a cyber attack of this magnitude. Media Interviews with various government ministers indicated that Estonia would consider this an act of war at least in the early days after the attack. However, it is argued in the chapter, NATO had an impact in bringing Estonia back from the threshold and helped to placate its government with promises of a new cyber security agenda and office based in Tallinn. While Rid argues that Stuxnet provides the case closest to crossing the threshold, the Estonia case provides some notable insights into where some politicians believe that threshold lies. As Stuxnet remains the case that is most heavily researched for the purposes of cyber war, this research on Estonia provides a different perspective on an important cyber attack.

1.6 Case III: Hypothetical

The final 'case' is a study of a hypothetical cyber attack. This has precedent in the literature on cyber warfare, Clarke and Knake (2010) undertook a similar project though with a different agenda. The focus of this chapter is to expose the danger of miscalculation in the process between intention and reaction. This case study allows this research to contemplate a wider array of potential areas for miscalculation than the previous two. Through a variety of different scenarios combined with empirical examples to provide some context and precedent for arguments, this chapter will go further than Clarke and Knake in the analysis of what a potentially devastating cyber attack might look like and the impact it might have on inter-state relations.

Clarke and Knake's (2010) monograph outlined the impact of a hypothetical cyber-attack focussing on the relationship between states. This thesis uses a similar method to illustrate

where the potential for misalignment between actors may arise. Three different scenarios are laid out in the case of Action-Phase and Reception-Phase to show how decisions at different points can lead to the potential for escalation. The analysis of hypothetical decisions places emphasis on the prudential calculations that take place when deciding when to act and react. A counterfactual approach was considered in the initial stages but this was assessed to be unable to provide a sufficiently varied set of circumstances while maintaining plausibility for the overall argument.

The case posits a cyber attack that causes an effective blackout in a major city for a number of days. This chapter breaks down the potential reasons behind the conception of this specific type of action and how it is executed. It examines the different factors that might influence the intention and expectation of the acting state. It proceeds to consider in depth the potential for escalation via consideration of interpretation on the part of the affected state. If the acting state makes a miscalculation about political or societal value attribution, or misunderstands the previous context between the two states then there is significant scope for conflict escalation to occur. The chapter considers the role of unintended consequences as a source of misinterpretation on the part of state acted upon, as well as the different societal and political value attributions that take place in states that may have an impact on how they respond to attack. In the interpretation section, the chapter examines various scenarios where the intention and outcome are interpreted differently. Finally, this chapter analyses the different methods of response, examining the rationale for each.

This chapter allows us to examine a number of different ways in which action can be interpreted without being limited by historical cases. As yet there has been no cyber attack that has escalated a conflict from peace to war, but using hypotheticals is useful for assessing the potential for such an outcome.

1.7 Summary

Cyber attacks are increasingly being used as a tool to conduct foreign policy, but this has not triggered a conventional military response. This may lead to an assumption that a norm exists that restrains escalation from cyber attack to kinetic response because a cyber-only attack cannot constitute an act of war. This thesis seeks to question that assumption through a framework which emphasises the possibility for divergent interpretation regarding the legitimacy of conventional military response to a cyber attack. Using a two historical case studies as well as a hypothetical this thesis seeks to highlight the areas for potential disparity between an acting state's intentions and expectations and the state that has been acted upon's interpretation and reaction. This thesis argues that the rationale behind restraint in response thus far to cyber attacks has been prudential and contingent rather than based on a robust norm. Given different circumstances, it is possible that a state may have chosen to escalate to a conventional military response if the initial action were severe enough. This thesis builds on existing literature focusing on issues such as war and cyber and combines this with an approach that emphasises the importance of context, calculation and perception. Using case studies allows this thesis to see how cyber attacks could potentially have spilled over into war, if not for contingent prudential factors. The hypothetical case then illustrates the potential for different outcomes under plausible alternative circumstances. This helps us see how sufficiently severe cyber attack might bring about shifts in the threshold for war and the parameters for a legitimate response in a time where technological advancement has widened the scope for forms of aggression without precedent.

Chapter 2 Acts of War

War is a concept that describes a relationship between two or more actors. The literature on war is very broad with multiple focal points. Walzer for example focuses on Just War Theory; others have dealt with morality and ethics in war and studies of violence and violent conduct in war. Outside of the social sciences, much has been written on the history of war and warfare. Many scholars have sought to define war, but there is still ambiguity as to precisely when or how a state transitions from peace to war. A definition of war that covers the characteristics of every intuitive empirical case is challenging to arrive at. While it is generally accepted that war is a state of conflict, usually violent, between a number of actors (Wright, 1942; Gray, 2005: 30 Oppenheim, 1935: 173; Alexander, 2006: 168-169), there is wide variation between what that conflict pertains to, how is executed and how this affects the actors in question. This chapter will examine the background literature on war as it relates to how states conceive of war, and how states move from being at peace to a relationship that is one of war.

This chapter will examine war as a concept. In particular, the first section looks at discussions over what war pertains to and how it can be characterised. The first section illustrates the difference between *de facto* and *de jure* conceptions of war. The second section discusses how wars start, focussing on acts of war. This is done by categorising acts of war into three overarching types: violence against persons or property, violation of sovereignty and identity and ideology. The final section of this chapter examines why states would choose to go to war.

2.1 Understanding War as a concept

Many scholars have dedicated their efforts towards defining what we mean when we talk about war, acts of war and warfare. Clausewitz defines war as an act of force that compels the enemy to do the will of the acting state (2000: 264). His work provides the preliminary basis for most

definitions that followed it. In a famous formulation, he argues that war is a continuation of 'politics through other means' (Clausewitz, 2000: 264). Hedley Bull meanwhile defined it as organised violence by political units (1977: 184). The concept of violence, then, is important to the conceptualisation of war. Furthermore, there is an explicit understanding within much of the literature (Clausewitz, 2000; Wright, 1942; Buzan and Herring, 1998) that the actors in question are typically states.

These definitions inevitably give rise to questions about the threshold for transition to a state of war. For states, war is on one level a legal matter, whether initiated by the actions of the state itself or mandated by the actions of a perceived aggressor. The transition from peace to war has traditionally been signalled by a declaration of war (Schmitt, 2010: 152; Dinstein, 2011: 9; Hanson, 2009: 9; Fazal, 2012: 557), issued by one state against another. This legal shift often allows states to act in ways that under ordinary circumstances would be resisted by the public at large, e.g. conscription. A strictly legal view provides a clear-cut delineation of when a state is at war versus when it is not. However, while this approach may be useful in some contexts, it can also cause problems for analysts if it discounts conflicts that are generally accepted as war, even if they are not designated as such in the strictest legal sense. As a result, conventional definitions are not adequate for capturing every scenario that could qualify as war.

Not all wars are wars in a strict legal sense, but may be in the material sense (Bull, 1977: 185). In essence, some conflicts are wars but may not be legally so. This may be the case with civil wars, or an attempt to quickly counter an enemy advance without prior declaration, as in the Six Day War. Wars can also exist in the legal sense but not in the material sense - i.e. before the conclusion of a peace treaty but after violence has been suspended (Bull, 1977: 185). The United States provides a good example of the challenge in making the distinction between states that are *de facto* at war rather than *de jure* at war. The Congressional Research Service note that

there is a difference in the state of international affairs created by a declaration of war and the authorisation of a use of force (CRS 31133, 2014: 20). In its history, the United States has declared war eleven times on foreign states (CRS RL31133, 2014: i). Declarations of war have not been used by the United States since the end of WWII. But the US has used large scale force abroad many times. Few scholars would argue the difference between the authorisations of the use of force versus declarations of war on behalf of the United States creates a substantively meangingful distinction. To say that the United States has not been 'at war' since 1945 would lack credibility. Thus, it is arguable that states can be at war in a *de facto* manner without being at war *de jure*, even where there is a clear constitutional process for its declaration within that state.

States can also be at war in the legal sense without having any violent contact, which undermines definitions that require physical violence as a criterion for a state of war. This puts states on a war footing and gives them certain privileges in action towards other states – such as the unilateral imposition of economic sanctions, (though these are also used sometimes outside of war). The reality of 'war' in this instance is debatable. While Britain declared war on Finland in 1944, few would consider the relationship between the two states as resembling warfare. The declaration of war against Finland was made as a symbolic gesture of support for Russia rather than signalling any real hostility or the intention acting violently against it. Nor did Finland respond to the declaration of war with a commencement of armed conflict against Britain. Finland had more pressing concerns at the time as they faced Russian invasion. Ingrid Detter uses the example of Latin American States in the Second World War to illustrate this point. Many of the states declared war but had neither the willingness nor the resources to become effective belligerents in their own right in the war (Detter, 2013: 7). It is, therefore, possible to be legally *at* war without actually being *in* war in the sense of engaging in combat. This brings

forth the question of whether the legal aspects of war are necessary for understanding the nature of how wars begin.

Von Glahn states that "[g]eneral opinion has sanctioned a commencement of hostilities without issuing a declaration of war or other formal notice of intent to resort to the use of force." (1992: 500)[1]. Clausewitz's framework for the use of force is narrower than what some scholars suggest; it does not encompass political or economic force but focuses on violence or military use of force (Kliem, 2017: 370). If the legal act of declaring war has fallen out of use, then while we might consider it the most clear-cut arbiter of whether a state is at war or not, it is not the only one.

> 'Unilateral acts of force performed by one state against another without a previous declaration of war may be a cause of the outbreak of war but, they are not war in themselves, so long as they are not answered by similar hostile acts by the other side, or at least by a declaration of the other side that it considers them to be acts of war. Thus, it comes about that acts of force performed by on state against another by way of reprisal or during a pacific blockade in the case of an intervention, are not necessarily acts initiating war.' (Oppenheim, 1935: 173).

This quote from Oppenheim represents a view of war that relies on declarations rather than merely acts or reprisals. From this viewpoint, two states cannot be at war without a declaration indicating that that the transition from peace to war has taken place.

[1] The CRS concludes the same (31133) as does Dinstein (2011: 9)

It is possible to imagine a situation whereby an act so heinous as to begin a war has occurred without the formalities of a prior declaration (as in the example of Pearl Harbor). In such cases it might verge on superfluous formality to state that war now exists between the victim and the perpetrator. Conversely, the Cold War had some features of wartime relations, but neither side cared to declare war nor ever struck a blow to the opposing military. Baudrillard notes that deterrence was a key component in preventing the Cold War from becoming 'hot' is a virtual exercise in power which would lead us to conclude that the Cold War was a war (1995: 8). In cases such as these, legal frameworks for war may be severely tested.

War and the methods for waging war have undergone great change throughout history.[2] Technology and methods have been adapted constantly to improve their effectiveness in war. The Spartans fighting the Athenians were surprised to note that instead of meeting them on the battlefield, the citizens stayed behind the walls (Hoffman, 2009: 34). The methods of war adapted to meet the conditions. In a little over 100 years the machine gun has gone from being a gimmick, not considered to be accurate enough or function consistently enough, to a staple part of a military's arsenal (Ellis, 1993: 17). The history of war, then, is one of adaption. A notable example is the Boers employing rifles and field guns against the British who were forced to adopt similar means to win the war (Hoffman, 2009: 36).

When nuclear weapons entered the arena of war, states were forced to rethink the notion that weapons must be deployed on the battlefield to achieve victory. The likely costs of their use was obvious. As a result, states could no longer rely on tradition and precedent (Freedman, 1989: 212). The superior military force traditionally won war. But the US was forced to concede that stronger military did not equate to a victory in Vietnam. The NATO force fighting in the Balkans

[2] Smith (2006: 64-104) presents a detailed impact of modernisations on the methods of warfare. Delbruck (1985) has a discussion on wars fought from feudal to Napoleonic era, clearly showing how the manner in which wars have been fought has changed. Mack (1975) has an article explaining why big states lose small wars which outlines how wars are adapted to meet the circumstances. Heuser (2013) and to a less extent Hanson (2009) have an excellent synopsises on changes in strategy.

in the 90s were forced to adapt its military strategy due to factors outside its control such as the horror of civilian casualties. This factor is critical for understanding why cyber attacks are considered preferable to 'boots on the ground' (Clark, 2001: 419; Gray, 2005: 165; Levy 1988: 664; Byford, 2002: 37). It is possible that states have moved towards a more rational method of calculating the cost of war, and adapted towards using war less frequently as means to conduct politics (Munkler, 2005: 117; Sharma, 2010: 1).

The underlying problem of examining war then, is that conceptualisations of war are fluid. War for Clausewitz was very different from the war of today. This is partly due to technological innovation, which has changed the methods of war. In addition to this, the legal approach to war might be inadequate for understanding how wars start as some states, such as the US, have moved away from the *de jure* usage of the term despite *de facto* using military force. The result is that when committing to an action, a state might miscalculate that their act will not cross the threshold to be considered an act of war.

2.2 Manifestations of Acts of War:

The nature of war is best understood by examining how wars begin. This means understanding the transition from peace to war. Examining the different manifestations of 'acts of war' also draws attention to the analytical importance of potential disparities in perception between the state acting and the state who has been acted upon.

What do we mean when we talk about an act of war? Broadly defined, an act of war takes place when the recipient of an action, through their own observation, deems that responding with the full range of options available during wartime is justified. We can categorise acts of war under three subsections: violence against persons or property; violations of sovereignty; and

allegiance to ideology or ideologies that are considered unacceptable or illegitimate or honour related offences. To fully assess what we mean by acts of war it is useful to examine each of these categories.

2.2.1 Violence Against Persons or Property

To assess the nature of violent acts of war it is necessary to clarify what we mean by violence. Hundley and Anderson (1996: 223) devote some time to outlining the various thresholds for violence and responses, but they underplay the potential significance of difference perceptions on the part of addressor and victim. Consider the case of one actor who punches another; this seems an obvious case. However, scholars such as Harris and Finlay argue that even at a fundamental level the meaning of violence can be contested. This is because violent acts can take different forms.

The emphasis on violence across the literature indicates its integral link with war. Harris distinguishes between acts of violence, sometimes defined as having 'purposes… either illegal, immoral or political'; and violent acts that include benign human actions involving physical impact, such as wood cutting (1980: 13-15). Take the example of the ambushing of an army: shooting or causing serious injury is doubtless a violent act. However, Harris notes that it is universally accepted that murdering in all its forms is an act of violence. If the soldiers were poisoned for example, their deaths would still be violent (1980: 15). Finlay however moves the debate forward by building on Harris's principles, noting that violence is the infliction of harm by humans on others usually causing some degree of injury to body or psychology. It may also encompass violence against property. This definition provides a more succinct analysis of violence as it accounts for violent acts and acts that *result* in violence. This contrasts with Harris, for whom they remain separate. This would be the case of the solider who dies of poisoning rather than a stabbing, for example. However, it also takes into account the notion of

psychological damage. This may be problematic, because unlike with a physical open wound, psychological damage can be difficult for professionals to diagnose or treat, despite recent advances in medicine. Psychological harm dealt with in detail later, however for the purposes of this thesis it falls into an overlapping space between violence against people and harm to things of perceived social value. This latter category can be problematic, as it depends on measuring how humans construct value and how that value is placed, as well as how harm to valued things that influences their opinions of other actors and their actions towards them. Thus, though Clausewitz describes violence as integral to acts of war, the significance of the violence suggested is often subjective.

Before an act of war, framing violence can be more difficult. Violence against objects rather than human beings, for example, raises several challenges for assigning significance. Firstly, it is potentially difficult to assign an objective weight of harm in these instances: damage to a building, for example, has a different impact depending on whether it is hospital or a military installation. Secondly, as the literature illustrates, the impact human life is inherently more important when ascertaining the cost of a violent act. Thus, it could be reasonably argued that damaging an empty building is less violent than causing injury to one person. However, if that building housed something vital to human survival, e,g, a food supply or an electricity generator? Then the cost to life could be much higher than the initial damage, complicating any simple ranking of direct violence against persons as more serious than that against property.

A third issue arises when assessing the damage done when an action is not necessarily violent in itself but the result is. Harris posits a case of cheese wire hung across lampposts to catch British military personnel on motorised vehicles (1980: 16). The action of attaching the cheese wire is not inherently violent, unlike stabbing the military officer for example. However, the outcome is violent, and few would dispute that such an act would be one of violence.

In Berkowitz's (1993) work this connects to the concept of 'aggression' and how aggressive acts are perceived. Berkowitz argues that "[o]bserved aggression is in the mind of the beholder" (1993: 212) and therefore it often falls to individuals to interpret if actions are aggressive or not. In his analysis, the punishment of perpetrators is good because it makes witnesses and the victim less likely to retaliate in kind or think of doing similar aggressive acts towards others (Berkowitz, 1993: 212). Berkowitz's approach to analysing aggression focuses on the interaction of perpetrator, victim, action and the perception of the action (1993:213). This interest in examining how violent acts are perceived by those who commit them and those who are impacted by them is a fundamental aspect of the framework discussed in Chapter 4.

These issues are further complicated by the concept of non-kinetic violence, i.e. when an act can have the same substantive impact as a violent attack but without the initial moment that relies on one object directly causing harm or damage to another. For example, an electromagnetic pulse [EMP] detonated in a large city could cause as much damage, if not more, than a bomb being set off in a power station. There is little kinetic effect, electrical devices stop working, but humans are not affected in any physical way comparable to an explosive device or a biological weapon. The ultimate cost is the damage to infrastructure, and the time it would take to get the city back to functioning at full capacity. For minor issues this could be solved with replacing fuses, but with other electrical devices, phones, laptops etc, the damage could be substantial. We have little real-world evidence of what the effect of a serious internet outage within a populated area might be, but the potential risk to the economy is high. If the EMP left hospitals without power, this would lead to the deaths of patients, some dying because of a failure of machines to keep them alive. Does this then constitute an act of lethal violence? Could we categorise acts that ultimately lead to such violent outcomes as violent acts? The possibility for cyber attacks to create violent acts such as these will be discussed in Chapter 7.

There is also a historical dimension to be considered as the type and degree of violence considered necessary to trigger war varies with time.

Invasion as a violent act of war has been prominent feature of armed conflicts before, during and after the twentieth century. In the 13th and 14th centuries, the Mongol Empire's quest for expansion meant that its violent incursions were received as an act of war by many of the civilisations it encountered. There was little legal procedure involved, but its *de facto* reality was plain.

It is unlikely that the death of an individual overseas would be considered grounds enough to warrant an act of war in the present day. In the case of the siege of the US Embassy in Libya for example, the death of J. Christopher Stevens did not persuade the United States to go to war in Libya. Though it later did engage in some military activity, some attempts at restricting flights over the airspace were made, and no armed forces were deployed on Libyan soil. Critically, it was not the Libyan government who engaged in the violence, although individual or group action against a foreign state has led to war in the past.

The inciting act of war in WWI is often considered to be the killing of the Archduke Franz Ferdinand by the Serbian nationalist Gavrillo Princip. 'The spark that lit the powder keg' was considered reason enough to justify the subsequent ultimatum by Austria-Hungary and the eventual invasion of Serbia, which brought with it, through a complex system of alliances, a global war (Joll and Martel: 2007).

The Arab-Israeli conflict provides examples of how a state can initiate wars that it interprets as self-defence, even involving pre-emptive attacks. The Israeli government's interpretation of the Six Day War is that the war was in self-defence. There is, however, a large amount of evidence demonstrating that it began in a pre-emptive attack (Schwedler and Gerner, 2008: 189).

This section illustrates that what constitutes an act of violence is contested and this forms part of a wider contest surrounding how we define acts of war within a given context. The significance of the intention, interpretation and reaction to acts of violence feed into how we define and classify acts of war. Analysis that fails to understand this lack depth. Responding to violence is a normalised rationale for war and a normalised vehicle for war. However, there is disagreement and uncertainty over what actions should be considered violent and the level of violence required before the threshold for war is reached.

2.2.2 Violation of Sovereignty

Several of the examples previously cited have another major element in common: the breach of sovereignty of one state by another. Sovereignty is a contested notion. It can be defined in a number of ways but is critically important to our understanding of acts of war. For example, the military invasion of another state is a breach of sovereignty. However, if only one soldier crosses the border would this give the victim state the right to respond with force? The following section will examine how the concept of sovereignty related to war and acts of war.

Walzer defines sovereignty as the liberty of states to exert their autonomy free from foreign control or coercion (2006: 89). There are two elements within sovereignty that allow a state to do this. Firstly, an internal sovereignty exists, allowing the state to be the ultimate authority above all other political institutions and bodies within a given territory (Bull, 1985: 8). Thus,

sovereignty can come from a lack of 'other' control within a given geographical area. Internal sovereignty relies on the authority looking in and derives its sovereignty in some senses from being the ultimate arbiter of control. Secondly there is external sovereignty that relates to the independence of the authority from other actors within the system (Bull, 1985: 8). It relies to some degree on the normative assumption that sovereignty should be respected by external actors (Bull, 1985: 8). Wendt goes further to state that '[s]tates recognise each other as having rights to life, liberty and property and limit their aggression accordingly' (1999: 324).

The reality of sovereignty becomes contested when one or other state is weak or absent. Walzer correctly points out that not all *de facto* independent states are sovereign, i.e., some do not have external recognition. States can have internal sovereignty, i.e., be recognised by their own populace as being sovereign without having recognition of external sovereignty by other states and vice versa. Equally challenging is in the case of states where sovereignty is legally present but nominally absent. In essence, it is possible to have a 'sovereign' state that despite not being recognised for possessing usually accepted characteristics. Recognition of states by others is important in wider international relations: some smaller states only exist because of the recognition from larger states (Wendt, 1999: 339). Because of its importance to states, recognition of sovereignty is a critical component of how states relate to each other. There is an element of normativity to sovereignty. It makes states adhere to certain rules and norms[3]. Fear of incursions against a state's own sovereignty may be enough to deter it from violating the sovereignty of others.

Having introduced the topic of sovereignty it is important to analyse what bearing this concept has on acts of war. To what extent does a breach of sovereignty entitle a state to react with military force? Walzer offers a rationale for the use of force in response: 'every violation of the

[3] Glennon (2005) writes on the issue of norms and war

territorial integrity or political sovereignty of an independent state is … aggression' (Walzer, 2006: 52). With regard to territorial integrity, Walzer envisions a direct invasion of some description. But not all such challenges to sovereignty are backed with military invasions. It is unclear how Walzer rates less aggressive transgressions against sovereignty like verbal or legal claims to territory. Political sovereignty can also come under varying degrees of challenge. Is it not possible to undermine a government, and thus reduce its sovereignty, without directly controlling or coercing its state level institutions?

Klein argues that strategic violence, including acts of war can be understood as states attempting to assert their sovereignty (1994: 7). This can take the form of invasion for example, where states look to expand their sovereign territory by annexing another state. It is also true in the case of foreign 'intervention' – where states exercise their power over another by intervening militarily within their sovereign territory. This also speaks to Bull's idea that states go to war, to preserve or extend sovereignty (1985: 185).

The idea of sovereignty is ultimately rooted in the legitimacy of the monopoly on the use of force within a given geographical space (Haatja, 2013: 315). Buzan and Herring argue that the use of force has the potential to expand a state's power and influence and consolidate its sovereignty, fail to do so, or even to undermine it (1998: 133). An act of war can, therefore, be a double-edged sword. The process underlying the decision to go to war is usually a calculated one according to Nye (2009: 26), with a state choosing to violate the sovereignty of another state using violent or non-violent means. Rules and norms of the international sphere play a role in determining how this will be received (Bull, 1985: 186). One can hypothesise a situation where a state is victim of a non-violent transgression against its sovereignty but and choses to respond with a conventional military response. Depending on how a state reacts to a given

dispute, over a perceived breach of sovereignty can in principle meet the threshold to be received as an act of war, even if minimally violent.

Where that threshold lies is a matter of social construction determined by how possible 'acts of war' are perceived, understood and reacted to within the context of sovereignty. How states choose to act on violations of sovereignty has changed over time, consequently the responses expected from violations of sovereignty could be expected to change. Problems will arise as a result of aggressor states being convinced that their violation of sovereignty does not cross the threshold if the victim state interprets events differently. Reliance on historical precedent could lead states to become complacent in this regard as the risk might be higher than they initially anticipated.

2.2.3 Identity and Ideology; wars fought for honour:

Where violence or violation of sovereignty are not considered the first act of war, then threats located in identity and ideology, or in certain cases breaches of honour can fill the role. The religious wars of the Middle Ages fall within this category, where the reason to go to war was not necessarily a violent attack in the first instance. Where the act of war is linked with identity, this can mean it is interpreted quite differently by opposing sides.

Religious fervour was the predominant reasoning behind the crusades. Thousands of men from Europe descended upon the Holy Lands to reclaim them from the perceived threat of heretics. War in this instance was made in defence of an identity rather than in response to any sort of violent act (Paine, 2001:24).

In the Daily Telegraph Affair, prior to the outbreak of WWI, Kaiser Wilhelm II managed to successfully alienate French, Japanese and Russian Empires while greatly insulting the British in an interview considered to be one of his biggest diplomatic blunders. Despite the grave insults to honour, and expressed disappointment of Queen Victoria over the matter, the matter resolved without immediate reaction (Joll and Martel, 2007). Going to war for the sake of stately honour has been diminished in plausibility as an act of war .

Modern examples of religious-identity driven wars are fewer, though some non-state actors provide useful examples of the link. Al Qaeda have cited pseudo-religious rationales for violence that garnered international attention, and later led to military intervention. The liberal and pluralistic ideals of the Western world, contras with the fundamentalist religious convictions of this group and enable it to justify its attacks to a wider audience. Al Qaeda is stateless, which complicates the relationship of its violent acts to acts of war. But the US response to 9/11, of declaring a 'war on terror' in 2001 indicates that a primarily ideological threat can be met with the conventional use of force in response.

Within several states, it is possible to discern a number of political actors that have justified violence by reference to militant religious ideology. Groups such as the Muslim Brotherhood in Egypt, the Islamic Salvation Front in Algeria and groups attached to Hamas in Lebanon and Palestine have all cited religious reasons to justify violent attacks (Schwedler, 2008: 392-4). ISIS combined such militancy with seizure of territory across Iraq and Syria. Their success in attracting foreign support for their cause illustrates the role of ideology and identity in fuelling violence.

While the tension between Russia and the United States never boiled over, the Cold War is also an important example identifying ideology with threat and provocation. Both countries' governments were on a war footing despite there being no direct military exchange between the two nations. Though realists might attribute the tension to power politics, also driving international relations in the period was the importance of ideology to society and identity. The proxy wars that both states became involved in were often justified on ideological grounds. Vietnam for example had limited importance in terms of military, strategic or economic resources. Even within former French Indochina, it represented only one of a number of troubled states coping with regime change post colonialism. The ideological standpoint of the North Vietnamese and the perception of a creeping threat from communism was key to moving the United States into a position where large-scale military force seemed justified.

Post-1991 and the fall of the Soviet Union, scholars notably Fukuyama (1993), believed ideological conflict would fade away. Others, like Huntington (2002), believed that the age of ideological warfare had passed, and the world would move towards civilizational conflict. Ethnic and cultural grounds rather than ideological ones would form the basis for future conflict. The 1990s saw the rise in ethnic conflict, notably in Rwanda in 1994 and later in Yugoslavia.

With time, the distinction between ideology and identity has come to seem less clear-cut. Ideology and identity str crucial to defining what constitutes an act of war for different social groups. In *Writing Security*, Campbell speaks to the notion that states (in his example the United States) generate a sense of inferiority and superiority between outsiders and insiders (1998: 196), often building a sense of fear surrounding the unknown. Value systems are an important part of social groups, allowing societies to assign a degree of worth to particular people, places, or things. Depending on the value system that has been generated and perpetuated at a national

level, a state may be forced to react if significant harm is perceived in by the public to a thing assigned high worth in the value system of the ingroup or nation.

Klein notes that war requires more than simply the gathering of material resources. Intrinsic to its organised violence is human resources mobilised by political identity (1994: 37). Identity fuels war as it lends legitimacy to governments. This makes it as important as military capabilities. Simply examining the discourse of the military may not be enough to develop a succinct view of the perceptions of identity and ideology governing a society's value system. Katzenstein, argues that collective identity and expectations can have very powerful causal effects (1996: 7). Campbell maintains that there are no stable identities as the identity of the state is contained and reproduced through its actions (1992: 11). This means states are constantly deciding and reaffirming what is valuable to them, via the policy choices they make, including those assigned to war and peace. Katzenstein notes the importance of rules and norms that 'define standards of appropriateness" (1996: 28). These rules however are subject to change, and how we define the standards of appropriateness is fluid. Therefore, while states still prepare and are organised to fight wars, norms change such that some grounds for war once considered normal may be seen as frivolous (Jepperson, Wendt, Katzenstein, 1996: 36).

Identity and ideology are a key element in examining how states transition from peace to war, because they play an important role in determining states' interpretation of events. As the identity and values of populations are subject to change, so the way in which actions are perceived is subject to change. This can lead to a disparity of views between states on the meaning of a given action. Depending on factors of identity and societal ideology, some societies may value things in specific ways, different from others. This opens space for states to react strongly against certain kinds of perceived threat or disrespect, even where no such threat or disrespect was intended.

2.3 The rational calculus of war:

If war is violent and leads to a loss of life, one could ask why rational states choose to use this method of using their power. Fearon (1995: 381) summarises the possibilities: '(1) anarchy; (2) expected benefits greater than expected costs; (3) rational preventive war; (4) rational miscalculation due to lack of information; and (5) rational miscalculation or disagreement about relative power'.

States go to war because there is an expectation that by doing so their situation will change in such a way that they are better off post-war than pre-war (Fearon, 1995: 379; Levy, 1984: 235; Suganami, 2001). This can include a desire to increase wealth (Aron, 1957) or expectation of a 'windfall of power assets' (Ikenberry, 2001:4). Wealth is an important factor as states will go to war expecting that they can afford the cost[4] (Keegan, 1994: 64; Fearon, 1995: 383). As states attempt to reduce casualties, the costs increase as weapons have to be more accurate. The US currently spends billions on this (Byford, 2002: 37; Strachan and Scheipers, 2014: 37). Then there is the cost that politicians have to face as a result of long wars, rising costs and casualties (Gat, 2001: 827-828).

States, meanwhile, have somewhat advanced beyond Clausewitz's idea of war as imposing will by force to understanding that the victim state retains some say in how that will is imposed (Heuser, 2013: 505). As such wars are not necessarily a pursuit of unconditional surrender (Cooper, 2—4: 55). Power remains central to war, it plays a major role in determining whether states choose to act or not (Baldwin, 1979). It may be fought to dissuade others from acting, or as a means of maintaining power within a region (Herz, 1951: 207; Mack 1975; Jensen, 2002).

[4] Warfare has also been impacted by privatisation which is linked to the high cost of maintaining standing militaries (Kaldor, 2012: 95-96).

2.4 Summary

For the purposes of this thesis, war is a conflict between two states typically characterised by exchanges of violence and may be accompanied by legal steps that limit or expand interaction between the two states. This thesis is concerned with how states transition between peace and war, triggered by some action that is considered by one or both parties to be an 'act of war'.

This chapter demonstrates that there are different types of acts of war: violent harm, violation of sovereignty or allegiance to ideology or identities considered unacceptable and honour related offences. We have noted, via reference to some historical examples, that there has been scope for change over time, such that the characteristics of an act of war in one period might be different than those of another. This scope for change means there is room for contestation at any given time about what states consider acts of war. Resultantly, the legitimate responses to actions will change too. The threshold for an act of war is a social construction. We can therefore debate where it lies, and answers may vary across and between societies. States often rely on precedent to guide their expectations, but it can be risky to rely on historical precedents when context has shifted in material ways.

The next chapter will examine how cyber attacks can increase the challenge of this zone of uncertainty, pushing us to consider potential shifts in how states interpret action.

Chapter 3 Cyber War

In the previous chapter we discussed the conceptual issues involved in defining war and acts of war. Technology has the potential to change not only the manner in which war is conducted, but also how rational actors interpret and handle certain situations where war is a possible but also avoidable outcome. Cyber space could be considered anarchical (Rovner and Moore, 2017) and thus we should be concerned with attempts to assert power that could be misinterpreted. Maness and Valeriano (2016: 78) note that nuclear states such as USA and China are more likely to posture using cyber in an attempt to assert power and status. Nuclear weapons brought about perhaps the largest change wartime strategy of any technological advance in history. Nye notes that as with nuclear weapons, the implications of cyber capabilities will take time to understand (2013: 13). Nuclear weapons have both an offensive and defensive aspect: the damage they can inflict is potentially enormous, but they can also be consequential while unused, a deterrent against an attack by an enemy. As new technologies are adapted for military use and integrated into the overall strategy for defending a country, cyber can similarly be used for offensive and defensive purposes. Cyber is a new technology and its use has hitherto been limited to small attacks. As a result there some ambiguities as to where cyber fits within the overall debate on warfare, and uncertainty as to whether war could be brought about through its use. This chapter shows how militaries are adapting cyber as a tool for foreign policy as well as outlining the more problematic issues this throws up.

Key to the argument of this thesis is the lack of certainty on the types of responses that a state can legitimately employ when they have been victim of a cyber attack. There is a potential danger in relying confidently on the restraint of the victim state to not employ military means as a response to a cyber attack. The history of cyber attacks thus far has been one where states have responded with restraint (Valeriano and Maness, 2016; Kreps and Schnieder, 2019: 3).

However there is a case to be made that this is reliant on prudential calculation rather than due to any robust or reliable norm. Due the relative newness of the technology, there has yet to be a wide-ranging test of how states would act in different eventualities. The question of the threshold after which a state might employ kinetic military force in response to cyber attack is important and unanswered as yet. We shall discuss it in the coming chapters.

Communications infrastructure provides the backbone of how societies function[5]. Through information pathways like the Internet, citizens have been able to generate income, make network connections and develop new ideas. Instant communications software has allowed state officials to communicate more effectively than in the past. As the opportunities to avoid conflict through communication have increased, so too have the possibilities for conflict as the internet connects everything, leaving information and dependent systems open or partially exposed creating threats to governments and industries (Shah and Mehtre 2013: 51; Thorton, 2015: 55; Arquilla and Ronfeldt: 2001: 14; Colorossi, 2015; Albenson et al, 2015; Duncan et al, 2014; Metz, 2012). The function of the Internet as a tool, communicator and as a source of information has meant the development of societal dependence on computers and information (Durante, 2015: 370). In 2010, a single-digit mistake crashed the New York Stock Exchange for several hours. The crashing of the Amazon Cloud service in 2013 was linked to a drop in an estimated 40% of internet usage for the period of outage (Dombrowski and Demchak, 2014: 72). While estimates of the potential damage of a more serious outage to major services exist, it is impossible to know what the actual impact would be on society or the economy. As our infrastructure becomes increasingly interdependent, what are the consequences for governments as they face a continuous barrage of cyber attacks to critical systems? As states increasingly try to use cyber attacks to achieve foreign policy goals, this changes the dynamics of their relationships with other states. The following sections will examine how we conceive of

[5] For more on the internet and connectivity see (Naughton, 2016; Pawlak and Barmpalio, 2017)

cyber, cyber space and cyber attacks and analyse the repercussions of these findings for the frontier between war and peace.

3.1 Militarisation of Cyber

'*Nation-states are spending more money in order to create their cyber capabilities and the role of using the cyber domain has been emphasised in national security and military strategies. This is just the beginning of the digital arms race, where the rules of engagement have not yet been codified*' (Limnéll, 2016: 51)

Increasingly cyber defence, and offence, has come under the purview of military control (O'Connell, 2012: 195; Precaido, 2012). It is necessary to examine this to understand how the military apparatus has become involved in the cyber realm and the implications of this for the overall development of cyber for use in war.

If cyber space is ungovernable, unknowable, makes us vulnerable, inevitably threatening and inhabited by threatening actors (Barnard-Willis and Ashenden, 2012: 116-119), then how can governments generate a coherent policy for their military to follow? The issue is incredibly challenging as states seem to accept that some regulation of the internet is required. However, there is simultaneous concern that any potential laws put in place may impact economies dependent on commerce, both domestic and international, facilitated by the internet. Despite the relative freedom of the internet, some rules have developed independently. However, there is recognition from academics that protection against cyber war is beyond the capacity of most private citizens or private institutions much like the protection against fraud and thus further policy and law-making is required (Barnard-Willis and Ashenden, 2012: 113).

Military forces come under the jurisdiction of international law, which constrains their freedom of action; torture of prisoners of war is forbidden, for example. However, because of the highly integrated and unregulated roll out of the internet in the past three decades, standards for international conduct have been difficult to establish or enforce. Many specialists in international law have cyber at the top of the agenda (O'Connell, 2012: 188), but there has been little by way of international agreement on regulation for cyber space. International law would, in theory, specify the combatants and constrain their actions to military targets. Currently, both military and civilian targets are subject to cyber attacks (Durante, 2015: 370), which creates potential for cyber attacks to violate the rules of armed conflict, though there has been no recorded death as yet as a result of a cyber attack (Farwell and Rohozinski, 2012: 109). The lack of precedent for dealing with cyber attacks has led to some ambiguity over how states should respond. However there have been some attempts in recent years by militaries, notably NATO and the US to create policy for their overall cyber defence strategy (O'Connell, 2012: 188; Ilves, 2016). Cyber became a part of NSA policy in 1997 (Black, 1997: 1). However, despite the growing trend towards cybersecurity in policy documents, there has been relatively little discussion about when a cyber attack becomes more than 'interference' and when it might rise to the level where it might be legitimate to respond with a use of conventional military force (Dever and Dever, 2013: 28).

The cyber attacks on Estonia in 2007 are considered the first national-level cyber attack that came to the attention of the media (Li Zhang, 2012: 801). The academic and media consensus is that Russian actors, either with direct or tacit government consent, were the aggressors in this instance. Estonia suffered a number of website outages, including several of their government departments and one of their major banks. The damage to the Estonian economy has never been officially quantified however the attacks showed clear holes in the Internet security of the state

and the Estonian minister went as far as to claim that the attacks were an act of cyber war (Traynor, 2007). Subsequent Russian attacks on Georgia were arguably more aggressive and did greater damage (Korns and Kastenberg, 2009: 60).

Estonia being one of the most cyber dependent and integrated countries in the EU, the damage to the economy could have been severe. Also, as a member of NATO, it was important that there was a unified response to the attacks. While NATO did not choose in this instance to respond to the attack with a cyber attack of its own, it chose Tallinn as the place to build its new Cooperative Cyber Defence Center For Excellence (O'Connell, 2012: 193-194). As a NATO member, Estonia could in principle have demanded a military response to this attack, requiring the organisation to make a difficult decision (Ducaru, 2016: 183). While NATO chose not to act directly, it is plausible that the placing of the centre for cyber defence was an attempt to on the one hand placate the Estonian government and people, and on the other to send a message to potential attackers that future attacks would not be tolerated. This fits within the idea of deterrence, though its effectiveness in this particular case is uncertain. Fuller discussion on the Estonian cyber attack case will be in Chapter 6.

Over the last two decades, states have begun to incorporate cyber and electronic warfare within their military doctrines and strategies. The change that this represents is twofold: firstly, it indicates that there has been a shift in understanding regarding the need for a national cyber security to meet new kinds of threat. Secondly, this change shows that states are expanding their military's national security brief to include the cybersphere. Much of this work involves shoring up defence (Buchanan, 2016; Gartzke and Lindsay, 2015; Colbaugh and Glass, 2011), including but not limited to, some of the issues highlighted by Thomas Rid: espionage, sabotage and subversion (2013). There has been some semantic debate as to whether this constitutes warfare (Bledstein, 2019: 107). Chinese military strategy takes into account the need for cyber

and electronic warfare (Lewis and Tamlin, 2011: 8), emphasising the need for the state to well prepare to deal with cyber attacks that could potentially damage national infrastructure. However, China has also developed a reputation for illegal hacking of infrastructure of other countries, notably the US and South Korea. The Chinese military arguably takes a more offensive posture than defensive when it comes to the cyber sphere (Bledstein,2019: 105). The United States Cyber Command (USCYBERCOM), works alongside but outside of traditional military apparatus (Lynn, 2012). Preferring to pair the cyber aspects of national foreign policy with intelligence, the US government has attempted to delineate between military and security functions of cyber. Operation Olympic Games, which brought Stuxnet to the world beginning in 2007, was borne from the beginnings of USCYBERCOM which was then a NSA/CIA led organisation. NATO does not define cyber attacks as clear military action, while USCYBERCOM LG Keith Alexander has explicitly stated that the US reserves the right to respond to cyber attacks on DoD systems (Farwell and Rohozinski, 2011: 30-32). Thus the military are willing to take a leading role in the response to attacks on offensive installations.

Israel has had some success with integrating its cyber policy within the framework of its military complex, through combining cyber attacks with traditional use of force. A 2007 attack by Israel on Syria was in part an act of cyber warfare, because the hacking of Syrian radar systems ultimately ended with the destruction of a facility. Thus the cyber attack ultimately achieved or partially achieved military goals (McGraw, 2013). As the primary target remained something other than people, this may have influenced the cost and risk calculations of the policy makers, as well as how attacks like these are framed (Rid, 2013: 57).

The US has also had some success in integrating cyber into its strategy. Academics such as Kehler, Lin and Sulmeyer (2017) have argued that the US has been successful in integrating the concerns about cyber into kinetic escalation while understanding the nuances of this new

method of conflict (also Lilienthal and Ahmad, 2015:399). Writing in 1970, Osgood argued that the US has traditionally has adapted well to new threats however the approach has always been ad-hoc, and this has continued with cyber strategy[6]. While there have certainly been advances in US thinking, it is not clear that there is a distinct threshold for what constitutes an attack meeting a conventional military response within their strategy. Flexibility regarding new threats and challenges is central to US thinking (Hammes, 2006: 273; Securing cyberspace for 44th Presidency CSIS, 2008). 'US military doctrine permits offensive cyber operations for 'damaging or destructive purposes' as long as they are conducted in accordance with the laws of war (Office of General Counsel DoD, 2015: 340). If Arquilla and Ronfeldt (2001: 351) were correct in suggesting that the US can set the standards for inter-state cyber relations, then Stuxnet and its subsequent doctrinal posture, suggest offensive cyber actions might become normalised practice.

Farwell and Rohozinski (2011,32) pose an interesting question: how far is the United States willing to go deploying its cyber capabilities in service of the goals of deterrence and pre-emption/prevention adopted after 9/11. They have already shown their willingness to take offensive sabotage action through the use of Stuxnet and other malware connected to Olympic Games such as Flame. Through the use of Prism and other aggressive data-harvesting NSA programmes, the United States has been implicated in the collection of data records on thousands of foreign citizens. Furthermore the continued support for anti-censorship software for use in countries such as Iran is arguably an act of deliberate subversion.

The remit for cyber defence goes beyond what private citizens and insitutions can be expected to handle alone; it requires government. While issues like fraud, and intentional damage to property or people are typically deal with by law enforcement rather than the military, the

[6] Also see (Fischerkeller and Harknett, 2017)

international dimension of many cyber attacks changes how states choose to tackle them. It is for this reason that many states have begun incorporating much of their cyber defence strategy into military and intelligence agencies rather than domestic security policy.

All levels of the US military now encompass some cyber divisions (Dombrowshi and Demchak, 2014: 73). USCYBERCOM fits within a military chain of command thus allowing the various branches to use information and tactical elements of the group. The United States is not the only country to do this. Russia has had its own cyber command since 2017 but has been developing cyber capability since at least 2004 (Cimbala and McDermott, 2015: 104; Thomas, 2014: 104). China has already integrated cyber forces within their military capability though they contest this (Brownlee, 2015; Pollpeter, 2015: 137-157). Some non-state actors such as Al-Qaeda could have 90% of their military efforts focussed within cyberspace (Dombrowshi and Demchak, 2014: 76). Thus, there is doubtless a military focus on how to handle the issue of cyber, defensively and offensively. State officials have accused China of outsourcing its cyber attacks to third parties (Farwell and Rohozinski, 2011: 26). Even without outsourcing its offensive capabilities to other parties, there is a degree of concern within the Chinese government over the degree of cyber attacks directed at its own infrastructure. China's cyber defence policy is based on 80,000 attacks per month (LiZhang, 2012: 805).

There are command and control issues within cyber (Miller I, 2011: 23). While Sanger remarks that Olympic Games was approved by two administrations (Bush II and Obama), it is not clear how the chain of command works in this instance. Who has final authority over a cyber attack? (Junio, 2013: 129) If it is the NSA then does this make them combatants if a war breaks out? If escalation occurred between the US and China, who would ultimately be making the decisions regarding sending another cyber attack? These issues are made difficult by the closed nature of

the decision-making process. The ultimate arbiter in this instance would be the president, but does a president oversee all elements of tactical deployment in a war situation? This is doubtful.

The ease of creation of cyber weapons changes how we perceive their use and potential impact. If offensive capability is more cost-effective than defensive capability – anti-malware programs are still consistently subverted (Farwell and Rohozinski, 2012: 11; Fischerkeller and Harknett, 2017: 391) – then a policy of developing and employing them seems logical. This has the potential to lead to serious escalation issues when examining Offence-Defence Balance theory (Locatelli, 2013: 10; Jervis, 1978; Glaser and Kaufman, 1998; Van Evera, 1999; Adams 2003). Cyber may not cause conflict in and of itself, but the militarisation of cyber makes the decision to escalate easier and cheaper (Saltzman, 2013: 41). The potential damage of the weapon is critical in calculating what type of retaliation to expect argues Luttwak (1987: 231), however given the lack of empirical data on which to base predictions, cyber attacks are problematic in this regard.

"The logic of asymmetric advantage in cyberspace assumes that barriers to entry for weak actors are falling while the vulnerabilities of strong actors are increasing" (Lindsay, 2013: 375[7]; Dever and Dever, 2013: 26). This is in essence changing the way policy makers think about the cyber sphere. Despite a large amount of cyber security focus in recent years, it may still be possible for smaller states to fund espionage or sabotage within larger states' networks. Countries like the UK and the US where economies are heavily dependent on the internet, would suffer massively in the event of a widespread cyber attack. A small team within the NSA/CIA designed Stuxnet, a worm that has become the most famous cyber attack to date. At a time when the Bush administration was heavily invested in Iraq and Afghanistan and even with a limited

[7] Lindsay later disputes this notion stating that states are less likely to engage.

budget, they managed to infiltrate one of the most secure locations on the planet with malware and take advantage of vulnerabilities within the software.

3.2 What is Cyber War?

In 1993 John Arquilla and Donald Ronfeldt published a controversial article stating that cyber war was close at hand. Over twenty years on, Scholars continue to debate the significance of cyber war and the impact that it could potentially have on human life. Much of the debate centres on the type of harm that could be done with a cyber attack (Heim, 1993; McGraw, 2013; Stone, 2013, Gervais, 2012; Liff, 2013; Lawson, 2013; Akdag, 2018; Black 1997[8]). In more recent years, however, there have been a series of challenges to the concept of cyberwar, foremost by Thomas Rid (2012), who emphasised that there has never been a cyber attack where a human has been injured or killed. In the previous chapter we examined war from a number of standpoints, noting most definitions include violence against humans if not explicitly then implicitly (Clausewitz, 2000; Bull, 1985; Walzer, 2007; Sitara Noor, 2014: 14-15). However absence of precedent does not predict with future outcomes with certainty. Russell (2017: 53) notes that nuclear conflict was empirically unlikely pre-1945 as the weapon had not existed and therefore there was no precedent for using it. Freedman notes that 'an imagined cyberwar was the natural culmination of a yearning for non-kinetic wars, forms of engagement that would disarm and disable a whole society without mass slaughter' (2017: 238). However it could also be argued that in the attempt to avoid conventional conflict, aggressive deployment of cyber could potentially lead to further tensions among states (Lonsdale, 2018: 423; Jenkins 2016, 108; Burton, 2015). Cyber attacks may be conceived to avoid 'boots on the ground' and reduce military casualties (Singer, 2010: 207-208; Libicki, 2016: 139), but there are possibilities for inadvertent escalation as cyber and its impact are poorly understood (Kosenkov 2016: 5-8; Libicki 2009; Floridi and Taddeo 2014). How does cyber fit within those traditional war

[8] Kan (2013) provides an excellent summary of the prominent debates in cyber. Futter (2018) notes the disparity among academics regarding their views on cyber.

frameworks? This section will consider this, drawing from some of the previous section to illustrate how cyber can be used to achieve foreign policy goals, but also how this in turn has the potential to be damaging to drive conflict between states to the point of war.

Cyber warfare can be understood as a form of Fourth Generation Warfare, a form of warfare driven by technological change that has the potential to impact civilian and military targets. What Lind et al (1989) argue is that this technology will come with opportunities for new tactics and strategies but will introduce new vulnerabilities into the system. The clear delineation between civilians and combatants becomes murky under this categorisation. Lind et al (1989) predicted the potential for cyber attacks to disrupt military and civilian targets using this form of warfare.

The scholarly work on cyber falls into four broad areas. The first attempts to examine the technical side of cyber attacks. The second examines the definition of cyber war. The third discusses whether such an event is possible or likely. The fourth considers the impact of cyber on other literatures such as attribution and deterrence and the legal aspects of cyber war. This section will examine each of these briefly. Beginning with the technical literature we shall indicate how cyber can be used as a destructive force and as a tool for states to impose their will on others. Secondly, this chapter shall also examine the problematic area of definitions within cyber warfare, distinguishing crucially between a standard war where cyber capabilities take an active role, and an, as yet, hypothetical war that takes place or at least begins entirely through cyber means. This question of definition has significant implications for the discussion over future likelihood. Finally, there is the relevance of cyber to other areas of traditional study or warfare, and vice versa, including attribution and deterrence, these also be discussed. There is a

large strand of literature that examines the legal aspects of cyber attacks[9]. These cover many of the areas discussed in Chapter 2, sovereignty, kinetic damage and what the lawful use of force pertains to. This thesis does not engage directly in legal argument though it does engage with some of the arguments presented in this literature.

Much of the literature on cyber is focused on the technical aspects (Lewis and Tamlin, 2011), (Langner, 2013), (Denning, 2012). This is useful for understanding the damage that can be caused by cyber attacks and gives a layer of context for postulating the potential scale and outcome of a targeted cyber attack. The information contained within these articles indicates that cyber attacks are growing in scale and that their precision can be pinpointed to specific industrial machines. The damage caused to an electricity generator by a military cyber attack exercise at the Idaho National Laboratory in 2007 serves to indicate the potential lethality of cyber attacks (Meserve, 2007). Since 2007, the world has seen several malware programs designed to attack specific targets, mostly in the Middle East: Stuxnet, Duqu, Flame and Gauss are just a handful of examples (Rid, 2014: 32, 93, 95, 97). It is almost universally accepted that Stuxnet will become the blueprint for many future malware programs, both on the part of states and private actors (Singer and Friedmann, 2014: 158-159), (Zetter, 2014), (Fidler, 2011).

US Department of Defense documents potentially provide an insight into the perception of policy makers of cyber attacks as a means of conducting offensive operations without going to war. The DoD defines the purpose of its cyber strategy as "to guide the development of DoD's cyber forces and strengthen our cyber defence and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DoD's three primary cyber missions" (2015).

[9] There are a number of legal scholars who have examined cyber and problematised the issues of its legality (McGhee, 2015; Mele, 2014; Payne and Finlay, 2017; Dunlap 2011; Jensen 2002; Schmitt 2010; Skelerov 2009; Valuch et al, 2017; Bellovin, Ladau and Lin, 2017; Hathaway et al, 2012; Skelerov, 2009; Lawson, 2012; Mavropoulou, 2015). Those who have looked at international law particularly (Bryans, 2017; Schmitt, 2013; Simmons, 2014; Stockhurger, 2016; Malekos Smith, 2016). Examination of sovereignty and cyber (Broeder, 2017; Buchan, 2012).

These three primary cyber missions are: defence of the DoD network; defence of US homeland and national interest; and the provision of "cyber support to military operational and contingency plans" (DoD, 2015). While the rhetoric of the DoD is rooted in defence and protection of national interests, there has been some headway in the planning and creation of a cyber mission force which includes combat mission teams, with the aim to "Provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations" (DoD, 2015). There is no policy document that directly considers at what threshold a cyber attack might become an act of war. Thus it is difficult to stipulate precisely how policy makers officially regard the deployment of malware programs such as Stuxnet designed by NSA operators. But from context we can reasonable infer they are considered an instrument short of war. Rid posits that in the future there will likely be cyber attacks where humans get hurt, but under his framework, these would be considered sabotage rather than warfare (2013: 79). As no one has yet died from a cyber attack, the first death might likely change perceptions as to how acts of cyber aggression are interpreted and reacted to.

It is important to distinguish between what we mean by a cyber attack and what constitutes cyber war. As we saw in the previous chapter, war involves both destruction and exploitation. The destruction comes from the force required to compel the opponent to make decisions that would not necessarily be in their interest. In addition to this, war is exploitative: the nature of its political existence hinges on perceived benefit to the aggressor (Durante, 2015: 396). Cyber has the potential to fit within this framework, but there are a number of issues with the destructive element that will be raised in the following sections.

The starting point for the debate over whether cyber attacks can be considered an act of war begins with Thomas Rid (2012). Rid has stated categorically that there will be no Cyber War and that the attacks will continue to fall under other frames of reference: sabotage, espionage and

subversion. The cyber warfare 'problem' in essence is as Lucas Kello describes: "because cyber weapons are not overtly violent their use is unlikely to fit traditional criterion of interstate war; rather, the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace – with important consequences for national and international security" (Kello, 2013: 8). It is arguable that Stuxnet was a military operation, designed and performed to satisfy military ends through military means. Sabotage, as Thomas Rid defines it, however, does not constitute an act of war (2014: 19). Given the innate differences between cyber and kinetic attacks, Taddeo (2018: 325) argues that it is not helpful to make analogies between the two. But as cyber crosses into the kinetic attack domain or at least into the space of potentially producing harmful outcomes comparable to kinetic military atttack, it is worth reflecting on how robust the asserted distinction between the two will remain.

John Stone, pushes back against Rid's claim that cyber war will not take place (2013). When examining Clausewitz, Stone argues, there is an importance attached to force, especially when connected to violence as a means for conducting warfare (Stone, 2013: 105). Rid's thinking focuses on on force begetting lethality rather than force leading to violence as Stone maintains is the Clausewitzian logic. Technology is a force multiplier, and when applied to the battlefield, it can produce far more violence than the force input (Stone, 2013: 105-6). He questions Rid's conception of war for its insistance on human casualties. But by Rid's conception, Stone argues the entire liberal way of conducting warfare could be seen as a form of sabotage, albeit on a grand scale (Stone, 2013: 105).

Gary McGraw uses the example of Operation Orchard in 2007 as the preeminent case for referring to a cyber attack as an act of war (McGraw, 2013: 112). By combining a cyber attack with strategic bombing of a facility, the Israeli government successfully integrated cyber into their wider military goals. Without the cyber attack, the Israeli fighter jets would have been

seen on radar and it would have allowed the Syrian regime an opportunity to respond before the threat was fully realised (McGraw, 2013: 112). An act of war has to have a kinetic effect according to McGraw's logic. Therefore cyber intrusion and espionage would not be considered acts of war in line with the Rid framework (McGraw, 2013: 112). But Chinese cyber attacks are often referred to using the language of 'warfare' despite the fact that they are merely espionage (Bledstein, 2019:2015). Such means can be useful to a weaker state which can execute cyber intrusion without breaching a threshold to trigger a violent response. States such as the US with a large military apparatus are still as vulnerable to espionage as smaller states, but the relative high cost of military action can shield a smaller state against reprisals (Bracken, 2017: 152). Espionage can potentially have a high economic cost, as businesses and industry can be particularly susceptible (Bechtsoudis and N. Sklavos 2012: 1755). Indeed, Bledstein (2019) argues that cyber espionage might be considered a new form of economic warfare (also Inkster, 2017: 31). However while the cost of large scale cyber attacks can be high, the average cost of smaller attacks is limited to $200,000, meaning their actual cost is significantly lower than that of warfare (Romanosky, 2016). Kilovaty (2015: 215) argues that until cyber is better understood by the international community, serious economic damage should be considered as an act of force. But Funn Cavelty (2012: 31) argues that treating cyber attacks on economic targets as merely espionage would helpfully de-securitise the issue, even though the economy is important.

When it comes to the question of what actions trigger war, Rid makes valid points but his is a rational decision-making model that does not give weight to the risks arising from divergent perceptions, leading to divergent calculations on each side. Rid is dismissive of the role of victim state escalation because there are no examples where war has been declared as a result of a cyber attack. While Farwell and Rohozinksi remark on the importance of critically examining how countries respond to cyber attacks, Rid appears to assume he threshold for war has a fixed

and objective quality rather than a social construction as others contend (Barnard-Willis and Ashenden, 2012: 110). The conceptual framework that this thesis posits is centred on a fluid notion of what war is and what constitutes acts of war. This contrasts with Rid's too-static conception. It is important to examine the both intentions and expectations of the actor who uses a cyber weapon and the subsequent interpretation of this attack by the victim state.

3.2.1 Aggression and Cyber War

Our understanding of whether cyber attacks should be considered acts of war is made difficult by the previously discussed lack of settled clarity of what constitutes war (Stone, 2013:101). The introduction of the cyber element intensifies the challenges because it does not fit within traditional paradigms of how war is fought. Damage only to objects rather than people seem to contradict much of the traditional literature's conception of 'war' including that of Clausewitz and others. There are also significant legal puzzles to resolve as to how cyber sits within or outside of a warfare framework. For example there are disputes over how to classify cyber attacks specifically; in a cross-border cyber attack, there is in one sense a clear violation of the rights of sovereign territory, but there are scant regulations regarding how this type of virtual incursion should be policed (McGhee, 2013: 86). Therefore there are issues over the definition of what is illegal: does cyber count as use of force? Lewis argues that a cyber incident that produced injury or death could certainly be an act of war (2015: 41). Could cyber attacks be construed as a form of intervention or aggression? (Fidler, 2011: 57). Answering these questions is not helped by the lack of dialogue among the international community. The nature of the internet has meant that it may prove increasingly difficult to prove the perpetrator of an attack in any event, making regulations difficult if not impossible to impose on states even if they should be agreed.

Rid breaks down Clausewitz's view on war into three separate elements: war must be political, instrumental and violent (Rid, 2012: 7-8). The cyber warfare 'problem' in essence is as Lucas Kello describes: "because cyber weapons are not overtly violent their use is unlikely to fit traditional criterion of interstate war; rather, the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace – with important consequences for national and international security" (Kello, 2013: 8). Rid uses the classical Clausewitzian notion of violence: war has to be physically violent (Rid, 2012: 7). This leads to a strong implication that an act of war must take the form of an act of physical destruction.

Rid's arguments neglect escalation mechanisms, however (Junio, 2013: 125). Cyber attacks perceived in a certain manner could provoke a kinetic response -something which Rid treats as improbable. In this case it would likely be a matter of dispute whether the initial 'act of war' was the cyber attack or the retaliation. Furthermore, his concerns seem to focus on the probability of cyber war, which he deems low. However as Scott Sagan points out, nuclear war might be improbable, but is nonetheless sufficiently probable that we worry about it (Junio, 2013: 129-130).

It is important to draw a distinction between two understandings of a possible cyber war. In the first instance, the state may conduct cyber attacks alongside a traditional military show of force. The cyber elements fit within a broader array of capabilities used by the military to achieve their objectives. Whether or not this merits the label 'cyber warfare' is debateable. If an initial cyber act were considered grave enough to warrant a kinetic military response then this seems like a good candidate. However if, as in the case of Operation Orchard in 2007, a cyber attack is simply the fore-runner of a conventional military assault then this is more dubious. The second conception of a possible cyber war is one that is fought entirely within the cyber sphere where conventional means of warfare are employed. This raises a definitional question of whether war

must be conducted in the physical world or if the term can be applied to conflict conducted purely through networked computer systems. To what extent must there be a spill over from the cyber-sphere to traditional warfare for a state to consider itself at war? This is where the Reception Phase in the model used later becomes important. An action in itself may be aggressive but it is the interpretation and ultimately the reaction that defines how the initial action is framed within a wider context.

2.2.2 Cyber war and kinetic impact

Damage to computer software can cause severe damage to a state's economy, but as yet there have been no declarations of war as a result of this kind of cyber attack. More fraught still, is a cyber attack that inflicts some level of kinetic impact: physical damage, to and via a computer or computer controlled system, which in certain scenarios might lead to explosions or other outcomes recognisable as violence, as conventionally understood.

McGraw argues that cyber attacks must have a kinetic effect if we are to consider them actions worthy of the term cyber warfare (2013: 112). This fits the parameters set by many definitions of war discussed earlier. Kinetic impact refers to a physical reaction or change in an object's state of being due to an external force acting upon it. But by this definition there have already been cyber attacks with a kinetic impact: at the Idaho National Laboratory in 2007 where a cyber attack was used to cause a generator to explode in an experiment. The boundaries of what is 'kinetic' may also be contestable. Suppose a cyber attack manages to change an operating system in such a way that it makes a network unusable? A zero-day exploit, as used in Stuxnet, could in theory bring down a series of linked computers requiring even the in the best case scenario that their owners wipe the hard-drives and reboot from a backup. Perhaps this threat could be merely time consuming not lethal. However as Farwell and Rohozinski point out, it is unclear how much damage would need to be done in order for such an action to be considered an act of violence (2011: 34).

A theme within the violence literature in the previous chapter was that one can in principle be violent without striking a direct physical blow. As noted in the last chapter, Finlay et al (2018) noted the possibility of non-violent harm. Farwell and Rohozinski remark that the failure of a successfully planted bomb to explode in New York would still be considered an act of violence and posit this could be show of force no less than the Stuxnet worm (2012: 113). *Potential* to do physical harm is considered in regards to bombs but not cyber attacks currently, which might lead to ambiguity when examining possible responses to a cyber attack. Stuxnet was designed to halt the progress of uranium enrichment however the worm caused serious damage to a number of nuclear centrifuges in the process. Damage to property remains an important factor in determining how an act of war is perceived by the victim state as property can represents a value, which may be weighted higher or lower than human life depending on the context and actors. In the case of the movement of the Soviet war memorial in Tallinn, a purely symbolic offence, was the rationale behind a series of cyber attacks on Estonian government and financial websites.

As we will highlight in the following chapters, the Stuxnet attack contained a danger of lethality as the operators had no way of knowing how the Iranian centrifuges would react to interference with their standard operating procedures. The spinning elements of the centrifuge are dangerous when operated at high speeds, something Stuxnet was designed to do. There was a danger therefore of exploding centrifuges, and the possible irradiation of scientists nearby (McGraw, 2013). Even without the potential lethality, the potential cost of a cyber attack could be extremely high (Junio, 2013: 131-132). If simple mistakes can cause the NYSE to crash then the cost of a serious coordinated assault on such an important financial institution could be catastrophic.

3.2.3 Practical Challenges: attribution, deterrence and law

If governments begin to think of cyber as a realm through which war can be conducted, this raises a number of concerns. Cyber war has the potential to radically alter the nature of international conflict, it provides a unique set of tools adaptable to many situations. However if we are to consider cyber attacks as potential acts of war, this raises some practical problems. One is the issue of attribution. Is it possible to accurately place blame when tracing the origin of a cyber attack is troublesome and time-consuming? Can cyber strategies incorporate an element of deterrence? Finally how do laws impact the development of cyber attacks for defensive and offensive purposes? As discussed previously, war is a regulated legal space: how can cyber be duly regulated by law?

A high level security breach into the US Bureau of Industry was never attributed, which is problematic as the state looks to respond (Brenner, 2007: 379-380). How can governments and militaries deal with the issue of anonymity and attribution in relation to cyber attacks? As discussed previously, acts of war are dependent on there being an aggressor and a victim. This framework is hard to apply if there is no identified aggressor to accuse of committing the act of aggression. That said, there have been significant advancements in the area of tracing online activity and thus this may reduce the problem. If a state has been attacked with a cyber weapon requiring a rare degree of expertise and substantial resources to design then it is can be inferred that a state rather than independent actors is highly likely to be responsible. In this way, Symantec and Kaspersky Laboratory both deduced that the Stuxnet worm was developed through state funding rather than by a lone group. There is, of course, a potential downside for victim states to identifying alleged perpetrators, as identifying a perpetrator might add pressure to act on the information by retaliating (Steiger et al, 2018: 79; Buchanan, 2017: 142)). Thomas Rid provides some interesting analysis of how to achieve feasible and practical attribution (2013).

Deterrence[10] is a critical element of modern armed forces as the principle relies on being able to do enough damage to a potential aggressor to make war appear to be a less advantageous decision that without it. Nuclear deterrence is a useful indicator of this as it presents the most recent technological advancement in the history of armed warfare prior to the introduction of cyber weapons. Indeed, Nye (2011) notes that there is much we can learn from nuclear when examining cyber attacks. However nuclear deterrence was not without its potential problematic elements: electronic warfare was seen to have potentially escalatory impact on nuclear deterrence as it weakened early warning systems. (Posen, 1991).

The ability to deter attacks is important in inter-state conflict as it affords states a degree of safety within which to act. Deterrence provides a limit on escalation, as the state acting will be aware of the risk to themselves. Cimbala (2014) argues that there is a strong temptation to trust in the assumption that nuclear deterrence will remain stable. Unlike cyber, nuclear has a series of norms and a shared framework of understanding that can limit the risk of its use by states (Buchanan, 2017: 103). Cyber does not necessarily provide comparable ability to deter further cyber attacks, although some argue through having vastly superior cyber offensive capabilities, the US can deter escalation because other states will fear a more destructive response (Gompert and Libicki, 2015: 9). But the lack of a shared framework remains problematic and undermines notions of a stable deterrence. Kliem argues that because of the uncertain efficacy of deterrence for cyber attacks, there is a need to find better methods of insuring security than relying on this (2017: 370).

[10] For more on deterrence see (Inkster, 2017; Osawa, 2017; Nye, 2016; Burton 2015; Sharma, 2010, Taddeo, 2018; Buchanan, 2016; Stevens, 2012; Lindsay, 2015 2)

The nuclear arms race was accompanied by the doctrine of mutually assured destruction and by institutionalised arms control, which is notably absent in cyber (Eilstrup-Sangiovanni, 2017: 404) Nuclear deterrence has arguably afforded states to co-exist, if not peacefully, certainly with less outright conflict than would have been achieved in previous centuries. There is a natural desire to rely on retaliation to deter potential attacks (Gompert and Libichi, 2015: 9). However the nature of cyber attacks and the norms that have become associated with them present a new challenge. While previously, an attack on a sovereign territory could have been deterred by the threat of a military response up to the level of a nuclear strike, now the situation has become more complicated. cyber attacks can be many or few, it may be difficult to assess who the perpetrator is, and traditional deterrence methods simply may not work. Cyber provides an active method of intervention within foreign territory in a manner that traditional military options could never be (Durante, 2015: 379).

However, it has been argued that deterrence can be applied to the cyber case – specifically in the case of Estonia post 2008. For example, the creation of the NATO hub for cyber defence in Tallinn as a result of cyber attacks could be construed as a deterrent against future attacks (O'Connell, 2012: 188-189). We might wish to resist the temptation, however to consider cyber as independent of all other forms of military strategy. If, as Dombrowski and Demchak assert, all levels of the US military have taken on a cyber dimension, then cyber becomes an inherent part of a wider military strategy that can act as a deterrent (2014: 74). Thus, while deterrence may be concern for a cyber attack in isolation, it still forms an important part of the total military apparatus as will be discussed in greater length in later sections.

Being at war puts certain restrictions on the civilian and military populations of a state. Perceiving cyber war as a war in its own right 'implies the applicability of laws of war, specifically principles of non-aggression, non-intervention, proportionality, discrimination and

respect for neutrality' (Gompert and Libicki, 2015: 8; Korns and Kastenberg, 2009). But many armed conflicts have taken place in the past have that deviated from one or more of these factors. Nevertheless, importantly states continue to operate under the guise of adherence to these rules in some forms or other, and their policy process and its decisions reflect this. Cyber, therefore, as a weapon, must be embedded and constrained within a wider legal and political system that reflects these principles.

3.3 Potential unintended consequences

We have already seen details of the nature of cyber attacks and how targets can be chosen and attacked with great precision. However as with the use of all weapons, there can be unintended consequences. Cyber weapons may be designed to try to avoid this (Farwell and Rohozinski, 2012: 108). A cyber weapon might be created to damage a specific system, for example, and programmed such that if it were released into the wild, it would not impact other systems, only the one it was coded to attack. However, while conventional bombs can be limited to a certain impact range and are immediately destroyed on use, cyber weapons, once in the wild can be adapted to attack other targets and can be reused with minor tweaks, making them a larger threat to the wider community (Kello, 2017: 122). Cyber attacks may not fall under military standards for collateral damage as there is not a strictly kinetic damage output (Romanosky and Goldberg, 2016: 16). But the fallout from its deployment could affect civilians significantly, breaching a norm of conventional warfare (Gross, 2009: 242).

While Operation Orchard was arguably a success, in that it managed to perform the radar blackout without any unintended consequences, there have been a number of malware weapons that have been unintentionally escaped into the wild. Flame, Duqu and Gauss, other elements of the overall strategy to extract information from Iranian officials and civilians eventually came

into the public domain, causing damage to computers worldwide. A further unintended consequence is that a cyber weapon may originate in one state but be reused or repurposed by another, in which case, it is unclear where the responsibility for software lies (Buchanan, 2016: 51; Cusumano, 2004: 27). Kehler, Lin and Sulmeyer (2017) note the importance of context to understanding attacks. Whereas any nuclear attack invited reprisal in kind, there is still much uncertainty, and therefore scope for divergent interpretations, as to what types of responses a cyber attack might require (Axelrod and Iliev, 2013: 119).

It is possible that a cyber attack could cause more, or indeed different harm to that that was intended. Stuxnet infected 50,000-100,000 computers, of which, 58% were in Iran. A large proportion of the infected systems were running the Siemens Step 7 software, which Stuxnet had been specifically designed to target. These specific infections made up 67% of Iran's overall infection numbers but only 13% of the rest of the world (Chen, 2010: 91). The initial attack was designed only to infect Iranian computers at a specific location but spread rapidly. A cyber attack too, on a power station for example might have more damaging impact because the attack had not anticipated a specific device being on site. There is considerable room for attacks to cause considerably more harm than intended.

3.4 Determining when a cyber attack becomes an act of war:

We can better understand the problem of threshold by examining the literature on escalation. A problem of escalation, set out by Smoke, is the risk that another state might misinterpret a decision that the acting state has made (1977: 6). The essence of escalation is that a state that has been acted against responds with a more severe action. An especially serious escalatory step is one that shifts a relationship between two states from peace to war. In the literature on escalation, signalling is a key concept. However, Carson and Yarhi-Milo that there are problems

with applying traditional signalling literature to cyber, as most attacks are undertaken with the expectation that they will not be discovered or attributed (2017:125). At the same time as it bypasses traditional signalling methods, in times of increased tension, non military tools such as cyber become key (Ven Bruusgaard 2016: 27).

Escalation is characterised by the increase in the intensity of conflict, but also by risk taking on the part of the actor hoping that the target will not overreact to their action (Duyvesteyn, 2012: 604; Kehler, Lin and Sulmeyer, 2017: 71). Thus, when it comes to responding to attacks, there is a desire to keep the response within the same 'currency' i.e. to make the punishment fit for the crime. There is an imagined link of proportion and kind between the crime and the punishment (Schelling, 1966). The bombing of one state might incur the retaliatory bombing of another. Where escalation occurs, the state that has been bombed in the first instance might choose to employ more powerful weaponry in its response. This, may, incur a similar escalation from the initial actor. Such escalation is particularly likely when states have competing areas for disagreement (Melin and Grigorescu, 2014). However if there is a misalignment of the expectation of the initial actor and the interpretation of the state that has been acted upon, states may choose to escalate using other means.

As we have shown in the previous chapter, there are a wide range of actions that can be considered as acts of war or escalatory. We noted above that states often keep responses within the same domain or 'currency', with an aim of matching crime with punishment. This means we might expect a sea-based move to be responded to with the same. Cross-domain attacks occur when an attack is responded to with an entirely different mechanism. It should be noted that cross-domain warfare is not new (Manzo, 2012: 9; Cimbala, 2017 2: 195). There are two possible, plausible conceptualisations of what 'cyber war' might mean: firstly, we can consider 'cyber' as a distinct domain and therefore cyber war as what occurs when two states use only

their cyber arsenal against each other. Secondly, we could consider cyber war to mean an escalation to conventional war in response to a cyber attack, which is to say an escalation from the cyber 'domain' to that of conventional force (Lewis, 2014: 575; Libicki, 2009: 121). In this thesis we are concerned with the second possibility, whether we call it 'cyber war' or not.

Cyber attacks have been shown to be able to inflict serious damage including bringing down power grids (Greenberg, 2017). However, as we have seen from this chapter, they lack a kinetic output. Some argue the lack of kinetic output puts them in a different domain to other forms of warfare, though whether place cyber merits its own domain is debateable (McGuffin and Mitchell, 2014: 441). It is clear from the increased link between militaries and cyber that states consider warfare that crosses between the cyber and conventional kinetic domains, or operations in both at once, conceivable. Important to note also is that some states involved in cyber only warfare, use it in the understanding that kinetic operations might result in a form of escalation, and therefore deploying cyber as a form of self-restraint (Lin, 2012: 65). The tacit expectations that a cyber attack will not result in escalation to conventional military force. (McGuffin and Mitchell, 2014; Kreps and Schnieder, 2019). But this is perhaps a more fragile assumption than is always recognised.

The argument regarding cross-domain escalation closely resembles that surrounding the limitability of conventional war versus nuclear war. Posen notes that there may be a public trust in the limitability of conventional war but that does a disservice to the nuanced nature of how wars are conducted and the escalatory processes that can occur (1982: 53). In assuming that conventional war will not escalate into a nuclear war, we are assuming that the domain cannot be crossed for some principled reason, in this case that nuclear war is so devastating that it is set apart from conventional warfare. In fact, it is contingent on how the conventional war is fought, and escalation is quite possible. What this means is that we must understand that the

gap between cyber and conventional warfare is not principled, but contingent. Though we have not seen a cyber attack be responded to with a conventional military response, it does not mean that there will never be an attack that triggers such an escalation. Martin Libicki notes that a kinetic response to a cyber attack could 'would trade the limited risks of cyberescalation with the nearly unlimited risk of violent escalation' (2012: 78). When we examine the action phase, reception-phase framework, we will expand on some of the limiting factors that influence escalating response.

There is a danger of escalating cyber attacks because there is no clear framework for shared understandings of the use of cyber weapons. States have developed their own frameworks for what cyber attacks refer to however there is still ambiguity and difference between states as to what impact cyber attacks might have and what appropriate responses might be (Manzo, 2012: 11; National Security Strategy, 2010). Attacks on military and civilian targets might breach the threshold for a conventional military response. In addition to this, the failure to avoid collateral damage or maintain command and control could lead to escalation (Cavaiola, Gompert and Libicki, 2015, 83). It may be that cyber attacks, in addition to kinetic attacks, may provide a new pathway to escalation (Long, 2017: 20). As there is no agreed consensus on what responses to cyber attacks might look like, states are forced to make decisions based on their own interpretation of the intention of the attacker. Indeed there is potential for unintended kinetic escalation if the victim perceives an intent in a cyber attack more extremely hostile than is the case, or reacts with unanticipated anger and ferocity to the harm done by one (Lindsay, 2015: 36). This will be further expanded upon in the following chapters.

3.6 Summary

This chapter has outlined how cyber technology defensive and offensive fits within the wider context of thinking about war. Cyber does not fit neatly within traditional categories, making its implications for warfare uncertain. The concepts of 'cyber war' is contested in meaning though it has attracted serious scholarship. Cyber weapons have the potential to be physically and kinetically violent, but there are no recorded examples of this manifesting in inter-state violence as yet. Military strategy is still catching up with the development of this new method of attacking another country. In considering how cyber fits within the wider picture of war and acts of war it is vital that we look at intentions, expectations, interpretations and reactions on the part of both aggressor and victim states because the threshold for war is, at bottom, socially constructed, and subject to change in the face of shifting circumstances.

Despite the work of Rid and others, further thinking is required regarding the threshold for military response to a cyber attack. Cyber technology allows states to conduct espionage, sabotage and subversion in a manner radically different to what went before it. However, the threshold at which such actions could become legitimate grounds for war is not clear. The location of this threshold is liable to be set by events yet to come.

Chapter 4 APRP model

> 'To date, the cyber security field tends to rely on thin case study descriptions of cyber incidents, using crucial cases to make inferences about actor motivation and the larger context of the cyber conflict, as well as using deductive reasoning to produce a foundation of theoretical knowledge regarding cyber conflict.' (Whyte, Valeriano, Jensen and Maness, 2018: 2)

Reliance on previous experience is of limited help for understanding the potential reactions to cyber attacks because of the limited number of cases. States are uncertain how to react and, what is proportionate, because they have very limited precedent to base this on. This thesis has previously discussed the various forms which acts of war take and the difficulty of categorising cyber attacks. It has been demonstrated that there is no clear threshold for when such an attack could become an act of war. This thesis chapter offers a framework to better understand the dynamics that operate under these conditions of uncertainty and ambiguity.

This framework begins with the calculation of the aggressor, how their intention is formulated, what the expected outcomes are in taking an action that impacts another state. This chapter argues that while in some cases their expectations will be correct, it is ultimately for those that have been acted against to decide what response is appropriate. The key question for this chapter is the scope for unintended consequences, and the influence these can have on the outcome of an action.

This framework highlights the importance of the interpretation of the victim of the attack. This in turn can be influenced by a number of factors, including domestic societal and political

pressures. This then feeds into a calculation process on the part of the affected state as to how to respond. Crucially, there may be a divergence between what states intend and expect as a result of a calculated action, and what the state affected interprets and how it reacts in turn. This scope for misalignment of perceptions raises the possibility that an act of war may be seen by one party, and responded to as such, when not intended to be such by the initial actor.

4.1 Action Phase

When considering the calculation behind initial actions, one key part is intention. Intention can be defined as the end sought from a calculated action (Meiland, 1970: 55). This thesis focusses on the intention of states to act such that they have an impact on other states. In order to do so it is necessary to first examine how intentions are formed; the influences that shape their formation and thus the resultant action. Also, we must assess how intention can be ascertained from context and documentary analysis. The second key element of calculation is expectation and risk. This concerns the outcomes an actor considers possible and likely in response to their action. This is shaped by considerations such as whether an action will be overt or covert, and whether there are established norms limiting the scope of appropriate response.

4.1.1 Intentions

The most straightforward method of discerning intention is to look at action, its expression. However, as Taylor notes, action may be an imperfect indicator of original intention (1979: 81). Both an action and its consequences can be misleading in terms of intention. As Jervis notes 'good motives can save bad policy' (1976: 39). Indeed, states are more likely to forgive a harmful action if they believe that its originator did not intend for the consequences to be as severe as they were. While it is important to study the consequences of the action, it is therefore

critical not to conflate them either with what was intended, or the interpretation of an action's intent by those affected.

Intention can be measured in a number of ways. Theoretically one might scrutinise the neurology of an actor to discern the workings of their brain and mind. Outside of basic research in a laboratory setting, however, this is not a feasible method for assessing intention. More plausibly, one can examine the claims of the individual e.g. through written or oral statements conducted through press conferences and interviews in order to discern what the actor intended to do and how they intended to proceed. From this, it may also be possible to ascertain what they hoped to achieve and what outcome they hoped to avoid, i.e. if a statesman hopes to avoid war by using sanctions, they might articulate why sanctions will avoid war. This of course relies on those making statements being truthful and explicit in their reasoning.

A third mode of enquiry overlaps with the second; it is to place the actions within wider context of actions and aims to discern possible explanations for goal-driven behaviour. Anscombe, for example, claims 'if you want to say at least some true thing about a man's intentions, you will have a strong chance of success if you mention what he actually did or is doing' (2000: 8). Contextualisation allows one the ability to place events within a wider picture in order to make sense of individual decisions. Gustafson points out, it is necessary that any account of intentional actions be placed within a larger context as all intentional actions are events within a wider history of interaction (1986: 15).

To establish intention, this thesis will therefore make use of public and private statements as revealed in investigative reportage. The method here will be threefold, firstly to examine the reports of intentions as laid out by officials in each of the case studies focusing on the different

approaches to using cyber attacks as a means for pursuing foreign policy. Secondly, we will examine the contextual framework, including the internal and external pressures on actors. Finally, it is necessary to note the overall policy at the time, which gives a broader indication of the intentions of governments from which intentions in regard to more specific actions might be inferred.

4.1.2 Expectations

While the terms contain some overlap it is possible to draw a difference between expectations and intentions: Expectations are predictive, i.e. they attempt to say something about what the potential outcome of an action might be. Meanwhile, intentions state what the desirable ultimate end might be. When we talk about expectations we are specifically referring to what reaction a state might reasonably expect from an action. Expectations and intentions are of course closely connected. When the US decided to act against Iran through the deployment of Stuxnet, a number of factors informed the intention and expectations on which that decision was based including; material resource and political strategy. Intentions are not fixed, however, they can change over the course of executing a series of actions. In contrast, expectations are built on a foundation of risk calculation and are derived from the action itself. It is unlikely that a state would embark upon a project without considering the variables that might affect its outcome. Contemplating these leads states to judgements about the responses to an action they consider possible, and likely.

When forming expectations, states have already engaged in some deliberate contemplation of uncertainty and risk. But reality may ultimately prove that actors can risk risks they did not expect. (Payne, 1996: 57). This might take the form of a risk calculation which assumed an outcome was less likely than it in fact was, i.e. it was considered but was perhaps thought too

unlikely to merit a contingency for it. Secondly, there is a possibility that the risk calculation does not take an outcome into consideration at all. As we shall discuss later, the possibility of a kinetic military escalation in response to a cyber attack may fall into one or both of these categories.

Intentions alone do not fully explain the prudential calculation that states undertake in deciding on actions. In light of expectations, states limit their behaviour to avoid certain degrees of risk associated with specific actions. Expectations are inherently predictive: they limit the range of responses considered plausible, at least in the calculations of the perpetrator. To bring in examples from chapter 2, it is unlikely that states will go to war over slights against monarchs in 2021. Therefore, policy makers make assessments on the likely outcomes of actions and the range of possible responses while effectively ruling some out of serious contention. These responses may be in line with, or different from the actual outcome depending on how astute the initial actor was in their assessment.

> 'The use of cyber capabilities makes a difference for policymakers since it allows them to minimize the risks of taking certain offensive actions, and it is a relatively effective low-cost alternative, (as the Israeli attack on Syria suggests), and it will become more common in the future' (Saltzman, 2013: 58).

When we consider risk we are considering the likelihood that a range of unfavourable outcomes will be the result of an action by an aggressor. Risk assessment is tied into the notion of prudential calculation, i.e. that a state will not make a decision it does not consider to be in its interest. Thus, the risk of an unwanted reaction to the aggressor is based on a estimation of the likelihood of various kinds of response. One way to estimate risk is to imagine how one's own

forces would react to a specific attack (Libicki, 2017: 34). An aggressor also has to consider that their actions may have consequences outside of their control.

Risks, and the taking of them, are informed by the presence of incentives: a state would not take an action where the consequences might be outside of its control unless there was something significant to be gained by doing so, or lost through inaction. Fear of threats leads policy makers to take risks, in order to prevent or mitigate the feared cost. In short, states will engage in risk taking both to achieve desirable outcomes and to prevent, or mitigate, undesirable outcomes.

Risks and threats are socially constructed (Clapton, 2011: 281), meaning their nature and reality is are open to different interpretations. This does not negate their impact on the decision-making process. It is because of their socially constructed nature that prudential calculation plays an important role in determining certain expectations. A poor conception of the risks one faces will lead to poorly informed expectations on the part of the decision-makers, and thus actions that are not only risky but run risks of which they are not fully cognisant when deciding upon them. Managing risks presents an integral part of the calculation that is undergone when expectations are created.

Calculated risks rely on a number of assumptions. Firstly, that the state making the calculation is capable of accounting sufficiently for enough variables that their intended outcome is likely i.e. there must be a plausible benefit to taking the risk in the first instance. Secondly, there is an assumption that states act coherently and rationally when attacked, meaning the state acted upon will respond only within a set of expected parameters. Generally, there is an expectation that states will react in certain ways to certain type of event or action, e.g. war would be an unexpected response to failure of economic trade talks. States will in this sense have both

intentions and expectations[11], the first being the desire ultimate result of an action, the second being the set of reactions thought possible and likely. Risks are taken as an attempt to 'tame uncertainty' but in doing so presuppose a number of future decisions and create future risks (Trenta, 2016: 17). For example, the United States might choose to use a cyber attack as a means of exerting power over another state, it has a number of expectations about the decisions that the target state will take in response. However, each decision comes with a degree of risk, meaning that the US could create greater risk and uncertainty by choosing to act, if they are wrong in their expectations. In this way, the utility and risk of the cyber attack is determined, 'by its expected effect on the intended target in relationship to the possible costs associated with failure' (Brantly, 2014: 475).

Any action comes with risks and potential benefits, and risks are often taken to mitigate potential threats, i.e. to create a benefit by averting a potential later cost of harm. Manipulating the perception of the state on the receiving end of the action is a key element in cyber attacks, where the aggressor often seeks to create a situation in which the victim believes that what is occurring is normal, when they are in fact under attack (Denning, 1999: 101). Acting to forestall threats can benefit a state, but it comes with the risk that an action might be characterised as an act of war. There is danger in inflating perceptions of threat: perceived threats can lead to arms races, for example, which in turn are more likely to incur conflict (Howard, 1983: 17). 'Overstating threats is dangerous because the response could then end up being the actual cause of more conflict' (Valeriano and Maness, 2015: 3). The 2003 invasion of Iraq was arguably driven by an overstatement of threat by the United States that ultimately led to a long and costly war. In this case, the benefit of removing Saddam Hussein from power and installing a democratic regime in his place was arguably not worth the risk if that risk had been accurately estimated at the time of the decision to invade. When pursuing actions that are against the

[11] Finlay (2018: 364) notes that there is a double intention: one to commit the act the second to limit the possibilities of response. We combine these intentions and argue that together these focus what the expectation of response should be.

interests of other states there will always be an element of risk. Any state that desires to expand its influence will also be faced with a degree of risk in this regard.

External political pressure can also incentivise action. If a state has alliances, acting against a shared threat can be a means to signal reliability and value as an ally, and this can constitute part of the intention behind it. The often covert aspect of cyber attacks however means their value as a signal is limited, though they can be used to signal to allied states that the acting state is willing to do something. This differentiates cyber from traditional forms of warfare where signalling is more prominent (Howard, 1983: 19). Cimbala (2017: 492-493) argues that transparency is key in cyber attacks, and signalling could take place. Indeed some academics have argues that cyber attacks are a relatively useless form of signalling to other actors on this very basis (Gartzke and Lindsay, 2017: 42). Due to cyber being at the forefront of covert actions (Brantly, 2014: 473-474) we could assert that their use while political is not intended to directly signal, at least in some cases.

Risk calculation takes place within the parameters of what reactions the actor thinks are likely enough to be worth taking into account for example, in a given scenario, an aggressor state may take into account the possibility of a victim state imposing economic sanctions in retaliation for its actions, but might discount some downside possibilities that are nonetheless present. For example, an aggressor state choosing to use a cyber attack may rely on the assumption that there is a precedent that the victim state can only respond with a cyber attack, or that it will choose not to escalate based on previous cyber attacks. However, this is in fact contingent on the victim interpreting the attack and the imagined boundaries of response in the same manner. Risk calculation on such basis may discount some scenarios as inconceivable based on precedents that are in fact more contingent than the aggressor state appreciates.

Cyber attacks can prove a useful method of demonstrating power in what is imagined to be a relatively safe manner. This might seem contradictory to the often-covert nature of their deployment. Considering intra-state cyber attacks such as Israel on Syria in Operation Orchard, Russia on Estonia in 2007 (discussed in depth in Chapter 6) or Georgia in 2008, it is possible to demonstrate power through cyber attacks.As there have been no instances of cyber attacks leading to a conventional force response, there is no precedent for states to retaliate in such a fashion. The danger is that this might lead states to invest undue weight in the precedent that states will or must always be restrained in their reactions to a cyber attack. Furthermore, cyber attacks can be thought safe and useful as they can be adapted to hide the perpetrator, eliminating, or mitigating to a large extent, any fear of reprisal. The following section will examine some of the expectations that are associated with cyber attacks and how they work to dilute the perception of risk on behalf of governments and policy makers.

4.1.3 Influences on calculation during the Action Phase:

It is important to analyse how intention is formed and how expectations shape the creation of policy action. A number of internal and external factors can influence the formation of intention and expectation. Lewis (2014) notes that some important factors are national and international threat perception, media, or bilateral and multilateral engagement. For analysis of cyber-attacks perception, the framework adopted here incorporates these factors within some broader categories to provide an understanding of the factors shaping the calculation process. Factors that can influence a state to act on a certain issue internally include: public opinion, prospect of financial or material gain; and pressure from political groups both within government and outside of it. External factors include: pressure from allied states; perceived threats from opposing states; regional instability and possibly responsibility to protect. We can also

distinguish between two categories of case: those where a state's intentions are largely arrived at autonomously; and those where a state's intentions are largely determined by circumstances.

- **Public Opinion**

Public opinion plays an important part in determining a state's foreign policy (Levy, 1988: 664; Berdal, 2009: 82). In democratic countries, the government is held accountable to the electorate and therefore must act mostly, if not at all times, in line with public interest. Public opinion can drive the agenda for decision-making and influence what states determine to be in their own interest. Lewis (2014:572) argues that the media and public opinion have an important role to play in determining threats. US public support for intervention in Afghanistan in 2001 was essential to the decision to invade, among other factors. In 2011, by contrast, Obama decided against the use of land-based troops for intervention in Libya, understanding that the public had no desire to be caught in another lengthy conflict in the MENA region (CNN Research Poll, 2011). There are occasions when the state may make decisions that run counter to the wishes of its public; but in democratic regimes this may bring about or hasten the end of a governing administration.

However, governments may also make decisions that they believe are in the best interest of the state despite lacking public support for doing so. In such circumstances, states may choose to hide their intentions and actions from the public view for fear of political backlash. In the second term of the Reagan administration, the Iran-Contra scandal almost brought down the President when it was uncovered. The secret selling of arms to Iran, and funding of Contras in Nicaragua, could be argued from a hawkish conservative perspective to be in the best interest of the state. But it contravened the Boland Act and was therefore illegal. The administration therefore pursed its policy covertly. The details of such actions may only be revealed by later

investigation and/or documentary analysis. States can thus be influenced towards or away from policies by public opinion, but may also purse policies with a shaky foundation in public support covertly such as through use of cyber attacks.

- **Gain**

Power and material gain at the expense of another state provides a drive for foreign policy (Gortzak et al, 2005: 174). States have an interest in self-preservation. Waltz argues that states will always act in their own self-interest even at the expense of others (2001: 160). Even seemingly mutually beneficial behaviour such as investment in another states, can reflect an ambition to reap asymmetric benefits, or gain leverage (Waltz 2001: 202-203). The most straightforward example might be that of state invading another for material gain, as in the case of Saddam Hussein's 1990 invasion of Kuwait (Milton-Edwards, 2010: 116). The desire for more power, prestige, and financial or material return can provide motivation for states to expand their reach into other states. This often provides crucial context for understanding the intentions behind actions which may have a different rationale officially proffered. The US was at no particular security risk from Iraq in 2003 prior to invasion, Hussein's state had been soundly beaten in 1991 and was unlikely to pose much of a threat to the surrounding region. Yet, the decision was made to invade. If we examine the documentary record alone, one might conclude that the Bush administration had compelling offensive security reasons for going to war in this instance i.e. the presence of weapons of mass destruction. However, by viewing the war in wider context, one can gain a fuller understanding of the background of the US-Iraq relationship and the desire to showcase the military might of the US in a region that is not only important militarily but also strategically important because of its resources.

Cyber attacks can be of value to states looking to assert and expand their power and influence in less costly way than using military options. Such limited, non-military aggression can be a form of leverage for smaller states (Valeriano and Maness, 2018: 351). Cyber attacks also increase the cost of defence for the victim state, further diminishing the resources that state might employ for other means (Rustici, 2011: 36).

- **Internal Political Pressure**

Pressure from organised political groups[12] within a state can drive the policy agenda in ways that interweave with public opinion and with financial and material gains but are distinct from the these other considerations. Groups which dominate certain areas that control large workforces for example can shape debates in their favour even to the detriment of other groups within the country. For example, the corn lobby in the United States helps to maintain support for a large number of farms and farmers through political pressure (Foley, 2013). Farming subsidies have artificially propped up the corn industry in the United States to the detriment of other land uses and indeed favours American farmers over cheaper corn imports from other parts of the world. The United States government continues to fund corn subsidies while a number of other sectors are not given a comparable degree of funding. This type of lobby pressure can be seen in US relations with other nations also. The US continues to give Israel financial and military aid despite the state holding one of the highest GDPs in the wider Middle East (Mearsheimer and Walt, 2007: 24). Pressure from internal groups can have a major impact on policy and is worth consideration as we later turn to the case studies.

- **External Political Pressure**

[12] Levy (1988), Gutmann (1988), Glenn (2009), Hoffman (2009) and Hughes (1988) all present arguments for the inclusion of analysing political groups as a means for understanding why states go to war.

Military alliances with key countries such as the United States can help provide security for other states that do not have the financial means to maintain large militaries themselves. This can also lead states into making decisions that may be against the wishes of the general public but are, in the eyes of the policy-makers, key to the maintenance of alliances required for future security. For example, while there was a lack of domestic support for the invasion of Iraq in 2003 within the UK, the decision was made to enter the war regardless (Travis, 2003). The UK government chose to uphold its military alliance with the US in a troubled and unstable time and thus it put a long-term interest in an alliance ahead of the desires of its people. This is evidence of the power of states to influence others and that certain states can influence others to make decisions that neither deliver them gain nor have popular support.

4.2 Reception Phase

4.2.1 Interpretation

When states act it is not in isolation. Intention and expectation are just part of the picture; the other part is interpretation (Feldman, 1999: 317). The acting state does not get to decide unilaterally how their action will be interpreted. There is scope for divergence of perception between the acting state and the state that has been acted upon. Because of the nature of cyber attacks, there is even more space (than in instances such as invasion) left to the victim to speculate as to the intentions and purpose (Hansel, 2018: 530). Thus, when looking at the case studies, it is important to also focus on the interpretation of the victim state in order to assess how states can misinterpret intentions and diverge in their interpretation of actions, which may have major implications for how states ultimately react. This section will analyse how interpretations play a role in the understanding of how states transition from peace to war, and what must be considered an act of war. Firstly, this section will look at defining interpretation, drawing largely on the work of Jervis (1976). In order to do so, it is useful to illustrate some of the problematic elements of expectation and intention, which underlines the importance of

interpretation as a component in this case. Secondly this section will look to set out potential elements associated with misperception: examining two different forms of misaligned interpretation – regarding intention, and outcome. This will further our understanding of how risk calculations can be thrown off by misjudged expectations on the part of policy makers. Thirdly, we shall focus on the factors that shape interpretation.

Interpretation relies heavily on attribution. The victim state cannot begin to accurately interpret an action without understanding who carried out the action and its relationship with that actor. When one state chooses to use traditional military force against another this attribution is clear. Cyber attacks are often more problematic (Faga, 2017; Buchanan, 2017). Covert action can allow for plausible deniability (Owens et al, 2009: 81). This also presents a challenge for the study of cyber attacks. The capture and treatment of massive amounts of published data pertaining to cyber conflict promises a unique resource for those seeking to assess the context of cyber security engagements.

The idea of interpretation as used here builds heavily on the literature of perception. 'Perception is... an active process of constructing reality' (Duelfer and Dyson, 2011: 76). However, it is more than simply a construction of reality, it is the reconstruction of reality as it appeared at a specific time; in essence the cyber attack damage can be considered limited by the attacker and still have a large impact on the victim depending on the societal context and established conceptual frameworks (Emerson, 2016: 192). Often, the reconstruction will occur more than once as more information is provided to the interpreter. Therefore, interpretation is a rolling process, not a singular moment. As we examined in the case of intention, there are a number of external factors that can impact the interpretation of a given event. These external factors include prior relationships and history of interaction, as well as current social and

political circumstances. Interpretation is also built around a number of internal sociological and societal factors that impact on the decision-making, and threat assessment of policymakers.

Scholarly work on perception heavily emphasises the social context of actors (Barrett et al, 2011; DeBusk and Austin, 2011; DiDonato et al, 2011). Such studies use statistical models to discern how different societies perceive each other as well as proposing frameworks for analysis. These can be useful in exploring how perception is formed, and the role of perception in shaping the reaction to potential acts of war. Studies from the psychological sciences can be relevant to understand issues of the sort discussed here, though the questions they seek to address are typically rather different. Often, they focus on societal distinctions, without much consideration of the context of prior relations and engagement. This literature can usefully be brought together with other studies focused more specifically on how states interpret action, to illuminate the phenomena of interest here. Other studies (Jervis, 1976; Duelfer and Dyson, 2011; Yarhi-Milo, 2013) examine how states interpret action. Therefore, it is necessary to bring together these schools in order to fully ascertain how perception is informed and the pressures within the system that lead states to make decisions on reactions.

A critical element of understanding interpretation relies on how societal value is assigned. Some institutions, people, buildings, etc. hold a specific societal importance that can only be fully understood by the people of that state (Singer, 1979: 5). These values are created through social myths and are replicated for the sake of continuity within the state (Kolakowski, 1973). Reality is determined by our perception of it, thus what states experience in the form of perception, is, in a profound sense, real (Denning, 1999: 101). This societal value confers significance on particular things that would not apply if they were simply replicated. An attack on Big Ben provides a useful example: if a bomb had been planted at another similar clock tower would the perception be the same? The building itself, but more importantly the institution it represents is

understood to be of critical value to the state and therefore the perception of that attack will be far graver than if the target had been elsewhere. Likewise, an attack on a member of the UK Royal family would warrant a perception that might seem out of proportion to an actor that unaware of the context that confers higher significance upon a single life. Thus, when we examine cyber attacks, it is important to note that states may have placed societal value on for example their energy infrastructure or another target. This has the potential to create unforeseen risk for the aggressor, as they might have a mistaken estimation of the societal value attached to a target, or believe targets are equivalent based on their material characteristics alone when they are not.

Cimbala (2017: 493) has connected this issue of societal difference and potential misunderstanding to the problems of deterrence. In today's geopolitics, US beliefs regarding China's motives are a key component of how the US responds to the rise of China (Glaser, 2015: 53). A miscalculation by the aggressor might lead to a target being chosen that has an unseen value, and therefore the perception of the attack's severity might be worse than expected. The death of a civilian might not weigh as highly as the death of a political official. The threshold for escalation is often hazily defined, as perception changes depending on the action and the target, since it is heavily dependent on the societal value assigned to the target and the type of action taken. Davis (2015: 348-349) illustrates well the potential of escalatory cyber attacks, noting qualitative differences between cyber measures carried out by China and those by the US which potentially increases the scope for future cyber attacks to be misperceived.

> 'A consideration of ''what do we have that others want,'' ''how valuable or important is it,'' and ''how well are we protecting it'' begins the process of risk assessment. Leadership must answer these questions in its assessment of asset risk, vulnerability, and value. The threat landscape should then be assessed to discern what the invaders

> want to achieve, and how they will likely attempt to achieve those aims.' (Mattern et al, 217: 710).

States will undergo a process of risk assessment on their critical infrastructure. These will be assigned a value or importance. How this value is attributed is particular to each state; there will be societal and political commitments that may weight similar things differently from case to case.

Feldman notes that interpretation requires an intricate and nuanced understanding of the other. Our interpretation of communication, events, and conflicts with another actor is based on our prior knowledge and experience with them (1999: 317). This further underlines the importance of societal and historical context. In international interaction, both sets of policy actors already have preconceptions regarding the other which inform their reading of particular events within their given context. However, those prior perceptions can be based on limited false information or skewed by particular events. If we accept Feldman's proposition that interpretation relies heavily on the interpreter embracing the intending agent as a 'member of a familiar societal community', then indirect societal knowledge exchange between two states through their limited prior international interactions will impact on their capability to understand each other's actions within a given context (1999: 326). In Feldman's example, this might mean Libya could to some degree accurately interpret US actions by drawing on prior societal knowledge, while there continues to be scope for misinterpretation. When we consider interpretation, it is vital to have an understanding of the context to fully grasp the rationale for actions. Interpretations are often built out of prior experience and this informs their construction.

When analysing interpretation, as with intention, there is a need for documentary analysis including and not limited to, the study of official documents, public speeches and statements from officials. This affords some insight into the thinking of policymakers. This comes with limitations however: interpretations and calculations suffer with the same problem of truth – it is possible to misrepresent perceptions or intentions in public to keep them hidden from a potential aggressor (Shusterman I, 1992: 171). This problem can be mitigated in part by placing decisions within their wider context; just as intention manifests and is practiced within a world of external actors, it is necessary to study the context in which perceptions are generated. One can also use sources such as journalistic coverage as part of a composite picture that attempts to ascertain the interpretation of a specific regime of an attack.

One source of potential unanticipated escalation following an attack is misinterpretation of intention. This can both stem from and lead to inflation of perceived threat relative to reality (Valeriano and Maness, 2018: 9; Hansel, 2018; Brake, 2015: 3). As Feldman notes, rationality is to some extent socially constructed, meaning it is only through the interpretation of intentions that communication is understood by different sides of an exchange (1999: 317).

For this reason, it is possible for both sides to exchange rationally but for misinterpretation to make the actions of one appear irrational to the other. In the case of the US intervention in Libya for example, There were multiple occasions when events could have unfolded differently depending on how the two sides coincided or diverged in their understanding of one another's intentions. Information warfare, which can be a component of cyber attacks can also further distort the perception of reality, potentially furthering tension between two or more states (Cimbala, 2017: 498).

One way in which intention can be misinterpreted is if victim state believes that the aggressor intended their action to do more harm than they did, when in reality, the harm in question was done as a result of some unintended consequence of their action. In such a case, the action causes more damage than the aggressor intended, leading the victim to believe that the damage was intended. In instances such as this, events occur that are outside of the control of the actor that influence the interpretation and reaction of the state which is acted upon, and may trigger a response not provided for in the initial actor's expectations (Jervis, 1976: 54). It has been plausibly suggested that states will have a more favourable interpretation of an event, and a more moderate reaction, if it is known that the aggressor did not intend for the action to do as much damage as it did (Nickel, 1974: 489). Thus, outcomes may be better if victims understand clearly the intention of the aggressor rather than being left to develop their own theory regarding the intentions.

As noted previously, an interpretation is typically constructed based on an assessment of previous engagement as well as anticipation of future interactions. In some cases, the state that has been attacked will discount decision maker's professed (possibly genuine) intentions, if an action/attack fits with their priors about the other side's likely actions and imagined intentions laid out (Jervis, 1976: 57; Shusterman I, 1992: 66). Thus, intentions will be ignored if it fits a narrative and/or with previous engagements with the aggressor. However, states' interpretations can be shaped on how the aggressor announces their intentions: i.e. if the perpetrator announces that the consequences actually resulting were not part of its intentions; the reaction may be more moderate and proportional than without such a clarification. However, the reverse is also true; if an aggressor state announces its intention to do as much harm as the action entailed, then the victim may perceive it more negatively, all ambiguity having been removed. A weapon's deployment could have a number of unintended consequences. In examining the unintended consequences in our case studies, it is important to

remember that there are two sides to the interpretation of its results: i.e. what is a bonus success for one side may be a disaster for the other, and vice versa.

A second form of misinterpretation may occur in a case where the outcome is exactly as the aggressor intended, but the affected state believes that part of the intent of the attacker was to deliberately commit an act of war. In this case, the aggressor did not intend to go to war, however the victim misperceives their intentions. This is distinct from the case where the action creates unintended consequences. In this example, the aggressor has underestimated not the literal effect of their actions but the message conveyed by them. This scenario is rooted in a failure of the aggressor to accurately assess the risk involved in their action. The miscalculation of risk combined with the misinterpretation of the state acted against, could create the conditions for war (Jervis, 1976: 82). In such cases, as communications breaks down between two states, it becomes increasingly difficult for both parties to avoid conflict.

In a case where a state uses an airstrike against critical infrastructure, the state attacked might reasonably misinterpret the intention behind the action in this way perhaps. Assuming that such an attack might precede future attacks. In a number of cases, such as Israel in 1976, such a strike signalled willingness to transition from peace to war. Similarly, in 1939, the German land invasion of Poland was preceded by an airstrike. Thus, there is ample precedent that actions of this kind can precipitate war. However, it is also possible for states to use airstrikes in such a manner that they do not consider themselves as going to war. Examples include US airstrikes in Libya in 2011 and Syria in 2017. The actions did not precede a US invasion of either country, nor did the United States consider itself at war in either case. In circumstances where the action of the aggressor does not speak for itself with regard to intention, the outcome depends heavily on judgement and interpretation. There is a discrepancy in vantage point between states that must look at the action and determine intention; and the aggressor that knows its own intention

and observes the outcome. In the case of cyber attacks, it is even more difficult to discern the intention due to a lack of signalling, making it hard for policy makers to calculate a response since they cannot be sure, whether an attack was motivated by security, greed or some other motive (Gartzke and Lindsay, 2017: 42; Glaser, 1997: 179; Hansel, 2018). The difficulty for the victim state when assessing the meaning behind the actions of the aggressor provides fuel for misinterpretation.

Another way in which interpretation can affect response lies in interpreting the outcome, as opposed to the intention. This means a state may disregard intention, stated or otherwise, and base its response on its view of the effect of what was done to it. However, two states can examine the same events and perceive them in quite different ways. Though assessing intentions is generally considered important, disregarding intention can be useful for a national narrative: as previously stated intention can be discounted if it seems to contradict previously established views and expectations of the victim predictions about the aggressor. However, it can also be that two states simply have different interpretations of the same result based on societal differences: one society might place more value on the ideas of sovereignty and thus perceive an airstrike as an act of war, whereas a society that experiences airstrikes regularly, which might consider one as an unfortunate incident, but not one rising to the level of war or even close to it[13].

An example of this is the different interpretations of the downing of a Russian fighter jet in Turkish airspace in 2016: The Turkish government had consistently noted their objections to the violations of airspace to the Russians but this had been ignored, they then felt that they were within their rights to shoot down a jet that violated their airspace. The Russian administration

[13] Agrafiotis et al (2018) presents an interesting discussion on creating a taxonomy of harms which include digital though this is separate out from other harms. Cyber can be considered a harm which crosses into other areas of the taxonomy such as reputational or social.

disagreed. Neither state focussed on the issue of intention: whether Russia had intentionally been crossing into Turkey or not was never an issue: instead, the focus was on the meaning of the outcome: the downing of the Russian jet. This suggests that states can look past the important notion of intention when building interpretations and assessing responses. To examine how and why this occurs it is useful to analyse two elements: societal differences and the role that they play in forming interpretations; and the notion of similarity, why states believe that others are similar and thus will perceive outcomes in the same manner.

4.2.5 Factors influencing interpretation:

An underlying proposition in this thesis is that there are societal differences that mean that the interpretation of events may be markedly different between two peoples or states, because of differences in where they invest value and that this may lead to consequential misalignments in how they anticipate, interpret and respond to one another's actions.

When analysing the formation of intention, we looked at the foreign and domestic pressures placed on the country at the time of decision and action. These pressures are important in the case of interpretation too: they influence the formation of interpretation as states make sense of actions within the international sphere. In examining the Iranian interpretation of the Stuxnet attack for example, it is helpful to detail the interactions between Iran and the US in the years leading up to the event. This helps to build a societal context from which we can make sense of the interpretation in our case. States build their interpretation on the foundation of prior experience (Feldman, 1999: 317). DeBusk and Austin, show that cross-group emotion recognition is higher in those that have greater social links with others; this means building an accurate interpretation of the other's intent and actions is aided by some level of shared experience (2011:764). Previous events and interpretations influence how victims later

understand an attack within the context of their relationship with the aggressor. Though a state's view of its own intentions is important, we must ask how the states against which they act perceive the attack, in the context of the existing relationship between the two states. An intrinsic part of defining a state within the global system is a distinction between self and 'other', this can make the notion of societal community difficult to achieve, especially if, as in the case of the US-Iran relationship, one state rejects large parts of the other's society and values (Campbell, 1998: 196). Fear or misunderstanding of victim state's society can lead to misalignment of an aggressor's expectations and the victim's interpretation.

Differences between societies and states of this kind can be grounded in a variety of areas, including race, culture, religion, ideology etc (Meissner and Brigham 2011: 764). The key point is that they may lead societies to assign value differently and to have limited or inaccurate understandings of one another's values and priorities. This leaves more room for misinterpretation of an action than in cases where states have similar social basis for understanding. Societies often tend to have more accurate interpretations of in-groups when contrasted against outsiders, and therefore, we should take this into account when examining e.g. how Iran responded to Stuxnet.

This is only part of the story, however. Societies often perceive groups to be different when in fact there is much similarity between them (DiDonato, Ullrich and Krueger, 2011: 66), and 'othering' in this sense performs a basic role in establishing states as distinct, coherent entities. It may lead to misinterpretation of one another's values and intentions, but it may not. And even similar states can misinterpret one another's actions and intentions. To understand this, we must look to a wider range of influences.

Two internal factors influencing a state's interpretation are: public opinion, which reflects and sets the social significance of the action; and political and pressure groups that shape the debate. There are also external factors: states can construct interpretations in light of security asserted them by an external actor and states can also have their interpretations dictated to them by an external actor.

Public interpretation has an important role in the formation of the state's policy after an attack. As with intention, public opinion is critical to our understanding of policy formation on this side of an action. Public opinion in response to events such as an attack allows governments, particularly in democratic regimes but also elsewhere, to justify foreign policy decisions. The public reaction to 9/11 was a key ingredient in the decision to respond to it by invading Afghanistan and further enabled the decision to invade Iraq even though it was not involved in 9/11. However, there are cases where public interpretation runs counter to government policy. There may be compelling prudential reasons not to use force in retaliation for an attack even if the public opinion is in favour. For example, in a scenario where Iran is bombed by the United States, public opinion might well favour military retaliation, but the regime's survival may rely on the restraint of its leaders given the state's relative capabilities. Public opinion is therefore a a factor to consider in understanding the decision-making process of a state but should not be understood as determining the outcome. Public should be taken into account when assessing a state's interpretation of an attack, but alongside a consideration of the value attached to the target of the attack by leaders as well as the public.

We can often better understand the interpretation placed on an attack by understanding the value invested in the target by the country attacked. This will heavily shape the moral force of the blow and the degree of legitimacy they feel in responding forcefully (Smith, 2006: 7). This may be influenced by the intention they read into the assault. But it also plays a role in the

'effects-based approach' outlined in Farrell and Glaser (2017: 8); a state should measure harm in the impact rather than simply in the destruction cost or weapon employed. The perception of intangible harm to larger, possibly abstract, values can be critical to the interpretation of an attack.

Political groups can influence policymakers and the public discourse and change perceptions of certain events by applying pressure. In the same manner as with intention, these groups can facilitate a change in understanding during the period between action and the formation of a state's interpretation. These groups can also change the dynamic between the state and other states through lobbying and political pressure. An example of this is UKIP's role as an anti-EU lobby in the UK. The political party managed to create change and a demand for change in a country where anti-EU sentiment was limited by exerting pressure on other parties via its public appeals and electoral campaigning. Thus, it is important to take the influence of political groups in account when considering how interpretations are formed. The agendas driven by such actors can contribute significantly to misinterpretation.

It is important to also analyse the influence of external interpretations on state's calculations. If a state's government believes that is has the support of other states for its interpretation, this helps validate it as worthy and plausible. Thus, states may wait to assess, and be informed by, the interpretations of others during their own formative interpretation process. In deciding how to react to events like an attack, the support of other states is integral to the decision-making process, particularly for non-superpowers. As states band together for security, a state that has been attacked may feel more secure in its view on retaliation if other states align their views with it. This can allow states to make bolder decisions while remaining rational. For example, Israel chose to act in 1967 to a perceived threat from Egypt triggering a pre-emptive strike against the country. It is not clear that Israel would have chosen to react in such a manner if it

had not had the support of the United States. Even if the US knew nothing of the planned attack, their close ties with Israel afforded the state some leeway in the decision-making process and a degree of safety if repercussions of a military response to a perceived threat turned against Israel. Thus, the interpretations of external others can allow states to choose their course based on the assurance that their fundamental security is underwritten.

As with intentions and expectations, interpretations can also be shaped by the deliberate manipulation or pressure by an external state or political group. Such actors may seek to take advantage of political situations for their own benefit or may attempt to shape events in order to increase their relative power. Larger and more powerful states may seek to impress their interpretations of events on to smaller states in order to gain an advantage in a larger contest. For example, Russia maintained good working relations with Ukraine before the civil war through pushing it to avoid close ties with the European Union. One could argue that the pressure of Russia significantly shaped interpretations of the EU and Europe within Ukraine, dampening any turn towards Western alignment. This Russian pressure also sustained a large body of opinion in Ukraine that close ties with the EU could and should be avoided. The impact of external interpretations on internal interpretation formation is therefore an important factor to consider when examining our case studies.

In summary, interpretation is critically important to how states understand their role and the actions of others and their own circumstances when subject to pressure or aggression. 'Moods which cannot be grounded in fact' are embedded in what would appear to be rational considerations (Blainey, 1976: 54). This section has noted that there are a number of factors that can cause states to interpret the same actions or events differently leading to potentially problematic consequences. It has defined interpretation and shown how one can seek to ascertain it via documentary records and context. It has discussed its relationship to intention. F

factors that can cause states to interpret the same actions or events differently leading to potentially problematic consequences. It has defined interpretation and shown how one can seek to ascertain it via documentary records and context. It has discussed its relationship to intention. Finally, we examined the factors that influence interpretation to better understand how it is constructed. Interpretation helps shed light on how states can inadvertently shift from peace to war, since misaligned interpretations can lead to one state's action being understood by another as an act of war. In the following section we will be examining how reactions follow as the final stage, emerging from interpretation.

4.2.4 Reaction

The final stage of the framework proposed here is reaction. This is where intentional action having been interpreted and possibly misinterpreted by the affected party generates action in response. In this section, we look to define reaction and examine its intertwined relationship with interpretation. Following from this, it is important to examine the types of reactions, including reactions that are both in and out of proportion to the original attack, because proportionality is key when examining responses (Finlay, 2018: 373). Reaction in this context can be defined as an action that takes place, which is seen by those taking it as a consequence for and response to another actor's previous action. For the purposes of this thesis it is supposed that states generally are somewhat rational in their reactions, bit that their rationality is shaped by the factors shaping intention and interpretation set out earlier.

It is possible for a state to interpret act against it such that responding with force would be a legitimate, reasonable and proportional response to an attack yet at the same time have its reaction be tempered. This is similar to an aggressor limiting their actions in the first instance based on expectations of possible escalation in response. Desire for self-preservation, or a

prudent understanding of the unviability of war as a tool for achieving desired ends, may lead a victim state away from choosing a forceful reaction. The fact that a state would consider itself justified in treating an action as an act of war does not mean it is compelled to respond with war no matter the cost. Indeed, it appears that states for the most part err on the side of caution when it comes to their reactions (Waltz, 2001: 234).

The ability to react exactly as interpretations demand depends on a number of factors worthy of considering. We can break these factors down into internal and external factors. Internally the interpretation of government as well as the pressure from political groups play a major role. So do the material resources available to mount any response and the plausibility of prevailing in any conflict. Externally, states may look to their allies for support, gauging to what extent they can rely on them depending on their choice of reaction. Furthermore, it is important to understand the interpretation from external actors and the influence this has on the decision to react in a specific manner.

Material resources are an important factor in considering how a state chooses to react to an attack. Relevant resources include, but are not limited to, military strength, access to natural resources and economic performance. These resources can allow that state to respond with a degree of security though only in the right combination (Mearsheimer, 2003: 57). Sizeable military and economic capabilities afford Russia the ability to respond to threats in the Middle East, notably in Syria through combating the Assad regime's domestic enemies. But large oil reserves did not translate into a meaningful military resistance from the Kuwaiti government when invaded by Iraq, and it eventually required assistance from an international coalition to be repel the invasion (Tétreault, 2008: 270-271). While one might intuit those states are more likely to respond if they have the means to do so, this is not always the case. Israel, for example, has a strong economy and a large active military. Despite chastising Iran in the media, Israel has

not mounted any significant overt military attack on Iran, despite the number of terrorist attacks that Israel has linked to Iranian funding. From this we can gather that resources are not the only factor that decides whether states choose to respond militarily to provocation from another state. One might note the same of Iran, which is periodically threatened by Israel or the United Sates but does not respond with force (at least not directly).

Reaction to aggression can come in kinetic or verbal forms. Often, by 'no reaction' we mean non-violent reactions. These might include a press conference to demand redress which is a 'non reaction' in the sense that it does not impose cost on aggressor directly. This can be contrasted with the costs imposed by a potential retaliation that might include air strikes, assassinations on the kinetic side, and possibly also economic and trade sanctions. The category of 'no response' can be useful to states even when in a situation where action against them would seem in their interpretation to justify a forceful response. For example, if Syria suffers an air strike on its military facilities from Israel, one could argue that this action requires a response. If both states held equal power in terms of their allies and potential resources, then Syria would likely reply in kind. However, the Syrian interpretation of the attack will be shadowed by the knowledge that a retaliatory attack on Israel might mean intervention from a larger power such as the United States. Though Syria relies heavily on the Russian government for support, they might be wary of retaliating in a fashion that might provoke a larger conflict. Thus a 'non-kinetic' response may be useful in that it allows states to be seen to protest an attack without being seen to treat the action as having initiated a war, from which they would likely not prosper. Many states, moreover, have either tacit or formal alliances that render them somewhat interdependent on others to provide economic, political and societal resources in the event of conflict (Jervis, 1979: 87). Thus, states that have limited resources will look to others when attacked in order to gauge interpretations while developing their own. States will often be guided by these interpretations.

During the decision-making that generates a reaction these factors are considered by the actor with a view to making a calculation on the costs and benefits of certain responses (Howard, 1983: 7, 22; Blainey, 1976: 129). It is possible for a victim state to believe itself *entitled* to respond to provocation with military force and thereby begin a war, without believing that it is prudential to react in that way. Prudential calculations provide a restraint on actors that might otherwise draw further damage upon themselves by calling an attack on them an act of war and reacting accordingly. However, restraint could be interpreted by the attacking state as a weakness encouraging further attacks, thus this decision to use restraint has quite serious implications (Glaser, 1997: 181). In situations where the victim state is far less powerful than the aggressor, prudential calculations might suggest that they take a less forceful approach in responding to an attack. As will be discussed later, Iran has reacted somewhat negatively to US and Israeli cyber attacks, but has been muted especially in the latter case, perhaps out of calculated wariness of precipitating an unbearably costly military engagement. (Valeriano and Maness, 2015: 315).

The state that has been acted against might still feel that they are legitimately entitled to respond with force and even desire that response in principle, but during the decision-making stage, it becomes clear that certain responses are not feasible. War in such a case is avoided because a state believes that a certain response is not worth the risk and cost of an escalated conflict. This is not assured however. Even a small state may be so affected by the aggressor's actions, that it decides that war is the only possible course, despite prospect of further damage to themselves. It is therefore important to note that despite these limiting factors, states do not always act in a way that is prudent. It is an error to confuse the unwillingness of states to treat an act of aggression or provocation as an act of war on the grounds of prudential cost-calculation, with their believing that they would not in principle be justified in do so.

4.2.5 Types of reaction: proportionality and disproportionality

It is necessary here to include some analysis on proportionality of response. Proportionality is considered important in relation to reprisals as it serves to limit the damage done by victims in retaliation and contain further conflict. Walzer notes that "in treatises on international law, the defence of reprisal is always qualified, first by a great show of reluctance and anxiety, and secondly by some words about the extremity of the case" (2006: 212). The threshold for the use of force must be finely balanced between an expected response and the state's desire to express its freedom of action (Pipyros et al, 2017: 381). However, the proportionality of responses is inherently variable depending on the judgement of the actors in question. An air strike might have different costs to different countries, i.e. those who have the materials to rebuild rather than those that do not. Eberle posits that if a plane was hacked and cost the lives of everyone on board, war would be the clear outcome, but using the same means for espionage would not customarily warrant a traditional military response (Eberle, 2013). An aggressor might intend simply to destroy an airfield with an air strike as a minor blow however they might underestimate the true cost to the victim state if they only consider how such a strike would impact themselves. Thus, the nature of unintended consequences may be an important aspect when examining proportionality. This is where interpretation becomes critically important: as what seems proportionate depends to some degree on interpretation of intention and of severity of outcome.

Reactions that are restrained or mirror the impact of the initial action can be characterised as responses that cause some further harm to the relationship between the two states but does not change the fundamental status of the relationship (Davis, 2015). Thus, if the initial action is deemed to be severe then a reaction might be chosen that has some potential cost to the aggressor but does not cross the threshold of war. This type of response is characterised by the desire to satisfy the need for retaliation, while maintaining rationality and preserving future

safety of the state. This type of response might be used by smaller states or those that have limited military capability when acted against by a more powerful state. It affords the state an opportunity for protest and perhaps limited retribution without the prospect of further escalation of violence. It is understood by the architects of this reaction that the relationship between both states has not crossed the threshold into war. The implication of such a response is to show that the actor is not willing to allow further attacks to go without response. An example of this type of response can be found in the use of economic sanctions against Russia in the wake of the on-going Ukrainian Civil War. As Russia was deemed to be the aggressor, a large number of states have instituted sanctions against the state. This type of response goes beyond a non-response, such as a verbal condemnation, but stops short of addressing the alleged crimes of Russia directly: ie through funding Ukrainian groups with the goal of violent resistance to Russia.

When one considers reactions that are in proportion to the initial attack, it is important to note that only the interpretations of the victim state are critical to the reaction formulation. If the initial attack is interpreted to be an act of war by the victim state, whether this be through misinterpretation or otherwise, then if the subsequent reaction is in proportion to the attack, then both sides will have made the transition from peace to war. Thus, reactions are the pivotal state in determining a shift in relationship between two states such that they are at war. Even deliberate efforts at proportional response can be risky however, even if states only respond to air strikes with air strikes, there is an underlying assumption that further violence might trigger war between the two states and it is important to note that the responding state may consider any action that it takes as in proportion to the initial action even if this is not how the state they are responding to would see it. The US almost went to war with Iran in 1996 after a bomb blast in Saudi Arabia killed a number of Americans and injured hundreds more (Freedman, 2008:

303-306). One could argue that this would have been disproportionate, but the US believed that it was a viable and potentially justified response.

'Crucial to an understanding of war – is the optimism with which most wars were commenced' (Blainey, 1976: 35). If the state decides to react in a manner that outstrips their own capabilities as well as the expectations of the aggressor, the result may be escalation of the conflict. The initial action might have been intended to cow or deter the state attacked but this can be counterproductive e.g. when the actor misinterprets the intention or is unexpectedly incensed by the damage caused by the initial action (Becker, 1968). This might lead the victim state to choose a method of response that is wholly out of proportion with expectations of the aggressor. In this case, war is the likely outcome, with the aggressor further responding to an escalated attack. The risk in this case is that the escalation will spiral (Glaser, 1997: 180).

When we considered intention, we examined the factors that pressure politicians and policymakers in their planning. Furthermore, the interpretation of the state can be influenced in such a way as to interpret an attack to be of far greater significance than it was intended to be. As a result, the miscalculation of both sides can lead to a situation whereby reactions can seem, at least to some participants, out of proportion to the original act. For example, one could argue that the 1914 Austro-Hungarian invasion of Serbia was a response out of proportion with the death of Franz Ferdinand. It is only through considering the construction of interpretations and intentions that we can make sense of the reaction in context. This type of reaction is an important object of study, as it represents a critical minority of cases where a state perceives itself so aggrieved that it is willing to escalate to war based on a perceived attack more severe than any intended by the state against which it goes to war.

4.3 Summary

In summary the Action Phase Reception Phase model presents a new framework for examining how states make decisions regarding actions and consequent reactions. Intention stems from the impact of domestic and international pressures, and refers to the desired outcome sought from a deliberate action. Intention is influenced by expectations about the possibilities of a specific outcome and likely responses to the initial action by the victim state. This tees up the possibility for a state to confound the expectations of the aggressor.

Interpretations and reactions make up the final sections of this chapter, are likewise influenced by internal as well as external pressures on the state. Interpretations are critical in understanding how a misalignment can occur between how an action is intended and the expectations of those who made the calculated decision to commit it, and how it is received by those affected. This can include scenarios where an action might be received as an act of war to which it would be legitimate to respond with military force, even though it is not intended as such. However, that does not mean a war will follow, since a state may choose for prudential reasons not to respond with escalation even if believes it would be justified, in principle, in doing so.

It is clear is that there is no universally agreed upon framework for understanding how cyber attacks should be conducted and how they should be reacted to. Normalised understandings have not yet been established because the technology is so new and methods of response have not been sufficiently tested (Finnemore and Sikkink, 1998: 896). There is considerable room for misperception. The subsequent chapters will apply the framework set out here, to elucidate the dangerous ambiguities and uncertainties this throws up regarding the threshold for committing an act of war.

Chapter 5 Stuxnet

This chapter will use the APRP framework laid out in the previous chapter to analyse the calculations and interpretations surrounding the Stuxnet cyber attack. To do so we examine intention through contextualisation of Stuxnet. We will analyse the reasoning behind pursuing such an attack and the internal and external pressures that influenced the Bush and Obama administrations. The expectations of the administrations will also be examined. It is clear that neither administration anticipated that Stuxnet would become public and be attributed to the United States. The method chosen was limited by a desire to remain within the bounds of international law as well as ensuring that war would not break out between Iran and the US. The Iranian interpretation forms a key part of understanding the subjectivity of the threshold between peace and war in this instance. We will analyse the evidence of the Iranian interpretation, as well as the broader political context for it. We will look at the factors that influenced the Iranian interpretation. In the final section, we will examine the types of reaction that might have been plausible for Iran in this scenario. We will analyse the limiting factors that may have constrained Iran's choices and we will examine the Iranian reaction itself in two steps: Firstly, we will discuss their restrained reaction i.e. the small number of press conferences that dealt with the attack after news of it became public. Secondly, we will examine the impact of their retaliatory cyber attack on the Saudi Arabian oil companies.

5.1 Action Phase

5.1.1 Intentions

Halfway through his second term, President George W. Bush tasked Secretary of State Condoleezza Rice and National Security Adviser Stephen Hadley with finding a solution to the Iranian nuclear programme. In February 2006, Iran had announced that it had halted its

voluntary adherehence to IAEA protocols, in April they had announced they had enriched uranium for the first time (Gul, 2012: 38). Threats of IAEA sanctions did not deter the Iranian programme so American interests in the region could be threatened by Iranian aggression. Armed with nuclear weapons, the Iranians could be assured of some protection against invasions of the kind the US mounted against other rogue regimes the same decade. General Michael Hayden, former National Security Agency Director, notes Bush felt his options in this case were binary: let Iran get a nuclear weapon or go to war to stop it. Given the problematic fallout from the war in Iraq, Bush requested a third option from the two aides, (Gibney, 2016, Sanger, 2012). Invasion of Iran or other major use of force, would lead to a situation that was unacceptable both to the US domestic audience and the wider global political one.

The solution came from within US Strategic Command (USSTRATCOM), under General James Cartwright. Alongside Director of National Intelligence Mike McConnell, Cartwright advocated for a cyber attack that would take advantage of the small cyber defence unit he had set up, that would later become US Cyber Command (USCYBERCOM) (Sanger, 2012: 191). As Iran announced a resumption of uranium enrichment in late 2006, it was evident that there was little time for internal wrangling between rival US agencies such as USSTRATCOM under the DoD and the NSA (Kroenig, 2014, 46). Thus, the solution was presented to Bush by Cartwright, as an attempt to 'throw sand in the gears'. There was some disagreement about the likely effectiveness of the proposed plan; the United States did not have a great deal of experience in cyber attacks and a number of senior administration officials were concerned about the ability to carry cyber attacks out (Sanger 2012, 192). However, the President was enthusiastic about the idea and gave it an immediate go ahead which enabled the beginning of Stuxnet's development, Rice and Hadley also supported the cyber idea but on the basis that the CIA had not found a workable kinetic solution (Sanger 2012, 192-193). Thus, work began on a cyber attack that would aim to slow the pace of the Iranian nuclear programme by a year or two. It

was generally understood that it would be a short-term solution to a long term problem, but there was hope among members of the Bush administration that this would buy precious time to devise other measures that would halt the programme permanently. The code name for this plan was Operation Olympic Games.

Stuxnet as it came to be known was the creation borne of an intention to manage the Iranian nuclear problem, in a safe and covert manner (Kushner, 2013). Financially, a cyber attack was preferable to another invasion of an enemy state. Cyber weapons do not require supplies, nor do they need constant field updates to ensure their safety. Much less expensive than a conventional military attack on an enemy target and potentially more effective. In addition, there was the political risk of a new major war without the support of the general public, which would hurt the administration if the military aims prove more difficult to achieve than expected. The argument was made that if the Israelis were allowed to bomb Natanz, the site of one the largest nuclear facilities in Iran: "it will take the Iranians two years to replace it- but they will do so deep underground; you won't be able to get it the next time, and you'll make them want the bomb even more" a participant in discussions surrounding the Iranian issue told Sanger (2012: 190; Kroenig, 2014: 47). The team that began work on Stuxnet was a joint NSA-CIA venture based out of Fort Meade, Maryland and a nuclear command base in Nebraska and were allocated a significant amount of the $300 million in resources allocated to countering the Iranian nuclear programme (Sanger, 2012: 191; Bohn, 2019; Slayton, 2017: 97).

The creation of a cyber weapon that could damage the Iranian nuclear programme without the need for a traditional military platform would be beneficial in other ways also. Cyber attacks lend a degree of anonymity to the attacker, meaning that it could be possible for the US to avoid blame for the effects of Stuxnet once they became clear, or even to misdirect blame towards other actors (Kushner, 2013). Anonymity in this sense is important; The US could avoid

retaliation because it would be hidden behind the relative safety of a covert, unattributed attack (Foltz, 2012: 46). The cyber attack had the potential to avoid retaliation in from both cyber and traditional military means.

Sanger (2012) argues that Stuxnet was a solution to a difficult problem and that the rationale behind its creation was to avoid another war essentially civilian means to achieve military goals. We have discussed the issue of intention of Stuxnet, from the point of view of the main actors, we now move to the internal and external pressures that faced the US in the wake of Iranian resumption of uranium enrichment. As a result, the US could have had good reason to believe that Iran would not find out about Stuxnet and thus would not have to worry about a retaliatory strike.

In this section we will examine the influences both internal and external that had an impact on the decision to deploy Stuxnet. These factors encouraged the formation of intention and drove the decision to act in the case of Iran.

In 2006, the United States and the Bush Administration was coming under increasing pressure on the domestic front as well as from their allies in the Middle East to deal with the issue of Iran. US-Iranian relations had been consistently poor since the 1979 revolution and were made worse by the nuclear issue (Davis et al, 2013: 44). By 2006, the United States was in a difficult situation; facing two lengthy wars in Afghanistan and Iraq as well as increasing tension over the Iranian nuclear programme. Domestically, Republicans such as John McCain, John Bolton and Democrats including Hillary Clinton had voiced their concerns about the Iranian problem and Bush complained to Secretary of State Condoleeza Rice as well as National Security Advisor Stephen Hadley (Guha and Gowers, 2005; Sanger, 2012: 191). It was understood that the

American public would not accept another war in the Middle East. Given the relative successes and failures of recent campaigns in the region, the United States could not be able to guarantee against further major loss of American life if military intervention was given the go-ahead in Iran.

However, it was important to the Bush Administration as well as American interests in the region more broadly, to ensure that the Iranian government did not obtain nuclear weapons. Zetter (2014) contends that it was the belief among certain White House staff in the period of 2009-2011 that Iran would not have to actually build a nuclear weapon to be a threat. Through enriching enough nuclear material, Iran could choose to build a bomb at a later date, safe in the knowledge that the most time-consuming element of the process was complete (Zetter, 2014: 82). A nuclear-armed Iran could upset the balance in the Middle East, allowing Iran certain protection against invasion from Israel for example. It would, of course, also give Iran power to continue to fund militant organisations that target Israel, Saudi Arabia and others without fear of reprisal. These factors put pressure on the US government to deal with the nuclear issue. The problem was how to do so while limiting potential retaliation.

There was pressure too, from Israel. The unique relationship and trade partnerships between the two countries has impacted on the foreign policy of the US in the wider Middle East. As one of the prominent allies of America in the region, Israel is strategically important for US interests. Many defence contractors in the US have a stake in the relationship for continued business as Israel depends on arms shipments as well as financial aid to combat terrorism within its own borders and to reassure its population regarding fears of invasion from their neighbours. Israel is still the only nuclear power in the region, though it does not officially acknowledge this (Cohen, 2010: 6). While the United States and Britain were engaged in conflict in the region, Israel's concern was the fringes of its own, contested, borders. Israeli government intelligence

consistently report that the Iranian government was funding the various Palestinian liberation movements indirectly (Cohen, 2010: 8; Kaye et al, 2011: 68).

In 2005 the Iranian government had an open policy of castigating the Israeli State, and prominent leaders, including then-President Ahmadinejad, espoused Anti-Semitic or Holocaust-denying sentiments (Vick, 2005; Zetter, 2014: 81). Furthermore, as the state in the region with some of the biggest oil reserves, Iran poses a threat economically, militarily and existentially to Israel. The Israeli government regularly made reference to the Iranian problem in dealings with the Obama Administration's US Middle East negotiator Dennis Ross (Sanger, 2012: 159). The threat of unilateral action against Iran by Israel was quite real. The Bush administration had refused to act on Syria despite considerable pressure from the Israeli government including former head of Mossad Meir Dagan. He had repeatedly warned Hadley about the dangers of Syria and that Israel would act without the help of the US (Sanger, 2012: 221).

With the same concerns for intervention in Syria as Iran, the Bush administration chose not to act and the Israeli air force bombed a Syrian facility in September of 2007 (Spector and Cohen, 2008: 15). Thus, when Dagan emphasised the Israeli concern regarding Iran to the Bush and Obama administrations, it was evident that the threat of unilateral Israeli action could not be taken lightly. This was combined with intelligence gathered on the Netanyahu administration which indicated to the Obama administration that the Israeli PM was shoring up support in the event that he ordered a bombing of the Natanz facility. Netanyahu, Dagan, as well as some members of both Bush and Obama administrations were clearly in favour of pursuing a kinetic option. Netanyahu in particular was unimpressed with the success of Stuxnet and believed that it only delayed the inevitable (Sanger, 2012: 225). Thus, there were considerable pressures on both Presidents to be seen to act on the issue of Iran. It was fundamental to the intentions of the

US in devising and deploying Stuxnet that it should deliver results which would alleviate this pressure somewhat.

Further pressure came from America's other allies in the Middle East and beyond. In a series of diplomatic cables, Saudi Arabia said that Iran had gone too far. King Abdullah al Saud pressed for American action on the issue, though he was clearly unwilling to plunge Saudi Arabia into a direct military conflict with its largest neighbour (Riyadh Diplomatic Cable I: 2008). He was not pleased with apparent inaction. The King of Bahrain was likewise concerned with Iran on sectarian grounds, fearing a Shi'a revolt under his minority Sunni leadership. The Jordanians, like Israel, raised matters regarding support for terrorist organisations within their country that seemingly led back to Iran (Sanger, 2012: 160). German intelligence was concerned about the Iranian nuclear programme too. Their own information seemed to contradict that of the US National Intelligence Estimate released in 2007 and the Germans were unconvinced that Iran did not pose a threat to the wider world (Berlin Diplomatic Cable I: 2008). This was echoed within the US. Mike McConnell then Director of National Intelligence remarked to the Senate Armed Services Committee that the NIE was not conclusive (Washington Times Wire, 2007). Defence Secretary Bob Gates would later dissent from the NIE at a congressional hearing (Zetter, 2014: 86). Thus, the US faced considerable pressure to deal militarily with the Iranian issue, as it was clear that the nuclear talks were not solving the problem (Davenport, 2021).

Meanwhile Iranian actions put further pressure on the US to be seen to do something. The inability to come to an agreement regarding the cessation of Iranian uranium enrichment brought the talks to a close and marked the failure of the Bush regime to bring an end to the controversial programme as a whole (Jones, 2014: 354). Iran resumed enrichment at Natanz in 2006 and the government announced that they were revoking their voluntary suspension of uranium enrichment and began feeding their Etafahan plant with nuclear material to the

consternation of the IAEA (Zetter, 2014: 82; Tarock, 2016: 1409). Further to this, in 2009, the regime announced a new nuclear facility at Qom after IAEA inspections. The Americans had been aware of this facility since 2007 and though Bush had had the opportunity to destroy the plant, he had chosen not to act because of the fear of potential hostages being taken and the deaths of American soliders on Iranian soil (Sanger, 2012: 155).

Iran has a history of having secretive nuclear facilities, Natanz was announced under similar circumstances in 2003. Senior aide on counterproliferation to the Obama administration, Gary Samore, noted that if Iranian government were working on a bomb, it would be at a hidden plant (Sanger, 2012: 154). The Natanz site was designed with a large amount of storage and laboratory space. Experts have calculated that 47,000 centrifuges that could fit within the 32,000m^2 facility (Zetter, 2014: 73; Clapper, 2011: 4). The Iranian nuclear scientists based at Natanz have never managed to completely fill the space with operating equipment.

It is clear then that the Iranian government's actions put a degree of pressure for action on its nearest neighbours and therefore the United States as their ally. These contextual factors are key to understanding the intentions behind the US decision to deploy Stuxnet. By 2006 the pressure was such that the Bush Administration had decided it must act on Iran. Such was the importance of Operation Olympic Games, that President Obama was given two briefings on the details of Stuxnet shortly after his inauguration (Sanger, 2012: 201; Gibney, 2016). The operation's purpose was to interrupt Iranian progress toward nuclear weapons, but – crucially- to do so without provoking a war with Iran.

Thus we can separate four separate goals that Stuxnet was designed to achieve: to hinder the Iranian uranium enrichment programme; to hide the origin of the malware such as to make the

attack unattributable; to avoid war; and finally to prevent Iran and other states from behaving in certain ways contrary to US interests. These are important goals to keep in mind as we will return to analyse the success of Stuxnet in achieving these goals later in the chapter.

5.1.2 Expectations

Both Obama and Bush insisted that Stuxnet be completely unattributable (Sanger, 2012: 202; 193). There was a simple reason for this: avoiding war. If none of the CIA's kinetic options could counter the nuclear option effectively, then either bombing or invasion seemed likely alternatives. The decision to go ahead with Stuxnet was as a result of risk calculation built around the probability of Iranian retaliatory in the event of a conventional military approach. The parameters and design of Stuxnet helped to mitigate these risks. Given the previously established risk of failure of any bombing attempt on Iranian nuclear site, and the domestic pressures that would come from another invasion in the Middle East, Stuxnet seemed like the best option.

Anonymity, however, was paramount and was one of the main reasons that Stuxnet was chosen as the best option in this case. Invasion, but also covert military operations such as an incursion and sabotage and bombing, can all be traced directly back to the actor relatively easily after the fact. The nature of the cyber attack in this case was to protect the US from retaliation by making this more difficult. Stuxnet was designed in such a manner that would make Iranian scientists question their own equipment rather than look for an outside source (Sanger 2012). One could argue that Stuxnet's mission failed in this important regard; it was eventually discovered, and the evidence pointed clearly to the US or Israel. Sanger notes that many of the early meetings surrounding Stuxnet were with lawyers discussing the nature of cyber attacks and the possibility that Iran could justify a physical use of force against the US or its allies in retaliation

(2012: 193). Colonel Gary Brown, formerly of USCYBERCOM, notes that his legal team were called in to discuss the legalities of different types of cyber attacks in during this period (Gibney, 2016). The prime concern at the time was that very few people were versed in both law of war and also cyber attacks. Brown's team looked at what the group could do, i.e. what was in the realm of technical possibility; then what they may do, i.e. what would be legally permissible; and finally to examine what the US should do (Brown, 2011: 72). This shows that there was serious concern among the groups in charge of overseeing cyber attacks such as Stuxnet regarding both the legal implications and the potential consequences in terms of legitimate Iranian response. By limiting potential damage and embarking legal oversight, the US aimed to control the parameters of the expected outcome.

The cyber attack, it was eventually decided, would not result in a retaliatory strike as Iran would have no legal grounds for doing so. Notwithstanding the advance of technology, the aim of international actors has always been to select the best means of achieving a goal following a calculation of benefit and risk (Shusterman, 1992a: 178). This necessarily involves anticipating the range of plausible and likely responses to an action. Cyber technology adopts a new method of acting upon others but does not transform this fundamental dynamic. It was this central to calculations at this stage, that US leaders believed they could determine what would – and would not – constitute an act of war. It is important to examine the technical aspects of the Stuxnet malware to understand the grounds on which they based their expectation that it would not lead to a military response.

Stuxnet was designed to upset uranium centrifuges, based on perceived imperative to disrupt the Iranian uranium enrichment process. Iran had supposedly discarded its nuclear weapons programme early in the 21st century, but its continued pursuit of enrichment raised suspicions as to the motives (Heinrich and Holland, 2010). At minimum conservative analysts have argued

advancing enrichment meant that if relations with Iran deteriorated further, the Iranian authorities could restart a weapons programme with relative ease (Davis et al, 2011: 19). Iranian enrichment activity was also a focus of concern for Israel and other US allies pressing the United States to act. At this time, it was reasonable for the US to assume that a cyber attack would not precipitate a kinetic response as there was no precedent for it.

Choosing a target for Stuxnet was integral to the creation and design of the worm itself. Stuxnet's specific operating procedure meant that it could only be effective in a limited number of cases. It appears that the Natanz facility was specifically targeted as it represented the best chance of success. The rationale behind this may have been linked to the reliance on the older IR-1 centrifuge at the facility. Natanz is also one of the largest uranium enrichment facilities in Iran. The plant at Qom was revealed by the Obama administration in 2009 and the Bush administration were aware of it in late 2007 (Sanger, 2012, 155). But as work on Stuxnet began in 2006, it is unlikely that Qom was the target and changing operating parameters for Stuxnet after work had begun might have led to unacceptable delay given the known threat posed by Natanz. Another site, Bushehr has been the subject of some attention: there had been a two month delay in bringing the reactor online – some cyber security experts were quick to blame Stuxnet for this and it later emerged that a number of the staff's personal computers had been infected (Chen, 2010: 3). But the official statement was that a fuel storage leak was the main reason for the delay (Chen, 2010: 3), and light water plutonium reactors, such as the one based at Bushehr, are ill-suited to the creation of weapons-grade radioactive material. This gives further credence to the belief that Natanz was the intended target (Farwell and Rohozinski, 2011: 25). Lending more support to Natanz's targeting comes from the evidence of the infiltration of two Iranian companies based close to the nuclear site: Behpajooh and a further industrial company Neda in the weeks prior to the worm appearing in the plant itself.

The United States has a history of working either alongside or against information based technology firms in order to further its interest online. Washington has worked with software giants such as Microsoft and Google in order to gain email information on specific individuals (Poulson, 2020). Siemens, the main producer of SCADA[14] systems, sold a number of machines to Iran and were later named as colluders for the Stuxnet intrusion (Dehghan, 2011), though there is no direct evidence in the public domain. Stuxnet was designed to work around Windows, the predominant operating system. As it was vulnerabilities within the Microsoft operating system that allowed Stuxnet to use the rootkit, it is conceivable that Microsoft may have given some help in finding of the zero-day vulnerabilities[15]. However, given the fact that Microsoft took nearly five years to patch the vulnerabilities exposed by Stuxnet (Mendoza, 2015), it is doubtful that the company would have used such exploits if the potential cost was so high. One incentive for the American officials that worked on the creation of Stuxnet to steer clear of using Siemens as a potential partner in the deal would have been that Washington was becoming increasingly concerned in the latter part of 2008 about the German intelligence services that had raised so many questions regarding the NIE in 2007. Doubtless with the help of Siemens itself the process may have been easier and faster to create. The company may have been willing to export new patches that included a version of Stuxnet to the Iranian nuclear scientists based at Natanz. But if more actors were brought into the operational sphere, it would threaten the vital imperative to maintain the anonymity of the source of the attack.

Stuxnet is different from common malware; it targets industrial control systems and delivers its payload under very specific conditions. This allowed the worm to take control of simple SCADA based controllers, which were responsible for keeping the machinery operating within a very specific set of parameters. The SCADA systems that were being run in Iran, operated with

[14] Siemens is the largest proprietor of SCADA systems, since their initial creation. The German company continues to provide software patches as well as the further introduction of new industrial systems to the controller.
[15] Zero-day vulnerabilities are previously undetected holes in software that allow malicious actors to gain access to key parts of a system (Zetter, 2014b; Greenberg, 2016)

WinCC/Step 7 software are similar to those run in Britain and the United States, indeed these controllers see widespread use in the factory and power plant industries around the world (Chen, 2010: 3). As such, if Stuxnet was to find its way into the uranium enrichment plants in Iran, it posed a serious threat to the programme. The level of difficulty in accessing SCADA systems indicates a high degree of effort. Ilias Chantzos, director of government relations at Symantec[16] estimated that it would have taken 5-10 people up to six months to code Stuxnet even with access to SCADA systems (Chen, 2010: 3). Despite being designed specifically for WinCC software, Stuxnet also had to be capable of communicating with Windows PCs to spread effectively. Ralph Langner notes that Stuxnet was capable of infecting any Windows PC but was very specific about the type of controller it attacked (2011: 49). Even though the perceived cost of this implementation may have been significant, Stuxnet still held a better chance of holding an effective cost to benefit ratio once it had been released than traditional military means to accomplish a similar task (Farwell and Rohozinski, 2011: 29). Indeed, it has been estimated that Stuxnet may have cost $10m, considerably less than the price of a single jet fighter (Butrimas, 2014: 21).

As a piece of malware, Stuxnet was larger and more complex than other forms of malware that had been found and used at the time (500kb is much larger than other worms such as the SQL Slammer worm which was 376b and the Nimda worm which was 60kb)[17] (Chen, 2010: 3). Given its size and complexity, it is arguably surprising that the Stuxnet worm went almost a year without being discovered. It was only once Stuxnet had been spread 'in the wild' and was beginning to attack personal computers that it was brought to the attention of cyber security firms. The size of the worm along with the fact that it had exploits for four unpatched vulnerabilities within the operating software meant that it was on a malware level that had never been seen before (Li and Mu, 2014: 1420). Based on the code, experts have suggested that

[16] Purveyor of Norton Anti-Virus software as well as a host of other cyber security products.
[17] 1kb (kilobytes) = 1024b (bytes)

the creators had detailed knowledge of the target and vast resources (Chen, 2010: 3). Zero day vulnerabilities are exceptionally rare and allow unparalleled access to system and root commands. These exploits have an average of 348 days before being discovered within systems (Zetter, 2014: 142).

The first and primary mission of Stuxnet was to monitor and record information that was processed through the network at Natanz (Sanger, 2012: 199). This data was vital in allowing the worm to remain hidden for such a long period of time. At such a time as the worm had gathered sufficient data, it would then begin to alter the operating parameters of the centrifuges, while in essence playing a recording of previous operations back to the screens and dials. This way, the nuclear scientists working at Natanz would be confused regarding the results of the ongoing enrichment as the data did not match the outcome. Stuxnet contained a rootkit that concealed commands downloaded from the SCADA systems (Farwell and Rohozinski, 2011: 25; Collins and McCombie, 2012: 85). This allowed the worm to better infiltrate the software: Stuxnet was in essence able to both see commands issued by Iranian nuclear scientists and issue its own while concealing its existence and interference. This rootkit also allowed for more direct control of SCADA systems from outside sources. Stuxnet would routinely attempt to gain access to the internet using peer-to-peer communication to learn about new updates to its own software, presumably to counterbalance patches released by Siemens (Collins and McCombie, 2012: 86; Chen, 2010, 3). Furthermore, it attempted to connect to command and control servers, which were located, enigmatically, in Denmark and Malaysia to report on data that it had intercepted and to download further executable files (Chen, 2010: 3). Stuxnet's control servers being located outside of the US or Israel held a number of benefits. In the immediate it deflected suspicion from either country. As the US had been involved in sabotage of the Iranian nuclear programme in 2005, it would be a highly ranked suspect as perpetrator of any new effort. Control servers in other countries would muddy the attribution of

blame. Furthermore, to trace information that may have been relayed through the servers back to the US or Israel would require cooperation from Danish and Malaysian authorities that might not be forthcoming

Stuxnet had a built-in expiration date of 24 June 2012, approximately three years after its initial release (Farwell and Rohozinski, 2011: 23). Its ability to continue to do damage was therefore relatively limited due to its expiration and the availability of antidotes. The rationale behind the expiration date may have been that the US expected Stuxnet to do more damage before being found. Stuxnet was discovered in November 2010, just under a third of the way through its life cycle, and while it had managed to cause a number of serious incidents, it had not had enough time to cause as much significant damage as could have been expected (Barzashka, 2013: 48). The expiration date may also have been built in to allow the US a cut off date if there had been any progress in nuclear diplomacy. Any rational actor would want to build in a control system to allow the cyber attack to be stopped at will. The worm was designed to operate semi-independently, which could have been problematic for the US in the long term. Had there been no expiration date on the Stuxnet malware, but nuclear talks had resumed and Stuxnet discovered; this would have placed further strain on the US-Iranian relationship (Weber, 2018: 245). The expiration date may also have been built in with future-proofing in mind: the Iranian nuclear scientists were already working on a newer more efficient uranium centrifuge to replace their older designs. Stuxnet was only designed to work on the original IR-1 centrifuge (Lindsay, 2013: 387). The US, being aware of the plans to replace the older models, would have seen little point in extending Stuxnet's operation beyond three years even with optimistic centrifuge replacement targets by the Iranians.

The Iranian IR-1 centrifuge[18] was developed from the Pakistani P-1, the plans for which were purchased from A. Q. Khan, one of the main architects behind the Pakistani nuclear weapons programme (Albright and Walrond, 2011: 1). Due to the restriction on sale of nuclear enrichment technology however, Iran was forced to make do with parts from the black market or custom-made Iranian parts to build their centrifuges. The IR-1 was notoriously unreliable, and it is estimated that the Iranians kept an estimated 5,000 centrifuges in reserve for parts or to serve as replacements as they broke down constantly (Langner, 2013: 15). The inefficiency and unreliability of the IR-1 was supplemented by the possibility to develop the centrifuges on an industrial scale. While the IR-1 was problematic, their use was still enabled by the ability of the Iranians to build and replace them as necessary (Langner, 2013: 6). The US had a history of sabotaging the Iranian nuclear programme, in 2006 it supplied defective equipment to Iran through a number of Swiss nuclear engineers and caused up to fifty uranium centrifuges to explode (Lindsay, 2013: 385). Arguably then the experience gained from this exercise would have served the cyber division well as it understood the weaknesses within the Iranian IR-1 design. While Stuxnet was by no means rushed into production, there may have been concerns about the effectiveness of the worm on the planned IR-2 centrifuge that would be more efficient and would be more reliable (Zetter, 2014: 830). 1,200 IR-2 centrifuges could produce enough weapons grade uranium for a bomb within a year, whereas it would take 3,000 IR-1 models to do the same (Zetter, 2014a). Had Stuxnet been released later in the production cycle, it is likely that the Iranians would have had more time to build and install the newer more resilient centrifuges, thereby limiting the impact that the worm had on the enrichment process.

The Israelis were an important part of the process of implementing the attack on the Natanz reactor. The nuclear plant near Dimona, Israel was the testing arena for Stuxnet and its

[18] In order to produce viable enriched uranium, the element must be turned into its gaseous form and then sent through the centrifuge in order to purify it. In order to boost efficiency, the uranium centrifuges are set into cascades, such that the enriched gas gets sent to another centrifuge for further purification. These cascades are arranged such that a number of failures on the line will not compromise the entire facility. In Natanz, cascades are made up of 164 centrifuges (Zetter, 2014: 1464).

predecessors, which allowed the operators some degree of experience when estimating the damage that could be done (Lindsay, 2013: 384). Their cyber focused Unit 8200 was responsible for the placement of the Stuxnet worm on pcs that may have been eventually linked to a SCADA based system (Lindsay, 2013: 384). Stuxnet's attack on the Iranian nuclear programme began on the 23rd June 2009 with an attack on a number of industrial companies[19]. Foolad International was the first victim of the Stuxnet attack. Though Zetter argues that Behpajooh was the far more effective attack the following week, Foolad is an international engineering company, based in Tehran, that focuses on steel management and modernisation (Foolad International). Another three companies were subsequently targeted by Unit 8200, including Neda Industrial, Kala and CGJ (Zetter, 2014: 339). The rationale behind attacking industrial companies rather than the facility itself was that there were likely to be easier ways to infiltrate a private company and infect their computers than getting into Natanz itself. The covert method of the attack was designed to avoid detection. By selecting several industrial companies, the US and Israel could not be guaranteed of a direct infiltration of Natanz, but the plan succeeded. Stuxnet infected the Natanz computers perhaps as soon as five weeks after the initial infection (Sanger, 2012: 192). Stuxnet's controllers in the US expected that once a number of centrifuges failed at Natanz, the Iranians would shut down the entire cascade, thus delaying uranium enrichment (Sanger, 2012: 199). According to Sanger, American officials have since attempted to reconstruct events as they led to Stuxnet being installed in Natanz (2012: 204). It has been postulated that an Iranian scientist connected a laptop to the facility's network; Stuxnet then transferred across and began conducting its work on the Natanz internal network.

According to Siemens 11 of 14 plants infected with Stuxnet were in Iran (Farwell and Rohozinski, 2011: 29). Though Stuxnet was clearly designed to impact one target, the spread of Stuxnet to other plants both within and outside of Iran was always a possibility. The US

[19] This date is important as it marks the announcement of the re-election of President Ahmadinejad. It seems highly likely that the two incidents are linked given the relationship between Ahmadinejad and the US.

government must have been aware of it and decided it represented an acceptable risk. As Stuxnet was installed on the SCADA systems in Natanz, it began to change the information sent to the controllers independently of the scientists' commands (Matrosov et al, 2010: 42). The centrifuges, being of a delicate design, could not withstand the parts spinning at rates that were outside of typical operating parameters. Exact figures for the number of centrifuges that were damaged by Stuxnet are difficult to find. Sanger noted that the third instance of Stuxnet shut down 984 centrifuges in Natanz (2012: 206; Albright et al, 2011: 2).

Iran stopped feeding Natanz centrifudges for a whole week in November which could have been an indication of a serious breakdown (Farwell and Rohozinski, 2011: 29). This combined with the 23% decline in number of operating centrifuges from mid-2009 to mid-2010 might have been as a result of the Stuxnet attack (Farwell and Rohozinski, 2011: 29). However, it cannot be definitively known if Stuxnet was solely responsible for these effects. It has been argued plausibly that Stuxnet could have destroyed most of the centrifuges all at once, but this was not its inherent function (Hagerott, 2014: 245). The estimated cost of replacing these centrifuges is $1.8 million (Slayton, 2017: 103). Stuxnet's power as a cyber weapon is underplayed in some reporting. The technology was in place to allow Stuxnet's controllers to cause greater damage the Iranian nuclear programme, both in terms of physical facilities and prestige. But Stuxnet's creators understood that doing so would mean that there was clear evidence of sabotage, and all research indicates that the creators did not intend for Stuxnet to be released 'into the wild' nor ever to be found. If one assumes that Stuxnet's creators did not intend to see Stuxnet discovered, then perhaps Hagerott's claim regarding the worm is correct: Stuxnet was designed to erode confidence in the system (2014: 245). By making Iranian scientists lose faith in their machinery, there may have been a chance that the nuclear programme would have been damaged on a longer-term basis. It has been estimated that even in the short period it did operate, the Stuxnet attack set back the chance of Iranian nuclear weapons by five years

(Roberts, 2013). Shortly after the news broke regarding Stuxnet, a senior Mossad official estimated that the damage to the Iranian nuclear programme could delay Iran's ability to build a nuclear weapon till 2015 (Lindsay, 2013: 366).

Stuxnet's discovery by VirusBlokAda in June 2010 may have surprised the NSA operators in control of it. Stuxnet's escape 'into the wild' caused numerous issues on personal as well as industrial computers. It was Kaspersky Laboratory, a Russian Cyber Security agency and Symantec that cracked the code to understanding what Stuxnet was and how it operated. It is from these findings that scholars deduced the origin of Stuxnet, its target and its alleged outcome (Kushner, 2013: 48). However, Langner (2013), notes that this was perhaps not the first iteration of the Stuxnet worm. In 2012 another worm was discovered that was, in fact, an older more complex version of the Stuxnet malware programme. Stuxnet's twin, was designed to be even more invasive than its successor. The rationale for the simplified form of Stuxnet as ultimately deployed is a matter of speculation, but arguably the US, seeing and understanding the difficulty of installing a larger, more complex file within the Iranian nuclear system, opted for the simpler model as a matter of ease and effectiveness.

McGraw states that the danger of the Stuxnet lay within the code itself (2013). The worm had an expiry date but did not prepare for every eventuality. There was no way for operators who sent the coded messages to Stuxnet to know the exact operating parameters of the IR-1 uranium centrifuge. Having some knowledge of the antiquated design allowed the NSA/Unit-8200 to build the code. But because the Iranian government had been under nuclear sanctions, they found it increasingly difficult to get parts specific to the design. This meant there could be any number of defects within just one centrifuge (Bernstein, 2014: 166). While Stuxnet was designed to damage the centrifuges beyond repair, there were eventualities that it simply could

not account for. However, this could also allow Stuxnet to hide between the faults that already existed.

The anonymous nature of Stuxnet gave the Obama administration plausible deniability which allowed them to take a calculated risk. Michael D Hayden, who was head of the CIA during the start of Stuxnet's deployment, has declined to state what he knew of the attacks while he was in office (Sanger, 2012: 200). General James Cartwright was listed as party to the Stuxnet program several times in Sanger's work, however it was not until late 2016 when he was eventually tried and convicted for leaking the information to Sanger, that it was discovered he was the source of many of the public facts surrounding the operation (Guardian News Wire, 2013). Furthermore, the Department of Homeland Security also seemed to keep up appearances on Stuxnet. Within days of the attack coming to the attention of the general public, the Department had analysed Stuxnet and run it through a series of tests on centrifuges in Idaho. The operators at the ICS-CERT[20] laboratory had also reversed engineered much of the code hidden in Stuxnet within weeks of its discovery (Zetter, 2014: 185-186). There is no information that indicates that Homeland Security knew about the origin of the Stuxnet attack or that they were informed of the NSA operation at any point during their investigation. These factors show a willingness on behalf of the US government administration to continue to conceal any knowledge of Stuxnet. This afforded the Obama administration a certain degree of plausible deniability when faced with questions regarding Stuxnet and its impact. Outwardly the President and his administration continued to appear to want to work with the Iranian regime towards a non-violent resolution of the nuclear issue (Robb and Wald, 2014: 34).

The US expected that Stuxnet would remain undiscovered and complete its mission completely covertly. However even if Stuxnet were to be discovered there was a good chance that it would

[20] Cyber division of the Secret Service

not be attributed to the US, at least directly. Moreover, if Stuxnet was attributed to the US, there was no precedent for a kinetic response to a cyber attack and therefore they could expect that Stuxnet would not precipitate an act of war. Stuxnet's design was such that it had limited output to aid its covert nature. That limited output helped to ensure that even if Stuxnet was discovered and correctly attributed to the US, it would not be considered an act of war and so would not produce an Iranian reaction to that effect.

5.2.1 Summary Analysis

The range of actions towards Iran that the US deemed appropriate was limited by a number of factors: the financial cost and political risk of another potential war in the Middle East as well as the pressure from allies forced the US to re-evaluate the method of acting on the Iranian nuclear issue. Despite the pressures against acting, the US under Bush and later Obama was determined to be seen to be proactive on the issue. The intention to act was predicated on a number of expectations regarding the ability of a cyber attack to anonymously infiltrate the Iranian nuclear programme. There had been no cyber attack that had previously led to an armed conflict or indeed an armed response and thus the US was confident that the range of options for response on behalf of the Iranians would be limited to the cybersphere. Furthermore, a number of legal consultations with White House counsels helped to solidify the notion that the cyber attack did not breach international law. Stuxnet appeared to be a good solution to a difficult problem. The expectations of its capabilities as well as the predicted response were deemed within the bounds of acceptable risk and thus the US went ahead with their intention to use the cyber attack to infiltrate Natanz. Therefore, it is arguable that while Stuxnet was premised on the notion of unattributability, the US still had grounds to believe that a conventional military response was unlikely.

There are two assumptions that these expectations and intentions are based on: namely that Stuxnet would remain anonymous and the attack would not be discovered. In the minds of the US policymakers, this limited the range of responses and the risk of retaliation. The eventual discovery and publicity that surrounded Stuxnet proves that even some of the best coders cannot account for every eventuality. Thus, one could argue that the risk was not fully accounted for in this instance. Also the US could rely to a certain extent on its nuclear deterrence: it is unlikely that Iran would ever attempt a direct attack on the US homeland as losses ultimately incurred would not be proportionate to the damage to its nuclear programme for which it was retaliating. Such actions were considered outside of credible expectation. Furthermore, it was expected that the Iranian government would show restraint in the face of the attack. With no precedent for an armed retaliation, it would prove difficult for Iran to justify making a kinetic attack on the US. However, these expectations were based on contestable assumptions, about social facts subject to change. It is not clear that the US had completely accounted for all the variables. While Iran might have acted in a certain manner to the Stuxnet attack, this does not necessarily indicate that all cyber attacks can be formulated on the same premises. The risk associated in assuming that precedent assures outcome is a concerning issue that must not be underestimated.

5.3 Reception Phase

5.3.1 Interpretations:

In this section we will examine the Iranian interpretation of Stuxnet and the factors influencing it. We should break our study of the interpretation of Stuxnet into two sections. Firstly, it is necessary to fully understand the societal value that had been placed on it's target, the Iranian

nuclear programme. In such a way we can determine if it was of such significant value that a damaging that target would mean that war could not be avoided. Secondly, we should look at the interpretation of the Iranians to the attack itself.

It is important to understand how the Iranian media, public and the administration perceived of what had occurred at Natanz. How important was Natanz to the national narrative? The Iranian government has staunchly defended its right to continue a nuclear programme despite the protestations and sanction of other states and the UN (BBC News Wire, 2009a). This indicates the importance and prestige the Iranians attach to the notion of being a nuclear state. However, it does not necessarily show that the Iranian government was intent on building nuclear weapons. The ability to enrich nuclear material, such as uranium and plutonium, is a contested area: while the NPT maintains the right of states to undertake research in nuclear energy for peaceful purposes, the motives of the Iranian government have been questioned due to their previous weapons programme (NPT, 1968).

Iranian government officials have consistently argued that they have a right to produce their own enriched material and there is widespread public support for maintaining the nuclear programme (BBC News Wire, 2009a). Highly-enriched uranium has a number of uses, particularly medical which is one of the main reasons Iran has argued for the loosening of restrictions in this particular case. The Iranian governments relationships with the Western world have been fraught since the 1979 revolution and it could be argued that their attempt to build a strong nuclear power programme is an attempt to address this.

As a nuclear state, Iran perceives it would attain a level of prestige that is not currently afforded to it. In addition, the Iranian public see the nuclear programme as a mark of Iran's

modernisation; this is inherently tied into notions of economic and social betterment. Furthermore, Iranian oil will become prohibitively expensive to use as a fuel source as wells dry up and the natural resources of the country deplete. Thus, one could argue that the Iranian nuclear programme has become an important part of the national narrative, not just in terms of future use but also in maintaining the capacity of the state to act autonomously which is contrasted sharply with its past. An attack on such an important part of the Iranian national narrative could be interpreted as an assault on fundamental national sovereignty. If this narrative and sovereignty are conflated, then an attack on the nuclear programme must appear on par with a territorial incursion or the assassination of a political figure.

It is worth discussing the importance of the Iranian nuclear programme as a whole to the Iranian government and society, because it helps explain why an attack on it could produce devastating consequences. Iran's relationship with nuclear power and nuclear weapons has been made more problematic by its relationship with the US and Israel. As previously stated, the Iranian regime had given up on a nuclear weapons programme early in the 21st century but had continued to enrich uranium which was deemed a continuing threat to its neighbours. Under IAEA guidelines, any state has the right to nuclear power under specific conditions (1989). The Iranian regime had broken several of these guidelines in pursuit of becoming a nuclear state. By continuing to enrich uranium, the Iranian regime was signalling to the US and its allies in the region, that it would operate outside of its jurisdiction. The nuclear issue has become an important signifier of Iranian distinction from the rest of the Middle East and is often seen from an Israeli standpoint as signalling intent to become a nuclear weapons state. The creation of a nuclear weapon however would be a direct threat to not only Israel but also to Saudi Arabia, two of the strongest powers in the region (Ahmad et al, 2017: 103). Through the development of enriched uranium, the Iranian regime can continue to edge the balance of power in the region in its favour and signal its refusal to bow to US influence. The Natanz plant has therefore become

more than simply a scientific facility, it has become an Iranian symbol for resistance against imperial domination and an integral signifier of independence. The Iranian government has successfully manipulated the arguments at home to the extent that an attack on the Iranian nuclear programme has become an attack on Iranian sovereignty itself. This status on the part of the nuclear programme is clearly shown in the creation of a national day of nuclear power which is celebrated in Iran, heralding the work of nuclear scientists in the country in a manner interwoven with nationalism and societal identity (Mobasherat and Yan, 2013).

Several prior experiences may have influenced Iranian interpretation of Stuxnet. Since the 1979 revolution, the United States has continually attempted to undermine the Iranian regime, through supporting Iraq in the Iran-Iraq War and later imposing economic and trade sanctions against the country. Post-1979, anti-Americanism has been a theme of Iranian identity, at least as articulated by government. We have set out the rationale for Stuxnet from an American standpoint by reference to the background context and the pressures put on the US during the period 2006-2009. One could make similar arguments from the Iranian side for its lack of justification. The NIE, released in 2007, while Stuxnet was still be tested, concluded that Iran had given up its nuclear weapons program and there was no evidence that it had been restarted. From an Iranian standpoint, then, there was no legitimate basis for the deployment of Stuxnet except perhaps to further assert American dominance in the region. It may be true that it was unlikely that the US could have done nothing if Israel was threatening to do so unilaterally if there was inaction (Lindsay, 2013: 380). Had Israel decided to bomb the Iranian nuclear facility, there would have been far greater repercussions for the US and its interests in the region. But this obviously does not qualify as justified grounds from an Iranian perspective.

In the period between the deployment of Stuxnet and its discovery, almost 10% of the active centrifuges were replaced (Warrick, 2011). That this indicates is that there was no clear

understanding of where the problem lay. Iran may have felt that this was simply as a result of faulty equipment though this was a higher than normal replacement schedule. Therefore, we can make the case that the initial Iranian interpretation was likely one of confusion, in the deployment phase, surrounding the cause of the breakdown of a large number of centrifuges. As the number of failing centrifuges continued to rise, replacements were rolled out in order to keep up with production targets. When examining the apparent fall or otherwise of enriched uranium production, it is important to note that the statistics do not necessarily represent the facts on the ground. Indeed, the large amount of space at Natanz was specifically designed to allow for a larger number of centrifuges to operate than the Iranian Atomic Agency ever successfully managed to install and thus the large number of spare centrifuges made allowances for the shoddy construction and parts of the traditional IR-1 design. At least 900 centrifuges were replaced during this period according to surveillance data from within Natanz (Warrick, 2011).

Initial blame for the breakdown in the centrifuges was apparently placed upon the Head of the Iranian Atomic Energy Organisation. The attack on the Natanz facility meant that with no external blame to be found, it was necessary for Golam Reza Aghazadeh to resign (BBC News Wire, 2009). The notification of his stepping down came on July 16, which was just a few weeks after the initial Stuxnet infection. This perhaps indicates that there was an initial burst of activity once Stuxnet had been deployed in order to test its capabilities. At the time the BBC reported his resignation there were several concerns over his potential links to other Iranian presidential candidates and to his efforts in nuclear negotiations with the United States (BBC News Wire, 2009). Thus, the initial interpretation of the Iranian regime was to blame its own people for incompetence rather than to look to external forces as the source of the centrifuge breakdowns. It was a key part of the US intention before Stuxnet's deployment to undermine the confidence in the Iranian nuclear team. As a cyber attack of Stuxnet's character had never

been undertaken before, it is likely that the Iranians were not aware that a cyber attack had caused the destruction of a large number of centrifuges.

This combined with attempts to air-gap the system through completely disconnecting the facility from the internet, which may have made the Iranians unduly confident that the malfunctions were not as a result of a cyber attack. The internalisation of blame may also have been influenced by the international context and the nature of the Iranian system. Rather than immediately looking to blame an external force such as the US, in a time when many Iranian citizens seemed to regard the Obama administration favourably and in the wake of a tumultuous Iranian presidential campaign, Iran's leaders had incentives to prefer a more understated approach to the problem. There was no way to be certain of the absence of external intervention at Natanz, but it was not clear that the Iranian public would have been receptive to blaming external actors, and Ahmadinejad's reformist opponent in a disputed election still maintained a degree of support. The rise of the Green Movement and protests across Iran had forced the government to act, quelling the demonstrations, often violently (Debashi, 2010: 49). A public denunciation of an alleged sabotage without evidence or indeed the firing of an Iranian nuclear official for failure would have raised questions among the general populace as to the compentence of the government at a crucial juncture. Thus, Aghazadeh's resignation was downplayed, and it was not clear who or what was to blame for the breakdown of such a large number of centrifuges.

It was a year and a half later before the Stuxnet attack was made public through VirusBlokAda, during which time the Iranian nuclear scientists had continued to struggle to explain why centrifuges continued to fail and further work was expended replacing broken cascades with functioning ones (Warrick, 2011). By November 2010, it was not clear how far the Stuxnet infection had spread within the Natanz plant though it was spreading throughout the internet

and was being brought to the attention of the wider anti-malware community. The revelation of Stuxnet would have shocked the Iranian administration. It was clear from their earlier actions that the Iranian scientists considered that sabotage was not possible with an air-gap between Natanz and the outside world. What followed was a series of press interviews, the first indicating that the Iranian regime were aware of the attack but that it had not compromised their systems. The Head of the Bushehr power plant stated to the press that Stuxnet had only made its way on to personal computers of the staff and had not compromised the facility (Markoff, 2010). It was not until late November, when President Ahmadinejad gave a press conference outlining the damage that had been done and the cost of securing the Iranian computers, that it became clear that the Iranian government had suffered a severe setback in their nuclear programme.

A number of Iranian nuclear scientists were killed in suspicious circumstances over the following months, and it has been suggested that the Iranian regime was naturally displeased with how the initial infection of Stuxnet occurred (Sanger, 2012). The Iranian government may not have interpreted Stuxnet as a full-blown violation of sovereignty, but it took the damage done very seriously. The damage caused by Stuxnet was relatively limited as the Iranian scientists could replace broken centrifuges with new ones that were held in stock. Barzashka even argues that due to an increase in centrifuges operating during the period, there was no significant drop in output during the Stuxnet attack (2013: 53). There is no way to measure if the cyberattack had the intended consequences of causing scientists to second-guess their own work. However, the deaths of two senior scientists as well as the resignation of their head of the Iranian atomic agency, indicate the chilling effect on relations between the security state and the scientific programme. The initial lack of a vocal public response on the part of the Iranian government could plausibly have been motivated by a desire not to admit the vulnerabilities exposed by the attack.

Most other states have remained quiet about the revelation of Stuxnet (Fidler, 2011: 57). While the United States and Israel had motives for doing so, it is not entirely clear why other states such as Russia did come out to condemn unilateral action against Iran. While not specifically addressing Stuxnet, Russia has called for a greater role of the International Telecommunications Union that would undercut American hegemony in online matters. If the ITU attempted to stigmatize and limit cyber attacks like Stuxnet it could undermine US military advantage in this area (Lewis, 2011: 72). But the extent to which Russia would itself abide by such restrictions is not at all clear. Given the history of the Russian involvement in executing or facilitating cyber attacks on other states, its posture seems like a move solely designed to undermine the credibility of the US. Had other states been more vocal, then we might have seen Iran be more willing to respond with strong condemnation of US actions and contemplation of direct retaliatory response.

Typically, in the case of aggression between states, actors debate the relevance of international law as it applies to the specific case. However, this has not been the case with Stuxnet. 'Generally speaking, however, international lawyers perceive silence as acquiescence to the legal implications of actions or incidents. With Stuxnet, silence across the international system suggests that states don't perceive this situation triggered the rules on the use of force, armed attack, and aggression' (Lewis, 2011: 58). Indeed, it is not clear that the Americans were entirely clear on their obligations to international law when they began developing Stuxnet. Law makers focusing on international law are still struggling to develop legislation that encompasses the internet and cyber attacks. However, Lewis's conclusions may be overstated in this instance. The silence of nation states on cyber attacks has been broken several times, albeit not always forcefully by Russia, China, and the United States. Stuxnet may have received silence from so many states because the ends were regarded as justifying the means: there remains worldwide

disapproval of nuclear programmes that exist outside of IAEA approval. Political expediency justified the silence, while policy makers around the globe focus on the desirability of developing new cyber security techniques to combat malware like Stuxnet. Iranian spending on cyber security is at an all time high, however. Stuxnet may not have been significant enough to warrant widespread condemnation, but it has certainly changed the way in which policy makers consider cyber attacks.

5.3.2 Reaction

It is useful to discuss the types of responses available to the Iranian government when considering retaliation for Stuxnet. We can categorise the types of responses into a number of areas: kinetic verbal or cyber. A military response would mean an armed attack that might involve loss of life or damage to infrastructure. Verbal responses mean protestations and condemnations of the attack, but not going as far as to retaliate in any physical way. Finally, a cyber attack means responding with a reciprocal attack in cyber form, perhaps on a US institution or business, even critical infrastructure. Which kind of responses seem appropriate will be determined by the interpretation of the initial attack by the affected country, the state of existing relations between countries, and the prudential calculations of the reacting state as to the consequences of each possible response.

There are a number of responses that fall under the category of military for the purposes of this analysis. In typical war literature, the prevailing theme is that one state goes to war with another using the military as a tool for continuing 'politics through other means' (Clausewitz, 2000: 264). This provides a useful starting point, but as the earlier literature review on war clarified war can be conducted in various ways. Covert acts such as assassinations; bombings and perhaps even information theft could be considered part of the military framework. These

actions can be defined in part by loss of life or potentially creating the conditions leading to loss of life. Buchan has argued that if Stuxnet destroyed centrifuges then it could be considered an act of war as it is a breach of Article 2(4) of the UN Charter (2012). One can conceive of circumstances where an attack of this sort was sufficient severe and destructive that the Iranian government would consider it had no alternative to treat it as an act of war. If the Iranian government felt that the attack on the nuclear plant at Natanz warranted a military response, then they could have appealed to this reasoning in justification. However, Iranian consideration of a possible military retaliation for Stuxnet would likely have been muted by contemplation of the imbalance of power arising from superior US conventional capabilities. There is evident scope for miscalculation here. However, by an attacking state that mis-estimates how its actions wil be interpreted, or an attacked state that misperceives the thinking of the initial attacker.

The US has vastly superior resources at its disposal and the Iranian government would be aware of this. As we stated in the previous chapter, reaction depends heavily on prudential calculation. In this instance retaliation might have incurred a further response from the US, and escalation into full-blown war. It is difficult to envision a situation where Iran would be committed enough to the principle of sovereignty that it would go to war over Stuxnet. Such a response would simply make little rational sense. Thus, it is unlikely that the Iranians considered an outright attack on the US as a viable option. If the factors were weighted differently however, ie the US had a smaller military advantage and the attack was considered damaging enough to warrant a conventional military response, then Iran might quite plausibly have considered such a response legitimate. However, it is more likely that the Iranian government sought to use covert operations as retaliation for Stuxnet to avoid a direct military escalation with the US. The Stuxnet attack caused no injury to any person working at Natanz and therefore to react with a military strike would be widely seen as disproportionate. Therefore, there was little reason for the Iranian government to consider a military response to Stuxnet, since it met the standard of

neither rational nor proportional grounds for such a response. Furthermore, the prudential calculation would have indicated that such a response may have incurred far greater damage than the initial attack.

A verbal response can be an alternative to military retaliation where further conflict is to be avoided. Verbal responses neither commit to escalation nor do they put lives at risk. Condemnation of state actions has been a consistent feature throughout political history. However, examples where this appears to be an effective method of deterrence are few, unless mixed with some more coercive methods. In the previous chapter we saw that Israel consistently criticised the US for being too lenient with Iran: as the US had not intervened against Iran directly until the latter half of the decade despite frequent verbal condemnations. There was pressure therefore externally and internally to act rather than continue to merely condemn the Iranian regime. While good motives can save a bad policy, they cannot replace that policy: words may have some impact, but it is action that ultimately determines outcomes. The Iranian government would have felt similar pressure however the resources at their disposal to respond with direct action were more limited. In some cases, verbal responses may be the only recourse available to the state.

A cyber response meanwhile could allow the Iranian government to respond directly and proportionally to Stuxnet. Furthermore, it would also answer the arguments that state that Iran must be seen to do more than talk if it is to respond to threats. The cyber response option was limited however by Iran's relatively weak cyber intelligence network (Valeriano and Maness, 2016: 25). As the Iranian cyber offensive capability is much lower than the US's offensive and defensive capabilities, there was limited benefit to be gained by adopting this approach. However, one should note that the logic of asymmetric attacks means that Iran could still, in principle, inflict heavy damage on the US through successful a cyber attack (Lindsay, 2013: 375).

Indeed, it appears that states with relatively weak cyber security abilities can still rely on cyber attacks as a means of inflicting damage or in response to attacks and threats (Valeriano and Maness, 2016: 25). Russia has previously used cyber attacks in response to perceived threats in Estonia and Georgia and thus there is a precedent for using cyber attacks both as a tool for response. Using a cyber attack to respond to Stuxnet would confirm that the prevailing logic of cyber attacks was one of restraint (Valeriano and Maness, 2016: 61).

5.3.3 Choosing a reaction

The Iranian government had a variety of options open to them when considering how to respond to Stuxnet, though it was considerably constrained by the relative power of the United States and its allies in the region. We must separate out two ideas: what Iran considered a legitimate response in principle; and what response it considered prudent in the circumstances. With limiting factors such as financial and military considerations to take into account, Iran was forced into choosing a reaction that would allow it to save face, but not further escalate the situation[21]. As such the Iranian government made a rational decision to react in a manner that indicated the attack on them fell short of the threshold for an act of war thus a restrained reaction. Iran's reaction was to Stuxnet was to call a press conference to denounce the attack but stopped short of referring to it as an illegal use of force (Fidler, 2011: 59). It seems unlikely that any state in Iran's position would be tempted to escalated by responding with military means, so long as those involved are rational actors. But it is quite possible that Iran might have behaved differently in response to a cyber attack if the circumstances had been different. It is unclear that a larger, more public attack on the Iranian nuclear programme would have elicited such a restrained response.

[21] There have been some attempts to link the 2012 Schamoon cyber attack to Stuxnet however it is more likely that Iran was looking to retaliate to a prior cyber incident with Saudi Arabia rather than respond directly to Stuxnet. Furthermore the time lapsed between the two incidents might indicate that this is a response to a later attack (Chan, 2016). The impact was limited by comparison with Stuxnet's output and the gap in years between Stuxnet and Schamoon are the main factors that would argue against a link. Some scholars however accept that this was an attempt to deter future cyber attacks by other regimes on the Iranian administration (Craig and Valeriano, 2016: 150) The investment into cyber tools such as Schamoon on the part of Iran may have been precipitated by the Stuxnet attack (Kello, 2017: 125).

5.4 Summary

This chapter has examined the Stuxnet case and analysed the relationship between the two main actors: Iran and the United States. We have concluded that the Stuxnet attack might plausibly have been considered an act of war if the contingent circumstances had been somewhat different, for example, if Iran had the capacity to respond with military force without certain defeat. Iran may have perceived the attack as an act of war in principle but felt that it was insufficient to warrant a military response. Retaliating in such a manner against a superpower would be unwise considering the potential repercussions. Thus, Iran decided to react only verbally. By choosing to use press conferences rather than a military or retaliatory cyber attack, Iran showed that they would save face rather than escalate the situation further. Stuxnet set a new standard of norms for behaviour in cyberspace and encouraged other states to engage in spending to enhance their own capabilities (Weber, 2018: 245). The threshold for triggering war was not crossed in this instance. This case study is useful as it illustrates the rationale on both sides for how their chosen course was arrived at. We can see that there is considerable scope for divergence, however, and given different conditions the outcome might have been very different. We will further examine the disparity between two states' interpretation of a cyber attack in the next case study.

Chapter 6 Estonian Cyberattack

Having examined our first case, it is useful to apply the same framework to another. The Estonian cyber attack has been chosen because it offers a different scenario to Stuxnet while it also shows clearly how intention, expectation, interpretation, and reaction combined can be considered to understand outcome. In this case the key actors are: Estonia, as the state that was attacked; Russia, the alleged perpetrator; and NATO, the organisation of which Estonia is a member, and that can be called upon to react to acts of war against its member states. This chapter will examine the context surrounding the cyber attack and the conditions that allowed it to take place. Furthermore, we will look at the intentions of the Russian state to better understand what the motivations were behind using a cyber attack when there were other means, such as economic pressure, available. We will then turn to analyse the Estonian perception of the incident. This will allow us to better understand how the Estonian government and people felt about the cyber attack during and after the incident. We will also examine some of the context regarding the relationship between Estonia and Russia. It is also important to examine the decision-making process of Estonia during this period in order to clarify its position towards calling for assistance from NATO. By choosing not to go, or threaten, to war or over the cyber attack, NATO and Estonia undertook a calculation process that should be examined.

The Estonian case presents a different challenge than that of Stuxnet as the Russian government have not taken responsibility for the attack. We can link this back to the problem of attribution that was discussed in Chapter 3. There is a strong link between Russia and the Estonian cyber attack, including circumstantial evidence that would certainly incline towards attributing Russian involvement. One can look at the demonstrations in Tallin, orchestrated by ethnic Russians living in Estonia in response to the moving of a Soviet war memorial (Valeriano and

Maness, 2015: 143). The Russian government took umbridge with the Estonian government over the same issue (Rid, 2013: 6). The cyber attack was arranged on Russian speaking web forums ((Davis, 2007; Hughes, 2010: 352). A youth group that took responsibility for the attack has very close links with Putin's government (Shackelford, 2009: 205). The Russian Parliamentary Leader attempted to inject humour into the situation by implying that his assistant had been involved, which did little to de-escalate the situation (Singer and Friedman, 2014: 111). Finally, the Russian government did not agree to assist in finding the perpetrators when Estonia invoked a bilateral Mutal Assistance Treaty (Lucas, 2017: 118; Kello, 2017: 130). These facts coupled with the overarching relationship between Russia and its former allies present a compelling case for attributing the attack to Russia.

6.1 Action Phase:

6.1.1 Intention

To assess the intention of the Russian government in the weeks leading up to the cyber attack, it is important to understand the longer-term context. While the US and Iran have a relationship that has been troubled for the past 40 years, Estonia and Russia have a historical connection that has existed for close to 400 years, in which Estonia was controlled either directly or indirectly by the Russian state (Bruggemann and Kasekamp, 2008: 246). Following the fall of the Soviet Union, Estonia became an independent state and made moves towards joining NATO and the EU, both of which it joined in 2004 (Wrange and Bengtsson, 2019: 456). The move away from the former Soviet bloc towards a new partnership with the EU, and the West more broadly, signified a desire to move politically and ideologically away from the Russian sphere of influence (Lane et al, 2013: 172). This came with several new possibilities and challenges. The EU is more transparent in dealings with its member states, and based on cooperation rather than command and control as had been the case under Russian domination. The reorientation was widely accepted by most of the Estonian population as the being in the best interest of the

newly independent state. However, this has met resistance from Russia[22], which still sees the Baltic states as within its sphere of influence and from ethnic Russians living within Estonia who see the move towards the West as a threat to their national identity and the traditional links that the state had with Russia. Removal of symbols and monuments of Soviet/Union national identity valued by ethnic Russians have been controversial, though supported by a majority of Estonians.

February 2007 witnessed the passing of the Forbidden Structures Law by the Estonian Parliament. The law was designed to address the desire by a majority of the Estonian people to remove all signs of the deemed 'occupation' by the Soviet regime (Clarke and Knake, 2010: 12). The Estonian President argued that this was unconstitutional and vetoed the law. However after a fresh general election in March, the government decided to press forward with the removal of some of the contentious statues and memorials in Tallinn. A decision was made to move the Bronze Soldier statue that memorialised the Soviet defeat of the Nazis, as well as being a tomb of a number of soldiers, known and unknown (Clarke and Knake, 2010: 13). Lobbying and protest from within Estonia predominantly from ethnic Russians arguing against the removal did little to sway the government from their decision. The two-meter Bronze Solider was to be moved to a military graveyard on the outskirts of Tallinn. The bodies of the soldiers interred were to be laid to rest either with the Bronze Soldier or, in some cases, repatriated to Russia as per the wishes of the families (Rid, 2013: 6).

In Russia, outrage over the removal of the Bronze Soldier escalated quickly in the months leading up to its eventual move and beyond to its peak on May 9th. 71% of Russians were opposed to the move and 26% of Estonians believed the move was a bad decision (Valeriano

[22] Russia has been operating a system referred to as hybrid warfare which is a combination of cyber warfare, sanctions and direct military involvement to influence its neighbours (VenBruusgaard, 2016; Thorton, 2015: 41; Lanoszka, 2016: 175).

and Maness, 2015: 143). In Moscow, Russian youth group Nashi su[23] surrounded and attacked the Estonian embassy. This led to complaints from US, NATO and EU. The blockade of the embassy was eventually ended with pressure from the West, and a deal brokered by Germany (Shackelford, 2009: 206). In Estonia too there were a series of riots between the two ethnic groups between 26-27th April culminating in 1,300 arrests, 100 injuries and the death of an ethnic Russian (Rid, 2013: 6). This increase in violence in Estonia involving the ethnic Russian population, and the overwhelming disapproval of the removal of the Bronze Soldier, in Russia, influenced the Russian state towards acting on the issue.

Russia's intention in this case was to support the ethnic minority of Russians in Estonia. The Russian state may also have had some desire to punish Estonia for its reorientation away from the former Soviet states towards the EU and NATO. Estonia is not the only state at risk in this regard, however, as Estonia and Latvia have large ethnic Russian populations and are also members of NATO (Lindemann and Sarr, 2012: 1975). The ability to mobilise support and subversive activity among its ethnic population abroad has been a hallmark of Russian foreign policy into the twenty-first century. Approximately 7% of the Estonian population is ethnically Russian which represents a considerable political force if they can be mobilised (Valeriano and Maness, 2015: 144; Wlodarska, 2016: 154).

In the background of Russia's intentions was a sense of lost prestige after the fall of the USSR in 1991. The loss of superpower status, as well as considerable land and population loss to newly independent states were major setbacks the Russian state faced as a result of the end of communism. Since then Russian political leaders have resorted to appealing to nationalism as a means of maintaining domestic support (Mastriano, 2017: 71). In parallel, the state has been

[23] Nashi su (youth movement, ours!) are a pro-Kremlin government funded group founded in 2005 with an anti-fascist agenda. The group maintains a membership of over 100,000 (Shackelford, 2009: 205).

adapting its approach to war by adopting information campaigns aimed at influencing the Russian diaspora, mirroring some of the information and education campaigns that were used in the 1930s (Mastriano, 2017: 68).

Russia could not be sure of the damage from a cyber attack. Until 2007, it was not clear that DDoS[24] attacks could be so efficient at taking down websites for prolonged periods of time. The attack on Estonia was in many ways a learning exercise, useful when Russia later used similar attacks on Georgia. Valeriano and Maness argue that Russia's cyber attack was among the least likely to cause damage of any of the options available to them at that time (2015:41). Limiting fuel supplies to Estonia, or mobilising armed forces along the border might have created the same pressure without causing as much economic harm. Valeriano and Maness (2015) do not of course take into account the option of doing nothing, though one could argue that, given the context previously explained, Russia was obliged to act.

There was a desire among the ethnic Russian population as well as the nationalists on the domestic front, to see some action on the case of Estonia. In this way, the case is similar to Stuxnet. The American government was under pressure to be seen to act from audiences at home and abroad. The manner in which both states managed that pressure was also similar. In their planning, both the US and Russia focussed on anonymity and reliance on the ambiguity surrounding cyber to veil their responsibility for actions. Cyber allowed both states to show some degree of force regarding a potentially problematic state without the risks associated with kinetic action. One could argue that in both cases there was also a latent desire to prove expertise within the cyber field. Until the Estonian cyber attack, an attack on the scale seen in

[24] Distributed Denial of Service are unique in their ability to cause widespread disruption and are cheaper than the usual Denial of Service method. DDoS attacks a viable method for states to incur damage on others with limited means Deseriis (2017).

this case had never been witnessed. Smaller scale hacking between states had been attempted but the Estonian case, and later Stuxnet, dramatically shifted the way in which cyber attacks were deployed. Both cases provided a seemingly low-risk opportunity for the US and Russia to test their capabilities.

It is important to understand why Russia chose to use a cyber attack rather than resorting to its more traditional means of influencing its neighbours or former close allies: economic and military bullying. Russia has shown that it will use bullying tactics to maintain its strategic position in Europe, such as stating Denmark would face nuclear targeting if it joined NATO's missile defence shield (Mastriano, 2017: 71; Herszenhorn, 2015). Russia has also been willing to move troops to borders of neighbouring states and conduct military exercises in a show of force. Furthermore, it has used economic incentives to convince states to remain within its sphere of influence as well as the threat of limiting energy supplies to enforce obedience on certain issues (Mastriano, 2017: 72). These tools have proven relatively effective in warning states away from certain policy decisions towards ones that Russia deems in its interest.

Why did Russia embark on a new form of coercion when it had a number of effective tools already at its disposal? Mastriano argues that the reasons centre around Russia's strategy of ambiguity: using cyber attacks as a tool of foreign policy gives Russia a degree of ambiguity regarding the true origins of the attack and plausible deniability. The burden is on the attacked state to determine that the cyber attack is in response to perceived threats to Russian influence. Through using third parties, Russia can distribute the blame to private citizens while continuing to support and upgrade its cyber capabilities (Janicatova and Mlejnkova 2021; Mastriano, 2017: 71). The fact that there is still some debate over the true origins and result of the Estonian cyber attack is a testament to how this strategy has afforded Russia a degree of distance with regards to responsibility for its foreign policy actions. Russia is not the only state that engages in this

type of strategy: China and the United States also engage in cyber attack activities, and both have exploited the lack of certainty regarding attribution (Shackelford, 2010: 26). While this strategy has been somewhat effective thus far, it is unclear how sustainable it will prove going forward. Russia and the United States have an effective nuclear deterrent, which greatly affects how the two states interact with each other in the case of cyber attacks against one another. The interactions among states generally when dealing with cyber attacks has been marked with restraint, as laid out by Valeriano and Maness (2015). Both those scholars and Jervis (1976) are aware, however, that previously established patterns can be subject to change if the interpretation or intentions of the actors change.

Russia has been continually developing its cyber capabilities since the early 2000s. The state employs a large number of computer experts that affords it the ability to strike at low cost when compared with military intervention (Hughes, 2010: 532). In addition to this, Russia has exploited resentments and capacities of its citizens by often choosing not to trace or arrest those involved in cyber attacks on other countries. Private hackers willingly join these efforts out of a sense of patriotism, as they are not considered criminals in Russia but held in high esteem (Hughes, 2010: 352). Russia's use of semi-independent contractors affords it a degree of ambiguity in relation to its cyber policy, but also allows for a degree of anonymity.

To what extent did Russia control the cyber attack on Estonia? The consensus regarding the attack appears to be that there was not top-down command and control of the attack, but the Russian military provided some of the technical knowledge and tools that would be used by the attackers and further facilitated and abetted hackers in their efforts to bring down Estonian websites and other critical infrastructure. Unlike the Stuxnet case, however, the tools for DDoS attacks are relatively rudimentary and were widely available prior to the Estonian attack. This did not involve the creation of a novel cyber ‘weapon’ that could escape into the wild. The scale

of the human element within the Estonian case, however, allowed more opportunities for error. That DDoS attacks are more rudimentary means that they require more humans to decide on key targets and length of attacks. In the Estonia case, media and banking sectors were hit hard, and there was a relatively small chance of a loss of life as a result. It is unclear if the Russian state had mandated that hospitals and electrical companies be omitted from the targeting parameters. If we accept the Russian state's version of events, then a large number of hackers based within its borders had been particularly selective about its targets, deliberately avoiding those that could cause a potential loss of life. Using private citizens to conduct foreign policy however leads to more variables that cannot be accounted for. Such lack of a clear command and control structure could generate unforeseen or unintended outcomes in future cases.

Unlike the Stuxnet case, it appears that Russia is covertly providing skills and tools to private individuals, which could potentially pose some risk to the state itself. Shackelford argues that diplomats and policymakers often lack the technical expertise to create effective regulations that would curtail cyber attacks (2010, 26). This might mean that some decision-makers also lack important knowledge surrounding cyber attacks and the limits of their capability to control them once launched. This lack of understanding could lead to miscalculations which increase the risk of intentions being misperceived by the state that has been attacked.

6.1.2 Expectations

Russia made the decision to support these groups based on a number of expectations. There was an expectation that the pressure from the cyber attack would change the manner in which Estonia went about implementing its Forbidden Structures Act. Furthermore, there was an expectation going forward about the type of relationship that Russia would have with Estonia. The Baltic state had made it clear that it wished to be part of the EU and NATO and therefore

aligned itself with the traditional adversaries of the former Soviet Union. The cyber attack was a message to Estonia as well as its allies about the level of tolerance Russia had towards its neighbours as they continue to move away from it (Mastriano, 2017: 71). There were risks with this approach. Russia would have had to anticipate that NATO may choose to involve itself as a consequence of the attack. It's possible that Russia was to rely on plausible deniability if this was the case.

It seems likely that the Russian state anticipated that the attacks would be traced to actors in Russia but, because of their number and spread the responsibility of the state would remain ambiguous and deniable. By minimising the links between the Russian state and the hacking groups, officials hoped that there would be enough separation between state and the actors in question. Some legal scholars (Roscini, 2014; Bussolati, 2015) have questioned whether this is enough to absolve Russia of the responsibility to ensure that its citizens are not conducting illegal activity. However, this has not discouraged the technique, which was used again in Georgia in 2008 and in Ukraine in 2014-15, alongside more conventional forms of pressure and threat when ethnic Russians are being persecuted, as Russian policymakers see it. Russia has used armed forces along borders such as Ukraine and Estonia to dissuade action against subversives that it has encouraged directly or indirectly (Mastriano, 2017: 72).

One could argue that the cyber attack functioned as a means for testing the responsiveness of ethnic Russians and nationalist Russians to such an effort. The loss in prestige for Russia in the post-Soviet era and the destabilisation of national identity and status was evident (Miskimmon and O'Loughlin, 2017: 113). Since taking power, President Putin and his allies have increasingly used nationalist rhetoric as a means of mobilising political groups and maintaining support. This has cultivated a virulent nationalist section of the population eager to come to the 'defence of the motherland' to action and support of its Estonia policy (Mastriano, 2017; Baltic Times,

2007; Kaiser, 2012: 1047). By attempting to mobilise this group, Russia may have been intending to analyse the response rate to determine how effective its policies had been in the past and the likelihood of future success using the same methods. Russia's influence on ethnic Russians in Estonia stands as an early example of a policy that would later impact Ukrainians.

The relative ambiguity of information warfare online has provided a layer of anonymity and served to confuse policy makers regarding appropriate response. The ambiguity and indecision in this case is further compounded by the strength of Russia's military forces (Mastriano, 2017: 69). The Russian use of information warfare, to incite and promote its agenda abroad is increasingly important in the development of new military strategy (Mastriano, 2017: 71; Janicatova and Mlejnkova 2021). It affords the state a growing sense of support, providing the government with a large pool of nationalists who are willing to work without pay for the cause while advancing state policy aims (Lucas, 2017: 116). In terms of Russian expectations regarding the likely outcome of the cyber attack, it was not certain before the fact that there would be a large response to the call. Russian language chat rooms were used as a means of recruiting and disseminating information regarding the attack but there were no guarantees that this would allow for such a widespread attack (Davis, 2007; Hughes, 2010: 352). Though, as Mastriano points out the Russian military had some experience with this kind of information warfare going back to the late 1990s (2017: 69).

Russia's expectations of prospective outcomes must have been limited by the knowledge of their nuclear deterrent. It would have been irrational for Estonia and its allies to embark on a war with Russia given the costs of such a conflict and given that the cyber attack did not cost lives. Thus, Russia likely believed that a kinetic military response was highly unlikely. One could make the case however given the damage done to the Estonian economy, and the sense of fear that this cyber attack instilled within the Estonian populace, that Russia perhaps

underestimated the extent of the damage of their attack. The outcome was uncertain in advance for the Russian state as there had never been a state-targeted cyber attack on this scale before (Shackelford, 2009: 194).

As in the Stuxnet case, much of the Russian state's plans in regards to the cyber attack was based on secrecy and the ambiguity surrounding the perpetrators. The key difference in the two strategies was that Russia chose to invest in private individuals rather than running all activity through official state cyber actors (Mastriano, 2017; Haataja, 2017: 3-4; Janicatova and Mlejnkova, 2021: 313). Arguably the use of an official state department group such as USCYBERCOM, creates a degree of transparency about the way in which states operate their cyber policy. Russia has had a different method in its strategy on cyber: preferring to keep their policies classified and use independent activists and hackers to do work on its behalf.

Two weeks prior to May 9th, one of the most important national days in Russia, on the 27th of April, the first cyber attacks began on Estonian government websites (Tikk et al, 2010: 18). Attacks initially focused heavily on government websites but later also included attempts to take down financial sites.

Rid (2013) argues that the move of the statue was poorly timed given its proximity to May 9th. With a fresh election in March of 2007, the ruling party felt it had a mandate to bring about change. Over-eagerness to wield power under that mandate may have led the government to act rashly. The fate of the Bronze Soldier was originally to be its destruction, under the Forbidden Structures Law, until the President prevented this (Kaiser, 2012: 1052).

The President's veto of its destruction may have been prescient given the level deal of societal concern about the fate of the Bronze Soldier (Baltic Times, 2007). Perhaps this decision may even have placated ethnic Russians to some extent in advance of the cyber attack, helping to moderate the intensity of the resulting crisis somewhat.

6.2 Reception Phase:

In this section we will outline how the Estonian cyber attack took place, its impact and the perception of the Estonian state. We will first examine the cyber attack, analysing the type of attack before looking into the manner in which it was executed in collaboration by state and non-state actors. Importantly we will inspect the links between the Russian state and a number of Russian language chat rooms that played an important part in propagating the tools of attack to a large number of users. We will examine the impact of the attack, looking at the different types of targets, to further expand upon the account of Russian intent outlined in the previous section. The perception of Estonia, including its people and the institutions of government, will then be considered, followed by an examination of how this fed into its ultimate decision on how to respond.

The attack itself began in the late hours of the 27th of April 2007 against a background of violence and general public disorder not only in Tallinn but also at the Estonian Embassy in Moscow (Shackelford, 2010: 22). What began as a small number of hackers defacing websites and attempting to attack servers directly, swelled considerably in the weeks leading up to the May 9th Day of national celebration in Russia. A move to using DDoS attacks marked a significant change in the quantity of targets and the strength of the attack. At this time, the number of internet packets sent to Estonia rose from 20,000 to more than 4 million per second (Shackelford, 2009: 204). The attack focused firstly on a number of media outlets and Estonia's

largest bank, but also saw the defacement of several government websites, including that of the Estonian Prime Minister (Shackelford, 2009: 208). On May 9th itself, six Estonian government websites were brought down, including the foreign and justice ministries. Estonia's main news outlet, the Postimees was forced to take its own website down as a result of repeated cyber attacks (Davis, 2007). Hansapank, Estonia's largest bank was brought down for 90mins on May 9th and a further two hours on May 10th prior to government intervention. 58 websites were attacked at once in a coordinated effort that saw attack lengths range from one to ten hours (Rid, 2013: 6; Shackelford, 2010: 204).

Estonian citizens had trouble using Facebook and accessing email throughout the period of the attacks (Valeriano and Maness, 2015: 143). While the attacks peaked on May 9th, by the following day, the Estonian government had unilaterally decided to limit all internet traffic coming in and out of the country. The result was that the Estonian people could not have their story heard by the outside world. Shackelford maintains that the Estonian government was lucky to have a good Cyber Emergency Response Team that managed to combat the attacks to an extent (2009: 206). By May 10th, credit card services had gone down, telephone networks were suffering severe trouble, and library services were affected (Clarke and Knake, 2010: 15; Davis, 2007; Valeriano and Maness, 2015: 143). Shackelford argues that on May 10th, Estonia could have faced more attacks on critical systems and vital services and would have been on the verge of complete digital collapse (2009: 206). This could have been hyperbole; it was impossible to know in 2007 if Russia had the kind of cyber capability that would later allow it to bring down the Ukrainian power grid in 2015. In Estonia, the attacks continued until May 19th (Rid, 2013: 6). At its height, there were 128 DDoS attacks targeting Estonia (Shackelford, 2009: 204). Valeriano and Maness have estimated that $750 million was lost in government and business revenue as a result of the cyber attack (2015: 145). Commerce suffered mainly because of the internet being down, but lack of ability to process credit card payments and ATMs being

down caused serious problems both for consumers and businesses. An estimated 85,000 computers were used in the cyber attack, an unprecedented number at the time (Rid, 2013: 6).

It is important to note the difference between this type of cyber attack and ones that preceded it. Rid notes that initially the attacks consisted of ping flooding, basic requests from the server (2013: 6). These are akin to Denial of Service [DoS] attacks. How the attack changes from DoS to Distributed Denial of Service [DDoS] attacks attack works essentially the same way as a DoS, a request is sent to a server for information.

In order to understand how a DDoS works, it is useful to first understand how the internet deals with traffic via servers. To consider this, it is useful to compare a server to a cinema. There are only a limited number of seats and once each of these is taken, no one can enter the room. A server functions in the same way, it can only deal with a limited number of requests for information at any one time (Shui et al, 2014: 2246). Access can be limited by filling the server with bogey information requests and thereby stopping other individuals from accessing the website. Very few websites reach their capacity with any regularity. If they are targeted or have a busy period, some businesses will expand their bandwidth which increases the amount of room on their server, essentially allowing them to deal with more requests. Servers can only deal with so many requests before the bandwidth is exceeded and the server goes offline. In such a way a few tens of thousands of PCs with access to the internet can inflict serious downtime (Donner, 2007: 4).

DoS attacks are an easy way to test the strength of websites and servers but can be time consuming and resource intensive, as each DoS attack requires an individual computer to operate. The Distributed form of this attack uses automation to covercome this limitation. The

attack relies on a number of 'zombie' computers with a botnet in control of the larger attack (Sauter, 2014: 9-10). These zombie computers are typically ones that are unsecure and have had some of their resources taken over by an outside computer. The botnet functions as the controller for a large number of computers and helps to coordinate the attack from a central location. The owners of these zombie computers are usually unaware that their system is being used in an attack (Osanaiye et al, 2016:147). There is a significant benefit to using this type of attack over the standard DoS, as more computers allows for a larger attack output. The sheer numbers associated with DDoS attacks mean that the attack tends to be more effective at taking down websites and servers. It also means that the botnet takes the bulk of the work, allowing the attack to be less resource intensive.

Therefore when we consider that 85,000 computers were used in the attack on Estonia, only a small fraction of these were actually operated by the attackers themselves. That small groups can conduct cyber attacks on such a large scale is of course concerning beyond the Estonian cyber attack case.

DDoS attacks are not kinetic, meaning they don't result in physical damage to equipment or people, and as such provide a different set of variables when compared to a cyber attack like Stuxnet. However the intention behind both is not entirely dissimilar. Stuxnet was designed to frustrate and degrade capacity by rendering key systems dysfunctional, while DDoS attacks are designed to frustrate through preventing access to specific services or websites.

6.3.1 Interpretation

To assess the perception of the Estonian cyber attack in Estonia, it is vitally important to understand the context. Estonia is highly dependent on internet connectivity for economic and

social activity. Being a pioneer of public space Wi-Fi, online registration for marriages, births and deaths, and numerous other examples of early-adoption, Estonia has become one of the most digitally advanced societies anywhere in the world (Reynolds, 2016). In 2007, almost 50% of 16-74 year olds were using the internet and in October 2005, Estonia became the first country to use internet voting (Tikk et al, 2010: 17-18). Rid argues that Estonia was vulnerable to a cyber attack, in part because of its reliance on the internet for basic government and financial services (2013: 6). One could argue that Estonia's reliance on the internet made it a target for these kind of attacks – DDoS attacks had previously been successful in taking down internet services, though not on the scale seen in the 2007 attack (Crandall, 2014: 36). The Estonian case is special because the internet is more pervasive in Estonian society than anywhere else in the world. Thus, one could compare this type of attack on Estonia to attempts to block radio signals at a time when wireless was the main method of communication between state and its citizens. The intention may not have been to completely cripple the Estonian government and society. However, as we have seen such an outcome was possible. During the attack, the Estonian government eventually decided to halt internet traffic in and out of the country as the cyber attack hit the banking sector and the media. This made it difficult for individuals to communicate through social media and payments were further delayed to retail outlets as credit card systems remained out of use for the duration of the attack.

In their fear of cyber attacks, the Estonian people are not necessarily concerned about the impact of the 2007 attacks, damaging as they were, but the potential damage that future attacks might have. This fear is arguably well founded since there have been a number of cyber attacks that have shown that generators can be damaged, such as in Idaho in 2007. Indeed, Shackelford argues that cyber attacks can do as much damage as the electromagnetic pulse associated with a nuclear blast (2010: 23). While some empirical examples have shown the potential damage of a cyber attack, this has yet to materialise and therefore can only be treated as fear of potential.

The potential of cyber attacks has been documented and thus one could argue that the fear on behalf of Estonia is warranted. Bussolati uses the Estonian case as an example of how cyber attacks are beginning to show their potential for damage, and it is important to note that the scale of the damage can go beyond what historical precedent has shown cyber attacks to be capable of (2015: 102).

Much of the perceived import of the Estonian state is based on what *might* have happened. As Rid notes, the actual lasting effect of the cyber attack was relatively minor (2013: 6). The perception remains however that the state could have fallen victim to a far worse attack if it had not acted to limit internet traffic. The fear of an impending attack, and of its potential effects, continues to shape the debates surrounding cyber attacks both in academic literature generally and in Estonia particularly (Haukalla, 2009; Rid, 2014; Mastriano, 2017). The Russian state clearly anticipated that there might be some damage to the economy of Estonia during the cyber attack, but it is not clear whether they maintained control over the situation at all times (Lucas, 2017: 103). The Russian state expected the cyber attack to be unattributable, making sure the links between the groups and the state were tenuous enough to make firm attribution difficult (Maurer, 2018: 97). This would provide ambiguity behind which the Russian state would hide, therefore creating uncertainty in Estonia and among its allies (Radin, 2017: 6). The Russian state did not intend to go to war as a result of using this type of cyber attack. If it desired that outcome, it would have adopted other, more directly aggressive means.

To understand how Estonia interpreted the attack, it is important to appreciate the importance of its adoption of internet technology to its self-image. The Estonian government prided itself on providing internet services where possible and creating a safe online environment for economic activity and growth. That the internet telecommunications company Skype was created and based in Estonia reflects the government's active pushing of the innovation of the internet as a

means for communication and of providing for citizens. The attack represented not only an attempt to diminish the security felt by Estonian citizens when accessing the internet, but also the prestige that the state had gained in the area of internet telecommunications. The measures for the damage to the economy can be quantified to a degree but it is harder to put a concrete value on the internet as a source of prestige for the state.

This was after all the first state in the world to embark upon e-voting. To be driven off the internet by a Russian-backed group of hackers with what appears to be relative ease, and doubtless low cost, was a serious blow to Estonian prestige. This was a significant factor in the perception of the attack by the Estonian state and citizenry.

The impact of the cyber attack was magnified by its effect beyond government, on the banking and media sectors. The Estonian Speaker of Parliament and holder of a doctorate in nuclear physics, Ene Ergma compared the cyber attack to a nuclear explosion (Poulson, 2007). This was hyperbole of course. There was no loss of life and physical property such as homes, business premises and government buildings were not affected in any kinetic way. But the analogy served to emphatically convey to NATO and the EU, of which Estonia was a member, the seriousness of the situation and its relevance to those organisations.

In our examination of cyber war, we analysed Rid's conceptions of warfare and his conclusion notes that ‘war’ implies a lethal or potentially lethal nature (Rid, 2011: 6). The Estonian government invoked language that suggested they put this attack on that level, albeit perhaps with an eye on future escalation as much as on this attack in itself. But did they mean this literally, I.e. that the Russian attack might merit a response at the level of retaliation that a conventional attack would?

There is evidence that the Estonian government wanted a harsher response from NATO on the cyber issue. Estonian Prime Minister Andrus Ansip compared the DDoS attack to a siege or blockade: "What's the difference between a blockade of harbours or airports of sovereign states and the blockade of government institutions and newspaper web sites?" (Rid, 2013: 7). The Estonian officials were understandably concerned with their vulnerability to such a large-scale attack. Comparisons between the scale of the Russian and Estonian armies should not be discounted as this may have limited the language used in Ansip's comparison (Espiner, 2008).

Despite the lack of definite evidence that the Russian state was behind the attack, the Estonian government maintained that the threat was born of a Russian sanctioned attack on the state (Davis, 2007). Estonian Ministers were not alone in their concern. A former army intelligence officer in the US also indicated that he believed that the attack was state sanctioned by Russia (Rid, 2013: 7). Definitive attribution of the attack was difficult for the Estonian government. Their argument that Russia was the perpetrator is based on the activity of Russian websites and chatrooms (Roscini, 2015: 216). However, many of the PCs that were attacking or being used in attacks were based in the US, which is not unusual given the location of key internet servers (Geers, 2010: 300). It appeared that some evidence has shown that IP addresses based in Russia, including some based at state institutions, were linked to instigating the attack. However evidence was so scant that the Estonian foreign minister later retracted claims to having evidence that the Russian state was directly responsible for the attack (Rid, 2013: 7). Perhaps in an attempt to inject humour to the situation, Sergei Markov, former Russian Parliamentary Leader, announced that his assistant had taken a leading role in coordinating the attacks on Estonia. The assistant in question, who remains unnamed, was a leader in the youth organisation Nashi su, which has been implicated in the Estonian Embassy blockade (Singer and Friedman, 2014: 111).

Attribution was especially difficult in this case due to the nature of the attack. DDoS attacks, as noted above, require a large number of zombie computers to fully achieve their objectives. This was often achieved without the knowledge or consent of the owners of these computers. As a result, a large number of computers involved in the attack were used without their owners' permission. It proves difficult therefore to trace the source of the DDoS among a large number of users who are implicated but innocent. Shackelford notes that the attacks originated from a wide number of countries including Egypt, Peru and Russia (2009: 204). A further breakdown notes that 25% of attacks originated from computers based in the United States (Singer and Friedman, 2014: 73). Attribution is made more problematic by the difficulty in assessing attribution beyond these zombie computers. Some of the IP addresses were clearly located in Russia and some were traced further back to origins within the country, but there is no definitive link between the military complex and the hackers involved (Ottis, 2018: 4). However, it still appears that the Russian state had influence on the hackers responsible for the attack. Estonia did claim it had some degree of proof that the Russian state was behind the attacks, but it later retracted these claims and ultimately NATO took no action against Russia regarding the attack (Rid, 2013: 7). In order to determine attribution in this case it is useful to examine later Russian conflicts for a pattern of cyber activity that would lead one to suspect a strategy is in place for dealing with states on its borders.

Similar cyber attacks were used against Georgia in 2008. These attacks however focussed on the military IT systems, rendering the Georgian state relatively defenceless against the Russian intervention. The DDoS attack proved effective in shutting down Georgia's military communications systems. Thus, troop movements and information were slowed at a time great concern for the Georgian state (Valeriano and Maness, 2015: 147). A significantly different cyber attack took place in Ukraine in 2015, one which shut down the power grid (Greenberg,

2017). Greenberg (2017) asserts that this particular attack is merely the most publicised of any of the attacks that have been penetrating Ukraine for the last three years, with details of the attacks indicating that they originate from Russia. This is in line with the claims of Mastriano (2017) and Clarke (2010) that Russia has been continually upgrading its cyber capabilities and using these and information warfare as a means of conducting foreign policy. There are clear benefits to Russian policy with regards utilising this type of attack as a means of controlling situations. Furthermore, the history of Russian disagreements with its neighbouring states is consistent with there being an existent strategy regarding cyber operations that utilises independent hackers.

It is worth noting that consultations on the invocation of NATO's Article 4 were held regarding the Estonian case shortly after the incident (Tikk et al, 2010: 120). Furthermore, the Estonian government, particularly the Defence Minister were considering invoking Article 5 (Shackelford, 2009: 194). Given the comments made by the Estonian President and the speaker of Parliament, it is clear that the Estonian government was of the view that there was a serious breach of sovereignty that came about as a result of the cyber attack and, as noted in an earlier chapter, violation of sovereignty is among the major grounds cited as cause for war, historically.

In this section we have discussed the impact of the Estonian cyber attack, the perceptions that it drew from Estonian and NATO, and the factors and context that influenced these perceptions. Estonia may have believed that the cyber attack was an act of war. Particularly notable is Prime Minister Asip's remarks, in the wake of the attack, regarding the similarity between the blockading of harbours or airports and the blockade of government institutions and newspaper websites (Rid, 2013: 31). The prestige of the nation was attacked by cyber attacks that crippled infrastructure and caused serious economic damage to the country. NATO, however, was caught in a difficult situation as it had to be seen to protect Estonia as a member state but was not

eager to get involved in a potentially dangerous diplomatic or military escalation with Russia. The consultations that took place with Estonian officials can be categorised as placatory rather than entirely supportive to some degree, as they addressed some but not all of the Estonian concerns (Haukkala, 2009: 207). Thus, when considering the reaction category of our framework it is important to note that there was some gap between the severity of the attack as Estonia percieved it and the mildness of the ultimate response. There was a distinction between its judgement of how it would be entitled to respond and its calculation of the prudence of escalating, especially without full allied support, but it serves as a suggestive indication that states can consider a cyber only attack as an act of war in principle.

Ene Ergma argued that testing Estonia's cyber defences is a way of testing NATO's defences and its responses (Davis, 2007). While difficult to decern how much intention Russia had of provoking a NATO response, it seems evident that testing the Estonian response would test the strength of NATO's leadership in this regard. As a new member to NATO, Estonia would be most likely to engage with the organisation to resolve any disputes it had with its significantly larger neighbour (Veebel, 2018: 306). Therefore it is worthwhile examining NATO's perception of the cyber attack and how this played out in the consultations that took place between its member states. There was concern within NATO member states including the US regarding the cyber attack on Estonia. Former army intelligence officer, Ralph Peters accused the US DoD of underestimating the threat of cyber attacks in the wake of the Estonian incident (Rid, 2013: 31). However NATO governments were reluctant to act precipitately, focusing on the need for attribution before any intervention could be made. The US, argues Shackelford, was ambivilant in their response to the attack; he notes a former chief scientist at DARPA who referred to the attack as 'more of a cyber riot than a military attack' (2009: 209). Indeed, while the US showed some concerns surrounding the attack, they focused more on the extent to which it illustrated American vulnerabilities rather than intervening on behalf of the Estonian government

(Shackelford, 2009: 209). NATO therefore urged caution and restraint rather than indicating any desire to retaliate forcefully.

6.3.2 Reaction

In this section we will discuss the reaction of the Estonian state to the cyber attack. It is important to outline the various options that Estonia had to respond with and underline why it reacted in the way that it did. The outcome of the cyberattack was the foundation of the Cooperative Cyber Defence Centre for Excellence in Tallinn (Akdag, 2018: 10).

Choosing to go to war over the cyber attack might appear obviously disproportionate in retrospect, but it is worth discussing why Estonia did not choose this option. It is important to understand the relative security provided to Estonia through its alliances with NATO and the EU. Estonia may feel that it has a legitimate reason and ability to resist Russia with military force if necessary. Sleats argues that while the Estonian case did significant damage, it was not enough to justify beginning a war as it was not aggressive enough (2017: 332). Roscini argues that there is an inherent problem with classifying the Estonian cyber attack as an act of war. Although critical infrastructure was targeted, the Estonian cyber attack caused no material damage and therefore did not violate Article 2(4) of the United Nations even if attribution could be fully determined (2014: 63).

As with the Stuxnet case, there are a number of different types of response that the Estonian government could have considered before embarking on their decision. In the immediate face of a continuing onslaught of attacks from nearly 100,000 individual computers based around the world, the Estonian government saw no recourse but to close the country to external internet traffic (Valeriano and Maness, 2015: 35). This included all traffic going in and out of Estonia.

While this helped to stem the tide of attacks, it also had another critical side-effect in that it prevented the Estonian news outlets from informing the rest of the world about what was taking place. While the attack was causing considerable damage to government and media websites, forcing Estonia offline could be seen as a success for the various hacking groups and the Russian state. In essence, the Estonian government was doing their job for them.

Estonia's response was a series of condemnations of the cyber attacks and further allegations of the alleged perpetrators. Russia's energy diplomacy also posed issues for Estonia, particularly with arranging of energy supply lines into Europe. Its relationship with Russia has been poor since, which has been made further problematic by Estonia being bypassed as a potential energy transfer partner (Crandall, 2014: 30).

A main theme of much of the legal literature surrounding the Estonian cyber attack is whether or not invoking NATO's Article 5 would have been possible for Estonia. Legal scholars are in some disagreement over whether or not Article 5 could have been invoked given the nature of the cyber attack and the lack of kinetic damage or loss of life (Roscini, 2014; Ohlin et al, 2015). Valeriano and Maness maintain that Estonia could have chosen to react through NATO. The response with NATO may have been a tit-for-tat and potentially escalated the conflict further. Estonia chose instead to invest in its cyber defences and become one of the world leaders in cyber security (Valeriano and Maness, 2015: 146).

The decision of NATO member states was that cyber attacks should only invoke Article 4, meaning that NATO members will consult on the issue as a threat to security but will not go as far as to invoke Article 5, which relates to self-defence (Euractiv, 2012). This policy is aimed at avoiding escalation and encouraging restraint among its member states, though some

academics such as Mastriano have argued that the nuclear deterrent forced a weak NATO response regarding Russia (2017: 73).

In 2008, NATO opened the Cooperative Cyber Defence Centre for Excellence in the Estonian capital. This was partially in response to the cyber attacks in 2007 and has helped to put Estonia at the centre of cyber security research (Gardner, 2009; CCDCOE, 2021; McLaughlin, 2021). While the creation of the Cooperative Cyber Defence Centre for Excellence in Tallinn proves a useful step in the understanding of the problems of cyber attacks, NATO appears to have opted in favour of cyber defence rather than choosing a more offensive strategy. Thus, NATO does not yet consider cyber attacks as acts of war on its member states. Despite this, not long after the Estonian cyber attack, its Department of Public Diplomacy, released a short film about the incident entitled 'War in Cyberspace' (Singer and Friedman, 2014: 123). This perhaps indicates that the institution has changed its outlook regarding cyber attacks and furthermore better understands the problems and threats caused by cyber attacks and their users. It could also be that Estonia, having calculated the political, pragmatic and strategic elements itself, made a judgement to back away from a fuller demand for support from NATO that it may not have accepted.

Russian use of cyber and further information warfare techniques has continued to expand and increase in its intensity. The alleged Russian role in supporting US Presidential candidate Donald Trump in 2016 also appears to indicate the continued use of these tactics (Rid and Buchanan, 2018: 8; Muller, 2019: 36). Despite facing condemnations from within Europe and on the floor of the US House of Representatives, the Russian government has continued to use cyber attacks, in Georgia, as previously mentioned but also in Ukraine in 2014 (Valeriano and Maness, 2015: 147; Eder-Neuhauser et al, 2017: 11).

6.4 Summary:

Russia has continued to operate under what Mastriano termed a 'strategy of ambiguity' (2017: 71-73). The strategy is based on using subversive tactics in order to achieve foreign policy aims. The ambiguity and anonymity that cyber affords perpetrators gives states like Russia an opportunity to conduct foreign policy in a way that was inconceivable twenty years ago. While more traditional military operations are still condemned, and bring with them the cost of economic sanctions and military retaliation, Russia has been able to use cyber attacks to continually influence states around it that might pose a threat. The lack of clear attribution to the Russian government regarding the Estonian case is the perfect example of a strategy that works well in creating discord and sowing ambiguity. This type of strategy also creates risks that were not considered by the Russian government in the lead up to its implementation. It is still unclear where the threshold lies for cyber attacks qualifying as an act of war. If Russia continues to use this strategy effectively, problems may arise through implementation or through the creation of cyber attacks that its strategy cannot cope with. The reliance on anonymity and ambiguity with regards to cyber attacks in this particular instance protects the perpetrator but should attribution be determined; it is still unclear how states would react. The 'success' of the Estonian cyber attack brought with it a template for future attacks including against Georgia in 2008.

The Estonian cyber attack presents a further case in which war was not declared, though the term was used, as a result of the use of a cyber weapon. This case however presents an insight into the different dynamics that restrain states from acting in certain ways. It also examines a method of cyber attack that unlike Stuxnet has no particular kinetic properties built into its code. What this chapter has indicated is that this type of attack can still cause significant social, psychological, economic and political damage to a state and therefore might be grounds for

retaliating with military force under certain conditions. The intention of the Russian state was clearly to collude with nationalist forces within and outside of the borders to systemically undermine the Estonian government and its media and banking systems. Furthermore, this plan afforded the Russian government a degree of power over the Estonian state. The attempt was successful in large part due to the abilities of hackers to use simple tools to bring down Estonian websites and slow web traffic in and out of the country. The attack also cemented the belief within Estonia that the state is a target for cyber attacks and possibly deepened the fear of their former imperial overlord and its intentions.

We have examined the impact that this had on NATO and the response that both it and the Estonian government took to address the situation. It is clear from interviews and academic sources that the Estonian government felt that there were grounds for responding with military force to an attack they deemed a violation of their sovereignty (Lucas, 2017: 117; Rid, 2013: 7; Shackelford, 2009: 194). The state was constrained however by its allies in NATO and the EU to maintain peace with Russia and was placated with a number of initiatives that continue to operate to secure Estonia's cyber defences. In conclusion the decisions made by all parties in this case allowed for a major cyber attack to occur without military reaction to it. If Estonia had invoked Article 4, it is not clear that NATO would have responded. However, it is clear that they felt so aggrieved that they believed it necessary to meet with other member states. One could reasonably conclude that without constraining factors, Estonia may have chosen to react with escalation towards Russia. Following from this we shall move forward with the two empirical cases related in the previous two chapters and consider hypothetical cases which recreate some of the elements of the types of cyber attacks outlined but with differences that could be material to their outcome. This will allow us to further analyse the calculations that states are forced to make when threatened or attacked with these types of weapons or when considering deploying them.

Chapter 7 Hypothetical cases

In this chapter, we will consider a number of hypothetical scenarios that expand on some of the problems surrounding cyber security as laid out in the previous two case studies. What we have seen in the previous two chapters is the normalisation of cyber as a means of conducting foreign policy. There are still few precedents for cyber attacks and considerable scope for misunderstandings between states regarding their interpretation. Up to now, retaliation for cyber attacks has been marked by restraint rather than escalation. Presumption of the continuation of such restraint limits the range of expected responses considered by aggressor states. It is dangerous to rely on a supposed established norm that cyber attacks will provoke only verbal or cyber responses. In this chapter, we will critically analyse this assumption and consider circumstances and situations where it might break down. Key to this chapter is the idea that the attacked state has the capacity to determine how a cyber attack will be interpreted and that this may diverge from the intentions of an attacker. This might include considering an attack to have crossed the threshold for being an act of war, potentially meriting a conventional military response. As chapter six alluded to, there may be an assumption that cyber-only attacks can only be responded to in non-violent ways. But this assumption may not be as secure as some imagine. It is contingent on how a victim state interprets the attack and its prudential calculation as to whether it would gain from a military response.

Clarke and Knake (2012) posit a hypothetical case in their work, but consider the US and China as the main actors that are likely to go to war in the situation. In our scenarios, we will deal with imaginary hypothetical states as this proves a better means of drawing out the conceptual issues and possibilities, without the baggage of specific states or historical cases, though we may refer to some historical cases.

In the scenarios presented here, we refer to State A and State B. We shall assume that these states are not nuclear powers, because of the strong deterrent effect this has on military escalation under any circumstances. This may have influenced the Iranian decision not to go to war with the US or Israel and would have impacted NATO's response regarding the Estonian cyber attack. Both State A and State B are assumed to be of similar size and have a similar level of power in the international sphere. Critically, however, neither are superpowers. In these hypotheticals, we shall take into account that other states might have an influence on the decision-making process but the key actors in this scenario are the two states themselves rather than their allies. We will use State A as the aggressor and instigator in the conflict.

7.1 Action Phase

7.1.1 Intentions:

As in the previous two chapters, we examine the intentions of State A, considering its decision-making and the context of its relationship with State B. For this hypothetical case study, State A is the intentional actor and State B is the state that is acted upon. As with the previous two cases, it is useful to understand the context of the interaction between the two states as a means for explaining why State A would undertake a cyber attack. A common thread among the cases is the desire to exert power or control over another state to force it into compliance with the aggressor's wishes. Such action can take a number of different forms. We examined the use of force to coerce states in the chapter focusing on acts of war but have also noted that 'softer' uses of power can be used to influence behaviour (Nye, 2004).

In previous chapters we examined the factors that shape intention. One set of factors is political, both internal and external forces such as domestic pressure groups and foreign allies. Second, the financial or resource pressures may shape the options for action considered viable. A third

factor is public opinion, which may be distinct from organised political pressure. This can be more important in some states than in others. In the previous two cases, we have seen how different factors weigh more on some actions than others: Stuxnet was more heavily influenced by organised pressure from domestic lobbies and foreign actors rather than mass public opinion, whereas one could argue that the Estonian case was heavily influenced by public opinion. In this section, we can hypothesise scenarios where State A might be influenced by these factors. After this, we shall turn to expectations, which are informed by relationship context and by precedent regarding the outcomes of previous uses of similar actions.

Suppose State A intends to act against State B in response to some policy move of B's. This is probably because B's policy presents a perceived threat, of some kind, to A's security and A wishes to negate that somehow. This is a common element in the two cases discussed previously. In the case of Stuxnet, the worm was designed to mitigate the advance of a nuclear weapons programme. In the Estonian case, the perceived threat was an attack upon the identity narrative of ethnic Russians living in Estonia; also, a broader threat to the encroachment of the EU and NATO to Russian borders. As a result of this, we can argue that 'perceived threat' is an important indicator for intention and can drive the policy agenda.

We have previously noted the influence of both domestic and foreign actors on policy creation in these circumstances. In examining Stuxnet, it was clear that Israel and Saudi Arabia had a large part to play in influencing the US decision to act. Russia faced pressure from both domestic groups and interest groups within the Duma. In both cases, one could argue, there was a risk to the prestige of the state. On the one hand, the US was facing uncertainty regarding its continuing operations in the Middle East region. On the other hand, Russia, following the breakup of the USSR in the 1990s and the economic and political instability of Russia in the decade after, the Putin regime has consistently sought to increase its prestige and influence abroad. Both the US

and Russia wanted to maintain dominance, or the appearance of it, in the relevant region, but the state against which they acted seemed to threaten that. In this sense, when examining policymakers' possible actions, it is vital to consider the desire to defend states' prestige as a factor of intentions.

The desire for defence or expansion of a state's position in wealth or power should not be underestimated. In choosing to go to war, a state is implicitly calculating that there is something worthwhile to be gained by doing so (Mearsheimer, 2003: 148-149). We have previously argued that Stuxnet was used to avoid another costly war following the expensive campaign in Iraq. This shows how financial cost can be a limiting factor for states as they decide which means to utilise when conducting foreign policy, Moran (2009: 114) argues that there is a selling point for cyber attacks over conventional military ones, the desire to own or access resources may be an influencing factor in deciding to pursue a certain course of action. But resource considerations can also have the opposite effect, arresting any action for which a state does not have the resources to embark. If Iran does not have the material resources to train and outfit a military force that could combat the US, full-blown war is not a realistic option for its decision-makers. Likewise, if the state is limited in its material resources and cannot recoup those costs via a conflict, this counts against undertaking it. However, states may choose to disregard their material resources and embark upon a decision regardless of cost. Even though we can find cases that these considerations do not fit, material gain is a critical element in the decision-making process. shaping both intentions and expectations of any decision to act against another state.

This is in line with this study's assumption that states are generally attempting to be rational, even if they may not always succeed. Cyber attacks have appeal to decision-makers as a way to elicit an outcome from the world that they consider important. Also, as indicated above, to avoid

the costs and risks associated with war. Nevertheless, such rational calculations may prove flawed. If they have misjudged confidence that the cyber measures they take do not carry any risk of triggering a response that escalates to conventional military conflict. States may rationally undertake an action with the intention of producing the desired outcome at an acceptable cost, but they may still produce unintended consequences if their expectations are faulty, as to the spectrum of plausible reactions they are risking.

7.1.2 Expectations:

One can hypothesize three possible ways in which a state might mount a cyber attack in service of such intentions: with plausible deniability; with actual anonymity; or with the expectation of being definitively blamed for the attack. Thomas Rid (2013) notes that current cyber attacks fall within the realm of espionage, sabotage or subversion, all of which imply states seeking the maximum level of anonymity or deflection of blame.

The method of cyber attack contemplated by State A in a hypothetical scenario would be influenced by the degree of unattributable secrecy sought, the level of control they wish to exercise over the attack once initiated, and the extent of the damage intended. There is a level of predictability with cyber attacks. DDoS attacks, for example, have a limited number of uses and their results can be predicted to a certain degree[25]. Worm-like malware can be more precise and damaging however as in the case of Stuxnet, but there is some degree of unknown surrounding how the worm may act in the wild. The decision-makers in State A then have to consider the risk of using a cyber attack to achieve their intended limited consequences. A Trojan Horse would allow State A to do a myriad of nefarious actions to State B's computer network. Nonethless, State A relies heavily on poor cyber security on the part of State B as well as being installed

[25] Although one could argue that their use has been self-limited as the 'Largest DDoS attack was 1.2tb/s which is below estimated potential of 108.49tb/s' (Leverett and Kalplan, 2017)

directly on to the machine, presumably inadvertently. Ransomware presents another useful but difficult to manage form of malware that might be used in a cyber attack. For example, the NHS in Britain, as well as a large number of other private companies and state-run enterprises, were attacked in a global cyber attack in April 2017 (McKenna, 2017). The attack was effective in that it encrypted files rendering a large number of computers useless in a matter of hours. However, a state might be deterred from using this type of attack by the relative speed of recovery after the 2017 cyber attack.

For the purposes of these hypotheticals, it is useful to imagine State A would use a blueprint of several previous inter-state cyber attacks to formulate its own effective cyber weapon. Through combining a number of different attributes of cyber attacks, State A can expect that it would be able to effectively counter some of the measures that have been put in place as a result of, for example, Stuxnet. State A might use a mass-email system with a trojan attached in a Microsoft Word document or PDF. Based on the ransomware attacks of 2017, this is arguably a good tactic. State A might choose to target companies that are critical to State B's infrastructure as a means for implementing the attack. This would mirror Stuxnet's approach. By attacking Foolad and other industrial companies attached to Natanz, Stuxnet's infiltration into the facility was more likely. This approach would be most likely if State B has mandated an air gap between critical infrastructure, such as power plants and the wider internet.

A third hypothetical would build on the experience of the 2008 hacking of the Pentagon's secure network. An infected USB was plugged into a secure terminal in the Middle East, from where the worm quickly spread throughout the network: the resultant cleaning of the network took nearly fourteen months to complete (Shachtman, 2008; 2010). USB security is generally poor and thus there are opportunities for states to take advantage of this when utilising cyber attacks. Finally, State A might choose to use human operators either within State B or from State A to infiltrate

the target directly and place the cyber attack on the network. This would be more in line with traditional sabotage methods, but of course comes with the risk of human error and increases the risk of attribution. Using a mixture of these techniques for infiltration might serve State A well when considering an attack method.

Let's imagine three possible scenarios, hinging on different expectations regarding attribution, which in turn shape expectations regarding response.

Scenario 1:

In the first scenario, State A uses a cyber attack in the belief that they can plausibly deny involvement. State A's confidence that the cyber attack cannot be definitively attributed is important here. This means that State A is willing to take the risk on using a cyber attack that may be linked to it by inference from political motives, economic motives or through the coding of the weapon itself. Stuxnet had some of these elements, but the Russian cyber attack on Estonia was a closer fit. The aim here is not to ensure that State A remains blameless, but to put the burden of proof on State B. State A is relying on two assumptions: firstly, that State B will not be able to adequately prove that State A was the culprit; and secondly, that even though State B will suspect State A, their lack of concrete proof will restrain State B from deciding to escalate the conflict. In this example, State A could use a cyber attack similar to that in the Estonian case, as DDoS attacks may be harder to attribute (Klimburg, 2011: 42). In this scenario State A might be suspected of involvement, but they expect that State B will only react in a restrained way, using non-violent means. Such an expectation relies on the premise that a cyber attack could not ordinarily be construed as an act of war compounded by lack of definitive proof of origin for the attack. In this scenario, State A's expectations are that State B will show

restraint when considering a reaction, in a continuation of the trend toward restraint in the cyber sphere observed by Valeriano and Maness (2015).

Scenario 2:

In the second scenario, State A expects that the cyber attack will remain completely anonymous for the foreseeable future. This may seem optimistic given the cases we know of cyber attacks revealed or strongly suspected, but the discovery of some infiltrations of systems only a considerable period after they began is suggestive of the possibility that other such operations may go entirely undetected. In the case of Stuxnet, the American government did not expect for the attack to become public knowledge, and therefore was under-prepared for the release of information through Sanger's investigative work. Despite this, there was evidence of some planning for such an eventuality: the US government met regularly with international law specialists to determine what the consequences of such an outcome might be (Sanger, 2012: 193; Gibney, 2016). Based on Sanger's account, it could be argued that even a well-funded and militarily sophisticated state would be likely to take precautions when using cyber attacks, for fear of unintended disclosure. Also, one could argue that Stuxnet was limited in its effects by design, not because it was expected to become public knowledge, but because it was acknowledged that this risk could not be eliminated or ignored.

Valeriano and Maness (2016) emphasise restraint in the cyber realm. Their argument centres on the restraint of the state that has been attacked but we could apply it to aggressors also. It is apparent that large-scale state sponsored cyber attacks have taken place, though it can be difficult in certain circumstances, the occurrence of the attack can at least often be discerned through investigative analysis and from there culprits plausibly deduced. If anonymity cannot be assured, State A might have to rely on traditional means of deterrence to avoid a conflict with State B upon the discovery of the attack. There may have been cyber attacks of which we are

unaware, that have done damage comparable to the testing done at the Idaho National Laboratory in 2007 or to the Russian cyber attacks that are targeting power grids in Ukraine (Lindsay, 2013: 373; Greenberg, 2017). In this case, State A might be able to pursue a policy of cyber intrusion with impunity. However, it is unclear what norms governing such attacks should be. The restraint referred to previously seems to imply that some tacit understandings by which states govern themselves regarding responding to cyber attacks. The avoidance of cross-domain escalation might point to the normalisation of cyber attacks as existing only within the 'cyber realm' and, therefore, as meriting response only within that realm. This 'norm' if this is what it is, however, has not faced robust testing yet.

Scenario 3:

The final scenario posits that State A choses to act in the full expectation that the cyber attack will be both detected and attributed to them. In the case of State A deploying a cyber attack with a high likelihood of loss of life or severe damage to infrastructure or the economy of State B, this would likely apply. It is possible that in such a scenario State A would deliberately intend war, and its cyber attack might be accompanied by a traditional military strike. One can imagine a circumstance, however, where the attacking state believes that because its attack took an exclusively cyber form, that it should not expect any conventional military response unless it initiates further escalation in that domain.

A potential scenario would be the use of a worm to infiltrate the electrical grid of State B. In 2013, 59% of cyber attacks were targeted against the energy sector (ICS-CERT, 2013: 1-2). Hitherto, such attacks have never sought to unleash substantial destruction but as a technological matter they could well be much more destructive in the future if their designers so wished.

A decision to launch an attack such as this, would be related to a clear threat and urgent pressure to confront and neutralise it. The language that surrounded the Iraq War in 2003 was justified in pre-emptive terms, i.e. that it was known that US actions might be accused of aggression, but those actions were necessary because of a perceived threat. Often in international relations, the aim is to induce a state to change its policy. The threat, as well as the actual use of force, may prove useful to achieve this outcome. Similarly, the threat or use of force through cyber might be enough to cripple a state into conceding to the policy change that the aggressor is demanding. This may avoid war, as the victim state relents rather than escalating to a potentially even more costly conflict. In either case, the aggressor, State A should be prepared to deal with a potential military retaliation for the attack, since neither their intentions nor their responsibility has even the shield of plausible deniability. While there is not yet precedent for cyber attacks being wielded in this way; or being responded to with conventional force, and this may share the expectations of states regarding future cases, this may represent a failure of imagination, and potentially a consequential one.

7.2 The attack:

The timing of the attack was critical in both of the previous cases: Stuxnet was released, during a crucial period in the advance of the Iranian nuclear programme and coinciding with the announcement of the re-election of President Ahmadinejad; Estonia's cyber attack began in response to the public controversy surrounding the moving of the Bronze Soldier. In both cases there was a trigger for the release of the respective cyber weapon and therefore we could argue that the highest-profile cyber attacks between states have been reactive in nature. There is evidence that states are developing and refining this technology, however, in a way that would enable more severe aggressive first strikes against key infrastructure e.g. take down a power grid (Greenberg, 2017). This kind of capability could bring cyber attacks closer to a

Clausewitzian idea of force and war, i.e. something that can be used to compel or coerce an opponent through either its use or threat of it[26]. This desired outcome of coercively reorienting another state's policy would separate state-executed cyber attacks from those carried out by criminal private hackers, even though they might use some of the same technologies.

In this hypothetical case, let us posit a case whereby an electrical power plant is targeted. It is interesting to consider this because it represents a foreseeable further development in cyber attacks that may be on the cusp of becoming mainstream. Since 2015, Ukraine has suffered heavily from power outages as a result of Russian cyber attacks (Greenberg, 2017). The power outages typically only last a few hours, but the fact that such feats have been accomplished with the technology currently available shows the potential damage that could be done with a cyber attack as capabilities evolve.

The type of cyber attack deployed by Russia against Ukraine are difficult to specify with certainty, though they illustrate that despite a highly developed security net, it is still possible to be attacked (Sullivan and Kamensky, 2017: 35) Little definite official information has been forthcoming in various reports on the wide number of perfectly timed blackouts that have occurred in the region. Ukrainian power plants have been hit with ransomware in several attacks but this has not directly affected power output (Dearden, 2017). This Russian attack on Ukraine reportedly utilised a Trojan – a programme that disguises itself as something benign but, in fact, hides more nefarious attributes. The Trojan, in this case, software known as Black Energy 3, combined with the open source hard-drive eraser KillDisk, served as the main culprit in the attack (Finkle, 2016). What made this cyber attack so unique is that it used a multilayer approach to damaging systems. The Trojan was disguised originally within an Excel file but

[26] To reconcile this within a covert use of cyber attacks, states can use proxies to imply rather than implicate involvement at the state level. State B does not necessarily have to be aware that the cyber attack comes from State A in order to fulfill the conditions set out by Clausewitz.

found success in this case within a Microsoft Word document. The group behind the attack has been unofficially named 'Black Energy APT' by leading cyber security agency Kaspersky Lab. However, the attack has been linked to Russia, as the means and organisation are considered somewhat beyond that of average black hat hackers (Kaspersky, 2018;Finkle, 2016). US sources have claimed that the attack originated from the Russian hacking group Sandworm, based on a thorough analysis of the Trojan (Finkle, 2016).

While Stuxnet and the Estonian case provide some early insight into the types of cyber attacks available, the 2015 cyber attack on Ukrainian power plants suggested new forms of attack evolving. The Black Energy attack featured two aspects of cyber attacks that we had seen before, but this time combined. Black Energy, like Stuxnet, was designed to take advantage of loose security surrounding SCADA systems, however, it used DDoS-like operationality to ensure that it spread quickly and effectively. Any time SCADA systems are attacked there is some risk of damage and fatalities (Webber et al, 2012: 421). Unlike Stuxnet, it appears as though Black Energy was human operated throughout the hacking process introducing a new dimension into the unfolding of an attack over time (Zetter, 2016).

In order to posit a hypothetical cyber attack it is useful to draw on some elements from the examples laid out thus far. A power plant typically relies on a number of steam generators to develop electricity. The steam pressure is closely controlled to prevent damage to the turbines but also to the general infrastructure. In a manner similar to Stuxnet, it would be possible, in principle, for a worm to infect the critical systems of a power plant and change the normal operating parameters of the plant. This could involve changing the pressure threshold to outside of safe parameters. Under this pressure the turbine might break through stress, or steam build up to such an extent that it releases in a damaging explosive form. Alternatively, one could focus, as Black Energy did, on shutting down substations. Just 30 substations were enough

to limit electricity to nearly 230,000 homes in Ukraine for between 1-6 hours (Zetter, 2016). Attacking substations provides a different approach that may have been more effective than merely attacking one power plant. Substations are responsible for energy distribution, thus even with the rerouting of power from other sources to compensate for a disrupted plant, without the ability to distribute the power, this becomes a very effective attack. A combination attack of damaging both substations and turbines could cause significant damage and would potentially be very difficult to respond to effectively. Therefore, we might plausibly hypothesise a scenario where State A utilised an attack of this kind, combining several different types of cyber attack in order to effectively shut down the power grid of State B for a period of time.

The duration of such an effect represents the most dangerous variable of the cyber attack. The Black Energy attack was limited, and arguably this was due to human control. One could reasonably infer that the attack was less about the damage that it might cause, and more of a proof of concept: it is now clear that the Russian government has the ability to severely limit power supplies in ways that were previously only speculative. Attacking a power grid might be an effective means of coercing the state that has been attacked. But it also represents a significant shift beyond typical sabotage attacks that Rid (2013) mentions in his work. Sabotage incurs a limited amount of damage and is not typically considered an act of war. But an attack such as that envisaged here might have the same effect as a series of bombs on electrical substations. Rid might counter this argument with the precedent of the Ukrainian case since the power was only switched off for six hours in the worst case and therefore hardly represented a significant enough threat to be considered an act of war. Rid might be correct on this specific case, but it is worth contemplating the potential for unintended consequences in the outcome of any sabotage attempt. Several risks occur in this regard.

Firstly, one could hypothesise that the attack might be poorly coded. We have seen this within the Stuxnet case, the attack was never designed to deal with access to the wider internet. If a future attack did not have an end date built in, then unless a patch is released and installed, a cyber weapon might maintain potency for an extended period of time. The low cost of cyber attacks makes them attractive means for states to employ against their competitors and enemies (Slayton, 2016: 77). However, this can also make them susceptible to weakness in coding, if the operators attempt to design or execute attacks on the cheap. Furthermore, the attackers might choose to limit the amount of human interaction needed in order to further save on costs. Automation has its benefits in this regard: one can deploy a cyber weapon and expect it to do the job designed for. This limits options down the line, however, if unforeseen circumstances arise. For example, if the Ukrainian cyber attack had been purely automated, there might not have been safeguards to ensure that the timings of the substation shutoff would be limited to a maximum of six hours. Attempts by Ukrainian authorities to re-establish substation control might have failed, leaving 230,000 people without access to electricity indefinitely.

It is important not to understate the importance of restraint on the part of the attacker in terms of duration. Had Russia continued with its Estonia attack for longer, it is possible that there would have been considerably more damage done, resulting in a significantly different interpretation of the act by Estonia and NATO. The choosing of the target is also critical, allowing the opportunity to do enough damage to demand attention, while at the same time limiting harm to avoid incentivising escalation on the part of the victim state. In addition, there is a reliance on the ability of the creators of a cyber attack to ensure that there are no unintended consequences that might mean further damage is done that encourages escalation.

Even with a human element, there is significant scope for poor decision-making on the part of the operators. There are still poor command and control structures within elements of the US armed forces, for example, and due to a lack of transparency in the decision-making process, it is not always clear who should take the lead on specific decisions when it comes to cyber issues (Cavaiola, Gompert and Libicki, 2015: 83). This creates a problem if unintended effects are discovered by the cyber attack that are either outside of the control of the operator, or within the control but it is unclear from whom they should be receiving orders. Much like the length of time sanctions or occupation are deployed as a means of coercion, the amount of time that a state uses a cyber attack can determine the outcome. The hypothetical here prompts us to consider: how long would a cyber attack that denied electricity to all or substantial part of a state need to persist before the interpretation of the attacked state shifted from treating it as the limited virtual assault that cyber attacks have been seen as thus far, to be an act of war?

7.3 Reception Phase

7.3.1 Interpretation:

The interpretation of State B is crucial to considering how this scenario would play out. Much of this interpretation is built on the contextualisation of the relationship between States A and B. In this section, we will examine some different scenarios to better understand the development of interpretation. In considering these scenarios, it is important to note the societal significance and value that State B attributes to certain things, and how State A might misjudge or misperceive this.

There is often a non-trivial gap between two states when it comes to expectations, interpretations and eventual outcome due to the different national narratives and societal values to which they adhere. This can influence the choice of targets based on some significant

societal value they might hold for the state and its citizens. For example, one could imagine the ransomware cyber attack that hit the NHS in 2017 having a political motivation behind it. The NHS is a societal institution as much as it is a medical one, its decision-making with regards to spending constantly scrutinised by policy-makers and citizens. Had the cyber attack infected a non-critical government sector, then the fallout and resultant public backlash might not have been as strong. Thus, while a hypothetical cyber attack on the NHS and one on the Department of Media, Society and Sport, both conducted by a state, might be seen, to an outsider as equivalent in damage and output, the former would carry a much higher risk of response because of the societal significance and value placed on one institution over the other. Therefore, it is worth contemplating what such a scenario would look like.

For example, suppose State B has established a negative perception of State A as a result of previous interactions. Perhaps State A is the slightly larger of the two states and dominates their shared region of milieu, while State B has consistently opted to remain more economically and politically isolated. While State A has continued to improve its relations with other states in the region, State B has been more cautious in its approach and has suffered from being late to negotiate for trade deals. The success of State A's engagement with the region might stand in stark contrast to State B's insular nature. As a result, State A might have managed to garner significantly more prestige than State B. Having borne these costs for its policy choices and suffered, in comparison to State A, State B might decide to invest heavily in its military. This might be interpreted as a threat to the previously unchallenged dominance of State A.

Furthermore, if there are profound religious or other cultural differences between State A and State B, these could have the potential to exacerbate societal misunderstandings among the state leaders. They could also be a source of heightened tension if there is a history of conflict between the official or dominant religious or ethnic groups of the states and their national

conflicts have become tied to this deeper history. Israel and Iran would be real-world examples of this phenomenon. This context could be combined with the insular and isolationist policies of State B, posited earlier, to create greater room for misunderstanding and misinterpretation between the two states.

State B's pre-existing interpretation of State A has a profound impact on how a cyber attack would be viewed. In the Estonian case, for example, the dominant historical narrative of Estonian self-determination being hard-won, and a perennial struggle against Russian attempts to (re-)establish itself as the dominant force in the Baltic, fit neatly with the facts of the case. The historical context made it more likely that an attack that would be seen as vexing by any state in any circumstances might be interpreted as an existential challenge by Estonia.

State B's interpretation of an attack will depend in part on how it perceives (or misperceives) the intention behind it. It might sway State B away from escalating to warfare: if the intention of State A was not to provoke war. State A might have made its intentions clear prior to the cyber attack, in threat form or otherwise, allowing State B to accurately interpret its intentions. However, as noted in the AP-RP chapter: the intention of an act does not unilaterally govern how it is received. Therefore, even if State B interprets the intentions correctly, they still might be more aggrieved than the attacker anticipated and may be inclined to regard them as an act of war meriting proportionate response. Furthermore, State B has the potential to misinterpret the intentions of State A. Given the societal and political differences between the two states, this is not an unlikely situation. In the event that State B feels that it has been consistently undermined or attacked by State A's actions over an extended period, this pre-existing perception might encourage a tendency to believe the worst about intentions, including regarding unintended outcomes. A state with a strict honour society might also be prone to responding to perceived attacks on the national honour in a more violent manner than outsiders might anticipate. It is

also possible, of course, that misperception of an attacking state's intentions as more benign than they are might contribute to maintaining peace, though this is less likely.

Let's imagine three scenarios regarding the interpretation of a cyber attack.

Scenario 1:

In some cases where State B interprets the intention accurately, war is potentially thus averted. State A wants to avoid escalatio, and chose to use a cyber attack for this reason. Thus if State A manages to convey that intention by perhaps limiting the scope of the attack, this might enable State B to overlook the fallout from the cyber attack even if there were unintended consequences that severely affected critical infrastructure. This is contingent on a number of other factors, including the nature of the relationship between the two states and the societal significance of the target. Stuxnet provides a useful example here. Iran saw Stuxnet as a hindrance but not as a deliberate provocation to war which was what was intended by US policy-makers.

Scenario 2:

In the second scenario, State B misinterprets the intention of the attacker, supposing them to be more aggressive or violent than the reality. This relates to the ideas of expectation and risk in the AP-RP framework. State A necessarily makes assumptions about how State B will perceive and interpret a cyber attack, and likely be influenced by the fact that the precedent of cyber attacks thus far has been restrained in response (Valeriano and Maness, 2015). In the case that a cyber attack does more damage, or has more severe consequences, than planned, State B might not believe that these were unintended consequences or outside of the deliberate control of

State A. Even if the damage inflicted were limited, State B might come to believe State A intended, or at least accepted the risk of inflicting, greater damage than, in fact, unfolded. Both circumstances could lead State B to react in more extreme ways than State A expected, and perhaps even escalate to war.

Scenario 3:

In the final scenario, State B interprets the attacker's intention correctly but does not consider that it resolves the question of how reaction should be contained. Sometimes the perceptions of an attacked state are impacted more by the nature and consequences of an act than by the intention that drove it. Were an electrical grid to be brought down for a month, State B might perceive this attack as having crossed a threshold where intentions were no longer a decisive factor in determining the reaction appropriate. Where a state did more damage than intended, for example, the intention to do less damage is unlikely to appease the affected state.

While there might be a legal argument about the responsibility of State A for unforeseen consequences of an attack, or whether a cyber-only attack can, de jure, bring about a state of war, the potential for an attack of sufficient severity to trigger escalations leading to the outbreak of de facto warfare seems clear.

State B attaches a higher value to a certain target than State A appreciates, this could create a misalignment of State A's expectations with eventual outcomes. In the previous chapter, we explained the unusual importance of the internet to Estonia. This can be categorised on two levels: infrastructure and society. Much of Estonian business relies on the internet to function and therefore there is a clear, high cost when that critical infrastructure is taken away even

temporarily. However, there is also a psychological element attached to the internet. Estonians are perhaps unique in their attachment to the interactivity provided by a free and secure net and the state takes unusual pride in this facet of its society. This means an attack on the internet structures of the state is liable to have an especially strong negative impact on both citizens and society, putting pressure on the state to react forcefully. Arguably the same can be said for different institutions, organisations, buildings and people in societies across the world. In Britain, the importance of the NHS meant that post-cyber-attack, more financial aid was allocated to revamping the aging systems. The societal importance of the NHS expeditated this process, whereas other sectors of government might not have received as swift a response. Thus when judging how State B would perceive an attack on its electrical grid we can ask two questions: what is the infrastructural damage, and what is the societal damage, including the knock-on damage of cost power supply to other institutions and sectors of society? This generates scope for mutual misperceptions, misinterpretations, and misestimation of the outcome of an attack and likely response to it.

The danger of unintended consequences presents a significant factor for consideration in hypotheticals. With our previous two cases, it was clear that there were some degree of unintended consequences but that this did not seriously influence the outcome of the action. The unintentional spread of Stuxnet presented a possible hazard, as the original expectations of the attack presumed the anonymity of the worm. The discovery of Stuxnet in the wild and subsequent leaking of details regarding its design and deployment could have influenced the Iranian decision to react. In the Estonian case, the Russian government could not be sure how many individuals would use the advice posted on chat forums. The scale of mass mobilisation may have been a runaway success for Russia, but it was to some degree an uncontrolled consequence that may have led to more harm than originally estimated. This is an extension of the risks involved in any effort at coercion by a state: there is no way to fully quantify with

certainty and precision the potential risks that are a contingent element of intentional action. States are aware that their actions may have unintended consequences, and these are often accounted for to some degree in the planning stage – we see clear evidence of this in Sanger's (2012) work where he relates the role of international law experts in informing the NSA/CIA operational planning of Stuxnet. Such planning occurs within certain parameters of expectation regarding known risks, however, if outcomes range beyond this situation may escalate beyond even the outside expectations of an aggressor state. For example, if State A unleashed a cyber attack on a power grid, believing its destructive potential to be limited and controllable, and then the tools deployed ran out of control, or initiated a chain of events of greater severity than planned, this could expose it to risks of retaliation beyond those considered during planning.

In the event of an unintentional spread or a cascading chain of unforeseen consequences, the damage done by a cyber attack could generate harm to people, destruction of property and value, or perhaps even loss of life that, while not equal to a major kinetic military assault, could be significant in scale. The reliance of modern states on the internet for communication could mean severe economic and social cost while a state attempted to stem the tide of attacked computers in a manner similar but worse to that of Estonia in 2007. In the case of an attack on power infrastructure, not all states have the ability to reroute their power supplies in the event of a mass power failure, some states have systems that are fragile and close to capacity even under normal circumstances. Damage to a turbine or power plant facility or distribution system might take weeks to recover by which time much of the critical infrastructure that relies on electricity might have failed. Hospitals are usually prepared for such eventualities, as long as they are of limited duration. But even small generators rely on fuel source which in turn relies on some level of communication facilitated by electricity. Current decisions to use cyber attacks rest heavily on precedent, but there is no precedent for the kind of unintended consequences

speculated upon here, which could trigger a response outside of the range of expectations and calculated risk involved in planning.

7.3.2 Reaction:

In any of these scenarios, there are a number of possible reactions available to State B i) more limited than the initial attack i.e. restrained. This might involve public statements condemning State A for the attack, and tensions heightened for an interim period, but no major escalation toward conflict. ii) a reaction that seeks to mirror the initial attack. State B might employ a similar cyber attack for example, or through the use of other means, conducts an attack on State A with proportionate impact to its own damage sustained. Depending on the nature and intention of the cyber attack, this has the potential to further damage relations between State A and State B, but full escalation into war might still be avoided depending on the initial action being mirrored. iii) a reaction that is out of proportion to the initial attack. State B choses to respond with a desire to do more damage to State A than was originally done in the first attack or which shifts the domain of attack unexpectedly. This might involve escalating the conflict to war, or using traditional military force as a response. The choice between these types of reactions are influenced by the interpretation of the initial attack but also by the same factors that influence intention: political pressure, cost-benefit analysis and public opinion.

On this basis, let us consider scenarios in which State B considers these options for reaction, where an initial cyber attack has had severe consequences, some perhaps unintended.

Scenario 1:

State B might choose to react in a restrained manner that is more limited than the initial attack. One might expect such a restrained reaction where State A has successfully managed to conduct a cyber attack with the awareness that it may not be traced back to them or that they could rely on deniability. But there may be other factors, which prevent State B from retaliating with conventional military force. In the Estonian case, the Estonian reaction was to give public statements condemning the Russian government for their involvement in the 2007 cyber attack, but they stopped short of declaring war despite feeling they had cause (Schmitt, 2010: 151-152). This was not primarily a direct result of their interpretation of the cyber attack but a consequence of the context and the considerable power differential between Estonia and Russia. Estonia relied on NATO for backing, and NATO's reaction was muted because of a prudential calculation that escalation would not be worth the risks and costs. But this was a product of Russia's military strength, and perhaps also its energy ties to Europe, not an adjudication of the legitimacy of Estonia's cause (Crandall, 2014: 30; Mattern et al, 2017: 710).

Scenario 2:

State B might choose to react by mirroring the initial attack. In a situation where State A has successfully achieved anonymity this might be difficult, though as previously discussed (Rid and Buchanan, 2014), this response relies on State B making an assessment and correctly identifying the perpetrator. This might mean engaging in some retaliatory cyber attack that would damage State A in a manner similar to the harm it inflicted on State B. To some extent, Iran may have taken this course, with the Schamoon attack against Saudi Arabia following Stuxnet, although the gap between attacks leads some experts to conclude that this was a show of cyber strength rather than a direct reprisal (Craig and Valeriano, 2016: 150). Such measures do not need escalate conflict. The US and Iran, during the late Obama administration succeeded in pursuing diplomacy to a successful deal over its nuclear programme despite the Schamoon attack. Tit-for-tat reprisals for attacks are typically expected where attribution is clear, certainly

where states have internalised the notion of restraint in cross-domain escalation (Lucas, 2018: 118-119). The general rule of thumb here, which many may have internalised as a universal one, is that a cyber attack will only attract retaliation via cyber means.

Scenario 3:

The final type of reaction that State B might employ would be to escalate in their response to the initial attack. While State A views that military response as conceivable, this might still be highly unexpected. State A might have anticipated a cyber attack as the maximal likely response, even while carrying out an attack of their own doing damage comparable to using military means. But if State B lacks the capacity for a comparable cyber effort, it might consider it legitimate to resort to what means are at its disposal, including conventional force, to exact a price for the damage inflicted upon it. Indeed, they might calculate that such a move is not only legitimate, but necessary if the alternative is to simply acquiesce without resistance to domination and threat from State A. This might be further incentivised and enforced by elite and majority public pressure within State B. State B might even undertake such a course without considering itself to be the escalating party: it might regard the initial attack by State A as representing an act of war, and its response as simply following that, even if it had not been State A's intention.

7.4 Summary:

This chapter has considered some hypothetical scenarios that states may encounter when cyber capabilities are used offensively. We have outlined some possible scenarios in which the acting State A would choose to deploy cyber capabilities to coerce others, and the intentions, expectations and calculations underlying such action. We have speculated about a potential attack, drawing attention to key issues such as the limits placed on an attack, the control retained over a cyber weapon once deployed, the significance of the duration for which an

attack persists and the danger of unintended consequences. We also highlighted the scope for misinterpretation of intentions on the part of an attacked state, or indeed the possibility of its regarding an attack more seriously than expected, even when it has correctly assessed the intentions behind it, and opting to respond with escalation and force. We also note the crucial difference between an attacked state taking a restrained course in its reaction because of prudential considerations, and it is doing so because it does not believe a forceful response on its part would be warranted and legitimate. There is a risk that if states interpret limited precedents or restrained responses without reflecting on this difference, they may be unduly complacent in assuming that cyber-only attacks risk at most a cyber response from the attacked.

Chapter 8 Conclusion

It is clear that cyber technology has the potential to destabilise our understanding of where the threshold lies for an act of war, which is problematic given that war is commonly understood as permitting or even requiring the use of traditional military force. Some forms of cyber weapon and attack clearly fall within the military sphere, but their use does not match what we would consider traditional military use of force in all respects. Yet, there are elements of cyber attacks that have the potential to cause as much harm as a traditional military strike, perhaps more. This makes it important that we consider the potential for this technology to shift prior constructed understandings of the threshold for war. This entails considering how the intentions and expectations of a state deploying cyber attacks might intersect with the interpretations and reaction of a state thus attacked, to produce escalation from cyber measures to the use of conventional force.

The first chapter discusses the meaning of war and its potentially contestable elements. It also notes the erosion of war as a formally legally declared state, and the frequency with which war is today a *de facto* state or activity that may exist without formal recognition. The United States, for example has not officially declared war since 1945, despite participating in numerous *de facto* wars. This renders the occurrence of an 'act of war' as in great part, a matter of perception and response rather than declaration by the initial actor. The opening chapter discussed some conventionally accepted causes for war, which centre on violence against persons or items of value, violations of sovereignty and clashes of ideology, with the precise substance of these categories evolving. Escalation is an important concept in the outbreak of war and in this thesis. The argument here is that escalation can occur when there is a misalignment of the initial calculation behind an action, the interpretation of that action by another state, and then a reaction that reflects this miscalculation by one or both parties.

Cyber attacks as a means for achieving foreign policy are becoming more common and therefore worthy of serious consideration as a potential means and source of conflict. The third chapter of this thesis examines the various methods of conducting cyber attacks and their capabilities. We look at how states are increasingly incorporating cyber capabilities, offensive and defensive, into their military apparatus indicating a shift towards treating these tools as weapons of war. We noted the prominent argument of Thomas Rid (2012 and 2013) that 'cyber war will not take place'. Based on the evolution of technology and analysis presented in this thesis, it is my contention that Rid is more confident than is warranted that cross-domain escalation from cyber to the use of conventional military force won't occur. Rid's arguments do not explain all of the reasons why cyber war has not yet occurred. In this chapter we dealt with some practical challenges to cyber attacks, such as attribution and deterrence, important concepts to understand when examining the case studies presented later in the thesis. Anonymity plays a critical role in the decision of states to use cyber attacks as a means of conducting foreign policy and therefore is important to our understanding how and why states choose methods. Finally, this chapter discussed the potential for unintended consequences, which can play an important role in leading to misinterpretation, miscalculation and escalation.

In chapter 4, we set out a framework for analysis of cyber attacks called 'Action Phase, Reception Phase'. The study of the action phase involves understanding the processes and influences that went into a decision to attack. One key element of this is discerning intention including what motivates the action in question. Important factors in shaping intentions in this case are: political pressure from domestic and foreign actors, prospects for gain or cost, and public opinion. These factors can be seen at work in the cases studied in this thesis.

Calculation also involves expectation on the part of an attacking state regarding the range of outcomes they consider plausible in response, and the spread of likelihood within these. Consequently, they may discount some possibilities heavily or entirely rather than including them among the risks they believe themselves to be running. Examining expectations of this sort requires understanding the context of relations between the relevant states and their assumptions regarding the norms governing their interactions in the cyber and other realms. Expectations of this sort may lead a state to rule out, or heavily discount, the possibility that an act on its part will be received as an act of war. But their confidence in this may not always be supported by an accurate assessment of the interpretation place on its actions by the state against which it acts, or its ultimate response. Overconfident and misguided expectations of this kind can therefore be a major source of miscalculation. The appeal of cyber attacks in recent years has been that they are believed to entail only limited risk in terms of retaliation, and this has been supported by some precedent for restraint. But this thesis argues that this may be a dangerous expectation based on limited and quite contingent examples thus far.

The root of miscalculation lies in misalignment between the intentions and expectations of an attacking state and the interpretation of the state on the receiving end of its actions. This makes this interpretation the next important stage in analysing the dynamic. The next section of the thesis discusses the basis for such interpretations, noting in particular the wider context of the attack in terms of states' relationship and pressures upon the victim state, as well as the specific value that it places upon the target of the attack. In both cases, there is scope for divergence between the attacking state's suppositions in this regard and the perceptions of the state attacked. Failure to accurately appreciate the other side's reading of the context, or its attribution of unusually high societal or political value to certain targets (such as a nuclear technology programme, or a world-leading internet infrastructure) could lead to incorrect expectations as to how an attack will be interpreted and, therefore, in how it is responded to.

This chapter further elaborated on the different types of interpretation that are relevant. It highlighted specifically the interpretation of intention, and the interpretation of the outcome. The misalignment of intention and interpretation occurs when the state that has been attacked believes that the intention was to do more harm than was in fact intended. The misalignment of interpretations or outcome comes when an attacking state's intentions are understood accurately, but there is a misestimation as to the strength of feeling to which an attack will give rise, and therefore of the potential severity of the response to it. In such cases, aggravating factors might be unintended consequences from an attack or cultural, religious or ideological differences between societies that lead them to value different things highly. Such misalignments of interpretation can set the stage for a reaction that falls outside the expectations of the state instigating an attack.

The misalignment of particular importance to the analysis of this thesis is where an attacked state might believe that the actions against it cross the threshold to constitute an act of war, warranting and legitimating a response using conventional military force should the victim state will it. This is something explored here particularly in Chapter 7, which considers hypothetical future scenarios. This thesis argues that although what precedent there is in cases such as Stuxnet and Estonia suggest that cyber attacks do not cross the threshold to trigger war, this is more contingent and less principled than some may suppose. In the cases of both Iran and Estonia, the choices to respond with restraint and not escalate were more the product of prudential calculations, led by power considerations and in Estonia's case the views of allies, rather than a principled view that a cyber attack could not constitute an act of war. The thesis classifies the kinds of reaction available as: restrained reactions; proportionate reactions; and escalatory reactions. In choosing between them, prudence may often incentivise restraint or response to cyber attacked only via cyber means. But there is no inherent reason why this

should be so, if an attacked state has reason to favour other means (such as lack of capacity), or if it does not face a strong deterrent in conventional force terms.

Will a cyber attack ever be an act of war? Conceptions of what defines an act of war are subject to change over time. When we consider the novel nature of cyber attacks and their potential capabilities, it is apparent some aspects of cyber have already become militarised and therefore part of the infrastructure and discourse of war indirectly. There is an underlying lack of clarity over what 'cyber 'attacks are which has made it trickier to say in any blanket sense that they do or do not fall within the sphere of war (Futter, 2018: 208). Just as most societies have moved away from considering insults to the sovereign as grounds for going to war, conceptualisations of what constitutes an act of war and war itself might shift to incorporate cyber attacks as a legitimate grounds for conventional military retaliation. As we have discussed here, war has changed throughout the past century. Technology has meant that the kinetic aspect of war is considerably easier to accomplish than it was previously. The increase in military use of cyber attacks to conduct foreign policy may demand conceptualising cyber within this frame, especially given the potential of cyber-only attacks to bring about outcomes, and levels of harm, comparable to kinetic military operations.

All this means that, while it is not inevitable that a cyber attack will one day serve as the act that provides a war, we should accept intellectually that it is possible and prepare and plan with this in mind. The evidence on cyber attacks indicates that the intensity and yield of attacks is steadily increasing. Cyber attacks are becoming increasingly complex, this provides a benefit to the attacker as they can potentially attack targets with precision and avoid other systems. Alongside this, evidence suggests that cyber attacks are becoming easier to produce; they are

low cost both in creation and deployment relatively speaking[27]. Furthermore, cyber attacks typically provide a level of deniability for the attacker. On the basis of precedent, there might appear to be few drawbacks to their utilisation even when the attacker has been identified. If an assumption of restraint on the part of the attacked has been normalised into the discourse surrounding cyber attacks then states may be tempted to act even more boldly on the basis of anonymity and this restraint.

Their low cost means cyber attacks are potentially more financially viable even for resource-constrained states and there seems to be little risk of military retaliation as the responses thus far have remained within the cyber sphere or have even been in effect 'non-reactions'[28]. The relative ease of deployment when compared to the logistics of organising a military strike as well as the semi-autonomous nature of cyber attacks means that these types of attacks have some advantages over traditional military means. Therefore running a cyber operation is a viable option for states that cannot afford to further invest in traditional military apparatus even if there is the potential to rely on code that has previously been used (Smeets, 2018: 9).

All these advantages increase the likelihood for the selection of a cyber attack. There are significant drawbacks and risks, however. While cyber attacks *can* be more accurate in their precision and target choice, there is still significant scope for unintended consequences. Stuxnet was designed to only impact on Iranian nuclear centrifuge systems, but there were many cases of personal computers being affected by the worm[29].

[27] Ksherti (2014) make this point in relation to the asymmetry between US and North Korea

[28] Though states are beginning to spend more on cyber. Obama looked for $19billion for cybersecurity towards the end of his presidency (Abdollah, 2016).

[29] Several authors encourage further integration of public and private sectors with a view to increasing security: (Galinec et al, 2017: 285; Clinton, 2015; Carr, 2016; Zrahia, 2018; Chaudhary, Jordan, Salomone and Baxter 2018)

Cyber attacks can be later used as blueprints to form counter attacks against the initial attacker or against other states. There are problems with command and control regarding 'fire and forget' cyber attacks. We have noted the unintended consequences of Stuxnet but the Estonian case also serves as a warning in this regard. There is no way to completely control the ultimate level of damage wrought by a cyber attack that has been effectively subcontracted to diffuse networks of private individuals, and even with safeguards in place, an attack such as Stuxnet can cause irreparable damage to systems. We have noted the perceived low risk nature of cyber attacks as being an advantage. However it can also be considered to be one of its biggest weaknesses.

Cyber attacks currently rely on the normalisation of restraint. The users of these kinds of attack depend on that, supposing few serious negative consequences for their actions. The danger in this assumption is that it tempts complacency and miscalculation on the part of the attacker. As indicated in the previous chapter discussing hypotheticals, it is not clear how a state would respond if a cyber attack were severe enough to inflict damage similar to that of a conventional military strike. As the number of cyber attacks continue to rise, it seems plausible that the limits of this new technology will continue to be pushed, leading states to take bigger and bigger risks. They will do so in a way that is calculated, believing themselves to have taken into account the risks. But deciding whether a cyber attack crosses the threshold for provoking war is not something the initial actor gets to decide unilaterally. Though it might not be their intention, and might confound their expectation, the risk is real that any attempt to coerce another state via cyber measures could lead to unintended consequences and unintended escalation.

Policy makers need to be aware that while the global society treats cybersecurity as a public good, there is little regulation and this has the potential to lead to further conflict as states contest the space (Weber, 2017: 181). Moving forward it is likely that we will see further

attempts to restrict state actions in cyber space. States have previously engaged in restraint internally but there are limits to which this can be applied externally. For example, China might internally restrict cyber attacks on the US but is still limited when allies such as North Korea wish to use cyber attacks (Siers, 2015: 8-9, Sharp, 2017). What may be necessary moving forward is some form of international convention where a set of rules for cyber attacks is agreed (Gervais, 2012: 97; Stadnik, 2017; Radu, 2013; Hansel et al, 2018: 56; Azmi, Tibben and Win 2018; Eilstrup-Sangiovanni 2017).

It is possible that the increasing frequency of cyber attacks, and therefore in opportunities for dealing with them may in fact further embed the tendency towards restraint. Sheer frequency might imbue some degree of normalisation among states conducting these types of attacks. However, it is important to note that the nature of cyber weapons changes with each attack, as defences are shored up against prior incursions. Therefore cyber weapons will have to continue to become more intense in the nature of their attack, and also more complex and sophisticated. An increase in complexity and sophistication may increase the risk of unintended consequences open to misinterpretation by the state affected. This, combined with the increase in the number of occasions for miscalculation, leads us to conclude that the risk of a cyber attack being interpreted as an act of war by the state attacked, and provoking a response involving recourse to the full range of national capabilities, not just cyber ones, will surely increase. This should give policymakers pause when contemplating deployment of cyber attacks as a cheap, low-risk tool of coercion, the outcomes from which they can safely control and contain. It should also give analysts pause before discounting the possibility that wars in the future may have their immediate origin in cyber acts not intended or expected to produce that outcome.

Bibliography

Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Specter, M. and Weitzner, D. (2015) 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications'. *Journal of Cybersecurity*. 1 (1): 69–79.

Adams, K. (2003) 'Attack and Conquer?' *International Security.* 28(3): 45–83.

Abdollah, T. (2016) 'Obama Seeks Cybersecurity Boost to Replace 'Ancient' Tech'. *PBS.* 9th February. Available from:

https://www.pbs.org/newshour/politics/obama-seeks-cybersecurity-boost-to-replace-ancient-tech

[Accessed 3 December 2019]

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., and Upton, D. (2018) 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate'. *Journal of Cybersecurity*. 4 (1):1-15.

Ahmad, A., Salahieh, S., and Snyder, R. (2017) 'Multinational Uranium Enrichment in the Middle East'. *Energy Policy*. 106: 103-110.

Akdag, Y. (2018) 'The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective'. *Journal of Chinese Political Science.* 24 (2):225-247.

Albright, D. and Walrond, C. (2011) 'Iran's Advanced Centrifuges'. *Institute for Science and International Security.* 1-5.

Albright, D., Brannan, P., and Walrond, C. (2011) 'Stuxnet Malware and Natanz'. **I***nstitute for Science and National Security.* 1-12.

Alexander, C. (2009) *The War that killed Achilles*. Faber and Faber: London.

Alexander, D. (2012) 'Cyber Threats in the 21st Century'. *Security.* 49 (9):70-76.

Anscombe, G.E.M. (2000) *Intention*. Harvard University Press: London.

Aron, R. (1957) *War and Industrial Society.* Oxford University Press: Oxford.

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

Arquilla, J. and Ronfeldt, D. (eds.) (2001) *Networks and Netwars*. RAND: Pittsburgh.

Azmi, Riza., Tibben, W. and Win, K. (2018) 'Review of Cybersecurity Frameworks: Context and Shared Concepts'. *Journal of Cyber Policy.* 3(2): 258–83.

Baldwin, D. (1979) 'Power Analysis and World Politics : New Trends versus Old Tendencies' *World Politics.* 31(2): 161–94.

Baltic Times (2007) 'Forbidden Structures'. *Baltic Times* [online] 14th February. Available from: https://www.baltictimes.com/news/articles/17342/

[Accessed 25 June 2021]

Barnard-Wills, D. and Ashenden, D. (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk'. *Space and Society*. 15(2): 110–123.

Barzashka, I. (2013) 'Are Cyber-Weapons Effective?: Assessing Stuxnet's Impact on the Iranian Enrichment Programme'. *RUSI journal*. 158 (2): 48-56

Barrett, L., Mesquita, B. and Gendron, M. (2011) 'Context in Emotion Perception'. *Current Directions in Psychological Science.* 20 (5): 286-290.

Baudrillard, J. (1995) *The Gulf War Did Not Take Place.* Indiana University Press: Indianapolis. Translated by Paul Patton.

BBC News Wire (2009) 'Iranian Nuclear Chief Steps Down'. *BBC.* 16th July. Available from: http://news.bbc.co.uk/1/hi/world/middle_east/8153775.stm

[Accessed 2 January 2018]

BBC News Wire (2009a) 'Iranians Worried About Economy'. *BBC.* 14th January. Available from: http://news.bbc.co.uk/1/hi/world/middle_east/7827198.stm

[Accessed 2 January 2018]

Bechtsoudis, A. and Sklavos, N. (2012) 'Aiming at Higher Network Security through Extensive Penetration Tests'. *IEEE Latin America Transactions.* 10(3): 1752–56.

Becker, G. (1968) 'Crime and Punishment: An Economic Approach.' *Journal of Political Economy,* 76(2): 169–217.

Bellovin, S., Landau, S. and Lin, H. (2017) 'Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications'. *Journal of Cybersecurity.* 3(1): 59–68.

Berdal, M. (2009) *Building Peace after War.* IISS: London.

Berkowitz, L. (1993) *Aggression: Its Causes, Consequences, and Control.* Temple University Press: London.

Berlin Diplomatic Cable I (2008) Iran: German Officials Share Thoughts on NIE, P5+1 Incentive Package, and Autonomous Measures with Ambassador Schulte. 14th February. Available from: https://wikileaks.org/plusd/cables/08BERLIN180_a.html

[Accessed 2 January 2018]

Bernstein, J. (2014) *Nuclear Iran*. Harvard University Press: London.

Black, W. (1997) 'Thinking Out Loud About Cyberspace'. *Cryptolog.* 23(1): 1–4.

Blainey, G. (1976) *The Causes of War.* Sun Books: London.

Bledstein, N. (2013) 'Is Cyber Espionage a Form of Market Manipulation'. *Journal of Law and Cyber Warfare,* 2(1): 104–10.

Bohn, D. (2019) 'US Cyberattack Repeatedly Hits Iranian Targets. *The Verge.* June 20th. Available from: https://www.theverge.com/2019/6/22/18714010/us-cyberattack-iranian-targets-missile-command-report

[Accessed 19 June 2021]

Bracken, P. (2017) 'Cyberwar and Its Strategic Context'. *Georgetown Journal of International Affairs,* 18(3): 147–57.

Brake, B. (2015) 'Strategic Risks of Ambiguity in Cyberspace'**.** *Council on Foreign Relations* (2015): 1.

Brantly, A. (2014) 'Cyber Actions by State Actors: Motivation and Utility'. *International Journal of Intelligence and CounterIntelligence,* 27(3): 465–84.

Brenner, S. (2007) ''At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare'**.** *Journal of Criminal Law and Criminology, 97(2): 379–475.*

Brinkley, A. (2008) *The Unfinished Nation*. McGraw Hill: London.

Broeders, D. (2017) 'Aligning the International Protection of 'the Public Core of the Internet' with State Sovereignty and National Security'. *Journal of Cyber Policy,* 2(3): 366–76. https://doi.org/10.1080/23738871.2017.1403640.

Brown, C. and Eckersley, R. [eds.] (2018) *Oxford Handbook of International Political Theory*. Oxford University Press: Oxford.

Brown, G. (2011) 'Why Iran Didn't Admit Stuxnet Was an Attack'. *Joint Forces Quarterly*. 63 (4): 70-73.

Brownlee, L. (2015) 'Report: Chinese Hackers Used OPM Data To Steal US Military Intel; "Significant Risk To US Military."' *Forbes*. [online] 19th September 2015. Available from: https://www.forbes.com/sites/lisabrownlee/2015/09/19/report-chinese-hackers-used-opm-data-to-steal-us-military-intel-significant-risk-to-us-military/#8957fcd68293.

[Accessed 21 March 2018]

Bryans, J. (2017) 'The Internet of Automotive Things: Vulnerabilities, Risks and Policy Implications'**.** *Journal of Cyber Policy,* 2(2): 185–94.

Buchan, R. (2012) 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions'. *Journal of Conflict & Security Law,* 17(2): 211–27.

Buchanan, B. (2016) 'The Life Cycles of Cyber Threats'. *Survival,* 58(1): 39–58.

Buchanan, B. (2017) *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press: Oxford.

Bull, H. (1985) *The Anarchical Society*. Macmillan: Basingstoke.

Burton, J. (2015) 'NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation'. *Defence Studies,* 15(4): 297–319.

Bussolati, N. (2015) "The Rise of Non-State actors in Cyberwarfare" in Ohlin, J. Govern, K and Finkelstein, C. (eds.) *Cyberwar: Law and Ethics for Virtual Conflicts*. Oxford University Press: Oxford: 102-128.

Butrimas, V. (2014) 'National Security and International Policy Challenges in a Post Stuxnet World'. *Lithuanian Annual Strategic Review.* 12: 11-31.

Buzan B. and Herring, E. (1998) *The Arms Dynamic in World Politics.* Lynne Rienner: London.

Byford, G. (2002) 'The Wrong War'. *Foreign Affairs* 81(4): 34.

Campbell, D. (1998) *Writing Security.* Manchester University Press: Manchester.

Carr, M. (2016) 'Public – Private Partnerships in National Cyber-Security Strategies'. *International Affairs,* 92(1): 43–62.

Carson, A. and Yarhi-Milo, K. (2017) 'Covert Communication: The Intelligibility and Credibility of Signaling in Secret'. *Security Studies.* 26 (1): 124-156.

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

CCDCOE (2021) 'Cooperative Cyber Defence Centre of Excellence'. 13th June. Available from: https://ccdcoe.org/about-us/

[Accessed 13 June 2021]

Chan, Sewell (2016) 'Cyberattacks Strike Saudi Arabia Harming Aviation Agency'. *New York Times.* 1st December. Available from https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html

[Accessed 2 January 2018]

Chaudhary, T, Jordan, J., Salomone, M., and Baxter, P. (2018) 'Patchwork of Confusion: The Cybersecurity Coordination Problem'. *Journal of Cybersecurity.* 4(1): 1–13.

Chen, T. (2010) 'Stuxnet, the Real Start of Cyber Warfare?' *IEEE Networks*. 2-3.

Choucri, N., Madnick, S., and Ferwerda, J. (2014) 'Institutions for Cyber Security: International Responses and Global Imperatives'. *Information Technology for Development*. 20(2): 96–121.

Cimbala. S. (2014) 'Cyber War and Deterrence Stability: Post-START Nuclear Arms Control.' *Comparative Strategy*, 33:3, 279-286.

Cimbala, S. and McDermott, R. (2015) 'A New Coldwar? Missile Defenses, Cuclear Arms Reductions, and Cyberwar.' *Comparative Strategy.* 34(1): 95–111.

Cimbala, S. (2017) 'Nuclear Deterrence and Cyber Warfare: Coexistence or Competition?' *Defense and Security Analysis*. 33(3): 193–208.

Cimbala, S. (2017 II) 'Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War'. *Journal of Slavic Military Studies,* 30(4): 487–505.

Clapper, J. (2011) 'Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Committee on Armed Services'. *Director of National Intelligence*. 10th March. Available from:

https://www.dni.gov/files/documents/Newsroom/Testimonies/20110310_testimony_clapper.pdf

[Accessed 21 June 2021]

Clapton, W. (2011) 'Risk in International Relations'. *International Relations*. 25 (3): 280-295.

Clark, R. and Knake, R. (2012) *Cyber War: The Next Threat to National Security and What To Do About It*. HarperCollins: New York.

Clark, W. (2001) *Waging Modern War.* Public Affairs:New York.

Clausewitz, Karl Von, (2000) "On War" in Carr, C. (ed.) *The Book of War*. Modern Library, New York. pp. 264-984

Clinton, L. (2015) 'Best Practices for Operating Government-Industry Partnerships in Cyber Security'. *Journal of Strategic Security.* 8(4): 53–68.

Cohen, A. (2010)' Israel's Nuclear Future: Iran, Opacity and the Vision of Global Zero'. *Palestine-Israel Journal of Politics, Economics & Culture.* 16 (3): 6-20.

Colbaugh, R. and Glass, K. (2011) 'Proactive Defense for Evolving Cyber Threats'. *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, ISI* 2011: 125–30.

Collins, S. and McCombie, S. (2012) 'Stuxnet: The Emergence of a new Cyber Weapon and its Implications'. *Journal of Policing, Intelligence and Counter Terrorism*. 7 (1): 80-91.

Colorossi, J. (2015) *Security Supervision and Management: Theory and Practice of Asset Protection*: Fourth Edition. Elsevier Inc.

Cooper, R. (2004) *The Breaking of Nations*. Atlantic Books: London.

CNN (2011) 'Opinion Research Poll'. *CNN* [online] 14th March. Available from http://i2.cdn.turner.com/cnn/2011/images/03/14/rel4a.pdf

[Accessed 7 September 2017]

Craig, A. and Valeriano, B. (2016) 'Conceptualising Cyber Arms Races'. **I***nternational Conference on Cyber Conflict, CYCON* 2016-August: 141–58.

Crandall, M. (2014) 'Soft Security Threats and Small States: The Case of Estonia'. *Defence Studies* 14(1): 30–55.

Cronin, A. (2006) 'Cyber-Mobilization: The New Levée En Masse'. *Parameters.* 36(2): 77–88.

Cusumano, M. (2004) 'Who Is Liable for Bugs and Security Flaws in Software?' *Communications of the ACM.* 47(3): 25–27.

Dabashi, H. (2010) **I***ran, the Green Movement and the USA: the Fox and the Paradox*. Zed Books. Available from: https://ebookcentral.proquest.com/lib/bham/detail.action?docID=619254&pq-origsite=primo

[Accessed 22 June 2021]

Davenport, K (2021) 'Timeline of Nuclear Diplomacy With Iran'. *Arms Control Association*. 13th June. Available from: https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran

[Accessed 13 June 2021]

Davis, J. (2007) 'Hackers Take Down the Most Wired Country in Europe'. *Wired* [online] 21st August. Available from https://www.wired.com/2007/08/ff-estonia/

[Accessed 21 September 2017]

Davis, J., Pfaltzgraff, J., and Pfaltzgraff, R. (2013) *Anticipating a Nuclear Iran: Challenges for U.S. Security.* Columbia University Press, New York.

Available from: ProQuest Ebook Central. [21 June 2021].

Davis, P. 2014. 'Deterrence, Influence, Cyber Attack, and Cyberwar.' *Journal of International Law and Politics,* 47(2): 327–55.

Dearden, L. (2017) 'Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport hit by Hackers'. *Independent* [online] 27th June. Available from: https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html

[Accessed 23 May 2018]

DeBusk, K. and Austin, E. (2011) 'Emotion Intelligence and Social Perception'. *Personality and Individual Differences*. 51: 764-768.

Dehghan, S. (2011) 'Iran Accuses Siemens of Helping Launch Stuxnet Cyber-Attack'. *Guardian* [online] 17th April. Available from:

https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack

[Accessed 21 May 2018]

Delbruck, H. (1985) *History of the Art of War*. Greenwood Press: London.

Denning, D. (1999) *Information Warfare and Security*. ACM Press Books: Harlow.

Denning, D. (2012) 'Stuxnet: What has changed?' *Future Internet*. 4: 672-687

Deseriis, M. (2017) 'Hacktivism: On the Use of Botnets in Cyberattacks'. *Theory, Society and Society*. 34(4): 131–52.

Detter, I. (2013) *Justice, International Law and Global Security: Law of War***,** Ashgate Publishing Ltd, Farnham, Surrey, GBR. Available from: ProQuest ebrary. [1 December 2015].

Dever, J, (2013) 'Cyberwarfare: Attribution, Preemption, and National Self Defense'**.** *Journal of Law and Cyber Warfare, 2(1): 25–63.*

DiDonanto, T., Ullrich, J. and Krueger, J. (2011) 'Social Perception as Induction and Inference: An Integrative Model of Intergroup Differentiation, Ingroup Favoritism, and Differential Accuracy'. *Journal of Personality and Social Psychology*. 100 (1): 66-83.

Dinstein, Y. (2011) *War, Aggression and Self-Defence.* Cambridge University Press: Cambridge.

Dombrowski, P. and Demchak, C. (2014) 'Cyber War, Cybered Conflict, and the Maritime Domain'. *Naval War College Review.* 67(2): 70–96.

Donner, M. (2007) 'Cyber Assault on Estonia'. *IEEE Security and Privacy,* 5(4): 4.

Duelfer, C. and Dyson, S. (2011) 'Chronic Misperception and International Conflict'. *International Security*. 36 (1): 73-100.

Durante, M. (2015) 'Violence, Just Cyber War and Information'. *Philosophy and Technology*. 28(3): 369–385.

Ducaru, S. (2016) 'Is Cyber Defense Possible'. *Journal of International Affairs.* 70(1): 182–89.

Duncan, A, Creese, A., and Goldsmith. M. (2015) 'An Overview of Insider Attacks in Cloud Computing'. *Concurrency and Computation: Practice and Experience.* 27(12): 2964–81.

Dunlap, C. (2011) 'Perspectives for Cyber Strategists on Law for Cyberwar'. *Strategic Studies Quarterly***.** (Spring 2011): 81–99.

Dunn Cavelty, M. (2007) 'Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate'**.** *Journal of Information Technology,* 4(1): 19–37.

Duyvesteyn, I. (2012) 'The Escalation and De-escalation of Irregular War: Setting Out the Problem'. *Journal of Strategic Studies*. 35 (5): 601-611.

Eberle, C. (2013) 'Just War and Cyberwar'. *Journal of Military Ethics.* 12(1): 54–67.

Eder-Neuhauser, P., Zseby, T., Fabini, J. and Vormayr, G. (2017) 'Cyber Attack Models for Smart Grid Environments'**.** *Sustainable Energy, Grids and Networks***.** 12: 10–29.

Edwards, B., Furnas, A., Forrest, S., and Axelrod, S. (2017) 'Strategic Aspects of Cyberattack, Attribution, and Blame'. *Proceedings of the National Academy of Sciences of the United States of America,* 114(11): 2825–30.

Eilstrup-Sangiovanni, M. (2018) 'Why the World Needs an International Cyberwar Convention'. *Philosophy and Technology*. 31(3): 379–407.

Ellis, J. (1993) *The Social History of the Machine Gun*. Pimlico: London.

Elsea, J. & Weed, M. (2014) *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications*. 31133. Washington: Congressional Research Service.

Emerson, R. (2016) 'Limits to a Cyber-Threat'. *Contemporary Politics.* 22(2): 178–96.

Espiner, T. (2008) 'Estonia's Cyberattacks: Lessons Learned, a Year on'. *ZDNet* [online] 1st May. Available from: http://www.zdnet.com/article/estonias-cyberattacks-lessons-learned-a-year-on/

[Accessed 21 September 2017]

Euractiv (2012) 'NATO Agrees on Common Approach to Cyber Defence'. *Euractiv.* 28th May. Available from http://www.euractiv.com/section/digital/news/nato-agrees-common-approach-to-cyber-defence/

[Accessed 5 October 2017]

Faga, H. (2017) 'The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century'. *Baltic Journal of Law and Politics,* 10(1): 1–34.

Farrell, H, and Glaser, C. (2017) 'The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine'. *Journal of Cybersecurity*. 3(1): 7–17.

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

Fazal, T. (2012) 'Why States no Longer Declare War'. *Security Studies*. 21 (4): 557-593.

Fearon, J. (1995) 'Rationalist Explanations for War'. *International Organization***.** 49(3): 379–414.

Feldman, C. (1999) 'Intentionality and Interpretation' in Zelazo, P., Astington, J. and Olson, D. (eds.) *Developing theories of intention*. London: Lawrence Erlbaum Associates. 317-328.

Fidler, D. (2011) 'Was Stuxnet an Act of War?' *IEEE Computer and Reliability Societies.* 56-59

Fidler, M. (2015) 'Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis'. *A Journal of Law and Policy for the Information Society***.** 11(1): 405–83.

Finkle, J. (2016) 'US Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage'. *Reuters* [online] 8th January. Available from: https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108

[Accessed 23 May 2018]

Finlay, C. J. (2017) 'The Concept of Violence in International Theory: a Double-Intent Account'. *International Theory,* 9(1): 67–100.

Finlay, C. (2018) 'Just War, Cyber War, and the Concept of Violence'. *Philosophy and Technology*. 31(3): 357–77.

Finnemore, M. and Sikkink, K. (1998) 'International Norm Dynamics and Political Change'. *International Organization,* 52(4): 887–917.

Fischerkeller, M., and Harknett, R. (2017) 'Deterrence Is Not a Credible Strategy for Cyberspace'. *Orbis.* 61(3): 381–93.

Floridi, L., and Taddeo, M. (2016) 'What Is Data Ethics?' *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,* 374(2083): 360.

Foley, J. (2013)' It's Time to Rethink America's Corn System'. *Scientific American* [online] 5th March. Available from: https://www.scientificamerican.com/article/time-to-rethink-corn/

[Accessed 7 September 2017]

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

Freedman, L. (1989) *The Evolution of Military Strategy.* Basingstoke: Macmillan.

Freedman, L. (2003) 'War Is the Continuation of Politics by Other Means'. *Foreign Policy,* 16–24.

Freedman, L. (2008) *A Choice of Enemies*. Weidenfeld and Nicolson: London.

Freedman, L. (2017) *The Future of War*. Allen Lane: St. Ives.

Fukuyama, F. (1993) *The End of History*. Penguin: London.

Futter, A. (2018) ''Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies'. *Journal of Cyber Policy.* 3(2): 201–16.

Galinec, D., Moznik, D. and Guberina, B. (2017) 'Cybersecurity and Cyber Defence: National Level Strategic Approach'. *Automatika*. 58(3): 273–86.

Galtung, J. (1969) 'Violence, peace, and Peace Research'. *Journal of Peace Research*, 169–191.

Gardner, Frank (2009) 'NATO's Cyber Defence Warriors'. *BBC.* 3rd February. Available from:

http://news.bbc.co.uk/1/hi/world/europe/7851292.stm

[Accessed 13 June 2021]

Gartzke, E. and Lindsay, J. (2015) 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace'. *Security Studies*. 24(2): 316–48.

Gartzke, E. and Lindsay, J. (2017) 'Thermonuclear Cyberwar'. *Journal of Cybersecurity* 3(1): 37–48.

Gat, A. (2001) *A History of Military Thought.* Oxford: Oxford University Press.

Gat, A. (2007) 'The Return of Authoritarian Great Powers'. *Foreign Affairs.* 86(4): 59–69.

Geers, K. (2010) 'The Challenge of Cyber Attack Deterrence'. *Computer Law and Security Review*. 26(3): 298–303.

Gervais, M. (2012) 'Cyber Attacks and the Laws of War' *SSRN Electronic Journal* 1.

Gilbert, P. (2010) *Societal Identity and Political Ethics.* Edinburgh: Edinburgh University Press.

Glaser, C. (1997) 'The Security Dilemma Revisited'. *World Politics*. 50(1): 171–201.

Glaser, C. and Kaufmann, C. (1998) 'What Is the Offense-Defense Balance and Can We Measure It?' *International Security*. 44(39): 1–23.

Glaser, C. (2015) 'A U.S.-China Grand Bargain? The Hard Choice between Military Competition and Accommodation'. *International Security* 39(4): 49–90.

Glenn, R. (2009) 'Thoughts on 'Hybrid' Conflict'. *Small Wars Journal***.** 31(April 2008): 107–13.

Glennon, M. (2005) 'How International Rules Die'. *Georgetown Law Journal.* 93(3): 939–91.

Gompert, D. and Libicki, M. (2015) 'Waging Cyber War the American Way'*. Survival.* 57(4): 7–28.

Gortzak, Y., Haftel, Y., and Sweeney, K. (2005) 'Offense-Defense Theory: An Empirical Assessment'. *Journal of Conflict Resolution*. 49(1): 67–89.

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

Greenberg, A. (2016) 'The Shadow Brokers Mess is What Happens When NSA Hoards Zero-Days'. *Wired* [online] 17th August. Available from: https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/

[Accessed 23 May 2018]

Greenberg, A. (2017) 'How an Entire Nation Became Russia's Test Lab for Cyberwar'. *Wired* [online] 20th June. Available from: https://www.wired.com/story/russian-hackers-attack-ukraine/

[Accessed 18 May 2018]

Gross, M. (2009) *Moral Dilemmas of Modern War*. Cambridge: Cambridge University Press.

Guardian News Wire (2013) 'Former US General James Cartwright named in Stuxnet leak inquiry'. *Guardian.* 28th June. Available from: https://www.theguardian.com/world/2013/jun/28/general-cartwright-investigated-stuxnet-leak

[Accessed 2 January 2018]

Guha, K and Gowers, A. (2005)' McCain Cautions on use of orce in Iran'. *Financial Times*. 28th January. Available from: https://www.ft.com/content/f566e760-7169-11d9-a5d6-00000e2511c8

[Accessed 13 June 2021]

Gul, A. (2012) 'Iran's Pursuit of Peaceful Nuclear Technology'. *Pakistan Horizon*. 65 (1): 35-52.

Gustafson, D. (1986) *Intention and Agency*. Dordrecht: Reidel.

Haataja, S. (2013) 'Technology, Violence and law: Cyber Attacks and Uncertainty in International law.' In *ECIW 2013 12th European Conference on Information Warfare and Security*. 11-12 July 2013. Jyväskylä. Available from: https://research-repository.griffith.edu.au/bitstream/handle/10072/59770/92535_1.pdf?sequence=1&isAllowed=y

Hagerott, M. (2014) 'Stuxnet and the Vital Role of Critical Infrastructure Operators and Engineers. *International Journal of Critical Infrastructure Protection*. 7 (4): 244-246.

Hammes, T. (2006) *The Sling and the Stone*. Zenith: Minneapolis.

Hansel, M. (2018) 'Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks'. *Journal of International Relations and Development*. 21(3): 523–31.

Hansel, M., Mutschler, M. and Dickow, M. (2018) 'Taming Cyber Warfare: Lessons from Preventive Arms Control'. *Journal of Cyber Policy.* 3(1): 44–60.

Hanson, V. (2009) *The Western Way of War*. University of California Press: London.

Harris, J. (1980) *Violence and Responsibility*. Routledge: London.

Hathaway, O, Crootof, R., Perdue, W. and Levitz, P. (2012) 'The Law of Cyber-Attack'. *California Law Review*. 100(4): 817–85.

Haukkala, H. (2009) 'A Close Encounter of The Worst Kind? The Logic of Situated Actors and the Statue Crisis Between Estonia and Russia'. *Journal of Baltic Studies*. 40 (2): 201-213.

Heim, M. (1993) *The Metaphysics of Virtual Reality*. Oxford University Press: Oxford.

Heinrich, M. and Holland, S. (2010) 'IAEA Fears Iran Working now on Nuclear Warhead'. *Reuters*. 19th February. Available from:

https://www.reuters.com/article/us-nuclear-iran-iaea-idUSTRE61H4EH20100219

[Accessed 21 June 2021]

Herszenhorn, D. (2015) 'Russian Warns Denmark on Joining NATO Missile Defence'. N*ew York Times*. 22nd March. Available from:

https://www.nytimes.com/2015/03/23/world/europe/russian-warns-denmark-on-joining-nato-missile-defense.html

[Accessed 25 June 2021]

Herz, J. (1951) *Political Realism and Political Idealism*. University of Chicago Press: London.

Heuser, B. (2013) *Evolution of Strategy*. Cambridge University Press: Cambridge.

Hills, M. (2014) 'The Deregulation and Swarming of Cyberwarfare: The Need for and Limitations of Law in Enabling Aggressive Hacking-Back and Pre-Emption'. *Journal of Law & Cyberwarfare***.** 3(1): 43–51.

Hoffman, F. (2009) 'Hybrid Warfare and Challenges'. *Joint Forces Quarterly* (52): 34–39.

Howard, M. (1983) *The Causes of War and Other Essays*. Temple Smith: London.

Hughes, J. (1988) 'The Origins of World War II in Europe: British Deterrence Failure and German Expansionism'. *The Journal of Interdisciplinary History* 18(4): 851–91.

Hughes, R. (2010) 'A Treaty for Cyberspace'. *International Affairs.* 86 (2): 523–541.

Hundley, R. and Anderson, R. (1996) 'Emerging Challenge : Security and Safety in Cyberspace'. *IEEE Technology and Society*. Winter: 19–28.

Huntington, S. (2002) *Clash of Civilisations and the remaking of world order*. Shuster and Shuster: London.

IAEA (1989) *Statute*. IAEA. Available from: https://www.iaea.org/sites/default/files/statute.pdf [Accessed 22 June 2021]

ICS-Cert (2013) 'Incident Response Activity: Trends in Incident Response in 2013'**.** *ICT-CERT Monitor* (December): 1–14.

Iives, T. (2016) 'The Consequences of Cyber Attacks'. *Journal of International Affairs* 70(1): 175–78.

Ikenberry, J. (2001) *After Victory*. Princeton: Princeton University Press.

Inkster, N. (2017) 'Measuring Military Cyber Power'. *Survival*. 59(4): 27–34.

Janicatova, S. and Mlejnkova, P. (2021) 'The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political–Military Discourse on Russia's Hostile Activities'. *Contemporary Security Policy*. 42 (3): 312-344.

Jenkins, R. (2016) 'Cyberwarfare as Ideal War.' In Allhoff, F., Henschke, A. and Strawser, B. (eds.) *Binary Bullets,* Oxford: Oxford University Press, 89–114.

Jensen, E. (2002) 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense'. *Stanford Journal of International Law***.** 38(207): 207–40.

Jepperson, R.L., Wendt, A. and Katzenstein, P. (1996) 'Norms, Identity, and Society' in Katzenstein, P. (ed.) *The Society of National Security Norms and Identity in World Politics*. New York: Columbia University Press. 33–75.

Jervis, R. (1976) *Perception and Misperception in International Relations*. Princeton: Princeton University Press.

Jervis, R. (2010) 'Cooperation Under the Security Dilemma'. *World Politics* 30(2): 167–214.

Joll, J. and Martel, G. (2007) *The Origins of the First World War*. London: Pearson Longman.

Jonea, P. (2014) 'US-Iran Nuclear Track Two from 2005 to 2011: What have we learned? Where are we going?' *Negotiation Journal*. 30 (4): 347-367.

Junio, T. (2013) 'How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate'. *Journal of Strategic Studies*. 36(1): 125–133.

Kaiser, R. (2012) 'Reassembling the Event: Estonia's 'Bronze Night''. *Environment and Planning D: Society and Space***.** 30: 1046 – 1063.

Kaldor, M. (2012) *New and Old Wars* (3rd ed.) Polity: Cambridge.

Kan, P. (2013) 'Cyberwar to Wikiwar: Battles for Cyberspace'. *Parameters* 43(3): 111–18.

Kaspersky (2017) 'Black Energy APT Attacks in Ukraine'. *Kaspersky Lab* [online] Available from: https://www.kaspersky.co.uk/resource-center/threats/blackenergy

[Accessed 23 May 2018]

Kaye, D., Nader, A. and Roshan, P. (2011) *Israel and Iran: A Dangerous Rivalry.* Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/monographs/MG1143.html

Kazenstein, P. (ed.) (1996) *The Society of National Security*. New York: Columbia University Press.

Keegan, J. (1994) *A History of Warfare*. London: Pimlico.

Kello, L. (2013) 'The Meaning of the Cyber Revolution: Perils to theory and statecraft'. *International Security*, 38 (2): 7-40.

Kello, L. (2017) *The Virtual Weapon and International Order*. Yale University Press: London.

Kehler, C., Lin, H., and Sulmeyer, M. (2017) 'Rules of Engagement for Cyberspace Operations: A view from the USA'. *Journal of Cybersecurity,* 3(1): 69–80.

Kilovaty, I. (2015) 'Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter'. *Journal of Law and Cyber Warfare*. 4(3): 210–244.

Klimburg, A. (2011) 'Mobilising Cyber Power'. *Survival,* 53(1): 41–60.

Kliem, T. (2017) 'You Can't Cyber in Here, This is the War Room! A Rejection of the Effects Doctrine on Cyberwar and the Use of Force in International Law'. *Journal on the Use of Force and International Law*, 4(2): 344–370.

Klein, B. (1994) *Strategic Studies and World Order*. Cambridge: Cambridge University Press.

Kolakowski, L. (1973) *The Presence of Myth.* University of Chicago Press: London.

Korns, S. W., and Kastenberg, J. E. (2009) 'Georgia's Cyber Left Hook'. *Parameters*, (Winter 2008-09), 60–76.

Kosenkov, A. (2016) 'Cyber Conflicts as a new Global Threat'. *Future Internet*, 8(3).

KPMG. (2015) 'Connected and Autonomous Vehicles – The UK Economic Opportunity'. *KPMG International*, (March), 1–24.

Kreps, S and Schneider, J. (2019) 'Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics.' *Journal of Cybersecurity*, 5 (1): 1-11.

Kroenig, M. (2014) *A Time to Attack: The Looming Iranian Nuclear Threat.* Palgrave Macmillian: London.

Kshetri, N. (2014) 'Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses'. *East Asia*, 31(3): 183–201.

Kushner, D. (2013) 'The Real Story of Stuxnet'. *IEEE Spectrum.* 50 (3): 48-53.

Lane, T., Pabriks, A., Purs, A., and Smith, D. (2002) *The Baltic States : Estonia, Latvia and Lithuania*. Taylor & Francis Group: Florence. Available from: ProQuest Ebook Central.

[Accessed 25 June 2021]

Langner, R. (2013) 'To Kill a Centrifuge: A Technical Analysis of what Stuxnet's Creators tried to Achieve'. *The Langner Group*, 1-36.

Langner R. (2013a) 'Stuxnet's secret twin'. *Foreign Policy* [online] 19th November. Available from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

[Accessed 30 July 2015]

Lanoszka, A. (2016) 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe'. *International Affairs*, 92(1): 175–195.

Lawson, S. (2013) 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats'. *Journal of Information Technology and Politics*, 10(1): 86–103.

Lawson, S. (2012) 'Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States'. *First Monday*, 17(7): 555–562.

Leverett, E., and Kaplan, A. (2017) 'Towards Estimating the Untapped Potential: a Global Malicious DDoS mean Capacity Estimate'. *Journal of Cyber Policy*, 2(2): 195–208.

Levy, J. S. (2018) 'Domestic Politics and War'. *The Journal of Interdisciplinary History*, 18(4): 653–673.

Levy, J. S. (1984) 'The Offensive / Defensive Balance of Military Technology : A Theoretical and Historical Analysis'. *International Studies*, 28(2): 219–238.

Lewis, J. (2012) 'In Defense of Stuxnet'. *Military and Strategic Affairs*. 4 (3): 65-76.

Lewis, J. A. (2014) 'National Perceptions of Cyber Threats'. *Strategic Analysis*, 38(4): 566–576.

Li, Q. and Mu, L. (2014) 'Analysis of Security of SCADA System'. *Applied Mechanics and Materials.* 568-570: 1417-1421.

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

Libicki, M. C. (2012) 'Crisis and Escalation in Cyberspace'. *Rand Corporation*. Special Issue. Iii-198. Available from https://doi.org/10.7249/j.ctt24hrx7.

Libicki, M. C. (2016) 'Is There a Cybersecurity Dilemma?' *The Cyber Defense Review*, 1(1): 129–140.

Libicki, M. C. (2017) 'Second Acts in Cyberspace'. *Journal of Cybersecurity*, 3(1): 29–35.

Liddell-Hart, B. (1967) *Strategy: the Indirect Approach*. Faber and Faber: London.

Lieven, D. (2010) *Russia against Napoleon.* London: Penguin.

Liff, A. P. (2013) 'The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio'. *Journal of Strategic Studies*, 36(1): 134–138.

Lilienthal, G., and Ahmad, N. (2015) 'Cyber-attack as Inevitable Kinetic War'. *Computer Law and Security Review*, 31(3): 390–400.

Limnéll, J. (2016) 'The Cyber Arms Race is Accelerating – What are the Consequences?' *Journal of Cyber Policy*, 1(1): 50–60.

Lin, H. (2012) 'Escalation Dynamics and Conflict Termination in Cyberspace Terminology and Basic Concepts'. *Strategic Studies Quarterly*, Fall: 46–70.

Lind, W., Nightengale, K., Schmitt, J., Sutton, J. and Wilson, G. (1989)'The Changing Face of Warfare: Into the Fourth Generation' *Marine Corps Gazette*, October: 22-26

Lindemann, K. and Saar, E. (2012) 'Ethnic Inequalities in Education: Second-Generation Russians in Estonia'. *Ethnic and Racial Studies*. 35 (11): 1974-1998.

Lindsay, J (2013) 'Stuxnet and the Limits of Cyber Warfare'. *Security Studies*. 22 (3): 365-404.

Lindsay, J. R. (2015) 'The Impact of China on Cybersecurity: Fiction and Friction'. *International Security,* 39(3): 7–47.

Lindsay, J. R. (2015) 'Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack'. *Journal of Cybersecurity*, 1(1): 53–67.

Lindsay, J. Cheung, T. and Reveron, D. (eds.) (2015) *China and Cybersecurity*. Oxford University Press: Oxford.

Locatelli, A. (2011) 'The Offense/Defense Balance in Cyberspace'. *Strategic Studies,* 35(1): 1–10.

Long, A. (2017) 'A cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning'. *Journal of Cybersecurity*, 3(1): 19–28.

Lonsdale, D. J. (2018) 'Warfighting for Cyber Deterrence: a Strategic and Moral Imperative'. *Philosophy and Technology*, 31(3): 409–429.

Lucas, G. (2017) *Ethics and Cyber Warfare*. Oxford: Oxford University Press.

Luttwak, E. (1987) *Strategy*. London: Havard University Press.

McGhee, J. E. (2013) 'Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy'. *Journal of Law and Cyber Warfare*, 2(1): 64–103.

McGhee, J. (2015) 'Hack, Attack or Whack; The Politics of Imprecision in Cyber Law'. **J***ournal of Law and Cyber Warfare*, 4(1): 13–41.

McGraw G. (2013) 'Cyber War is Inevitable (Unless We Build Security In)'. *Journal of Strategic Studies*. 36 (1): 109-119.

McGuffin, C., and Mitchell, P. (2014) 'On Domains: Cyber and the Practice of Warfare'. *International Journal: Canada's Journal of Global Policy Analysis,* 69(3): 394–412.

McKenna, C (2017) 'NHS Ransomware Cyber-Attack Was Preventable'. *The Conversation* [online] 13th May. Available from: https://theconversation.com/nhs-ransomware-cyber-attack-was-preventable-77674

[Accessed 23 May 2018]

McLaughlin, D. (2021) 'Estonia at the Fore of Cyber Security After Major Attack in 2007'. *Irish Times*. 13th May. Available from: https://www.irishtimes.com/news/ireland/irish-news/estonia-at-the-fore-of-cyber-security-after-major-attack-in-2007-1.4571673

[Accessed 13 June 2021]

Mack, A. (1975) 'Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict'. *World Politics*, 27(2): 175–200.

Malekos Smith, J. (2016) 'No State is an Energy Island' *Journal of Law & Cyber Warfare*, 5(4): 4–65.

Maness, R. C., and Valeriano, B. (2016) 'Cyber Spillover Conflicts: Transitions From Cyber Conflict to Conventional Foreign Policy Disputes?' *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*,: 45–64.

Manzo, V. (2012) 'Deterrence and Escalation in Cross-domain Operations'. *Joint Force Quarterly*. 66 (3): 8-14.

Mastriano, D. (2017) 'Putin – The Masked Nemesis of the Strategy of Ambiguity'. *Defense & Security Analysis*. 33 (1): 68-76.

Matrosov, A., Rodionov, E., Harley, D.,and Malcho, J. (2010) 'Stuxnet Under the Microscope'. *ESET.com*. 15th October. Available from:

https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

Accessed 22 June 2021

Mattern, T., Felker, J., Borum, R., and Bamford, G. (2014) 'Operational Levels of Cyber Intelligence'. *International Journal of Intelligence and CounterIntelligence*, 27(4): 702–719.

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power.* Cambridge University Press: Cambridge.

Mavropoulou, E. (2015) 'Targeting in the Cyber Domain : Distinction to Cyber Attacks'. *Journal of Law & Cyber Warfare*, 23(4): 23–93.

Mearsheimer, J. (2003) *The Tragedy of Great Power Politics*. New York: Norton.

Mearsheimer, J. and Walt, S. (2007) *The Israel Lobby and US Foreign Policy*. London: Penguin.

Meiland, J. (1970) *The nature of Intention*. London: Methuen.

Meissner, C. and Brigham, J. (2001) 'Thirty Years of Investigating the Own-Race Bias in Memory for Faces. A Meta-Analytic Review'. *Psychology, Public Policy, and Law*. 7: 3–35.

Mele, S. (2014) 'Legal Considerations on Cyber-Weapons and Their Definition'. *Journal of Law & Cyber Warfare*, 3(1): 52–69.

Melin, M. and Grigorescu, A. (2014) 'Connecting the Dots: Dispute Resolution and Escalation in a World of Entangled Territorial Claims'. *Journal of Conflict Resolution*. 58 (6): 1085-1109.

Mendoza, M. (2015) 'Microsoft Patch Tuesday Update Plugs Freak Vulnerability'. *Tech Times* [online] 11th March. Available from:

http://www.techtimes.com/articles/38929/20150311/microsoft-patch-tuesday-update-plugs-freak-vulnerability-stuxnet-security-flaw-and-more.htm

[Accessed 21 May 2018]

Menserve, J. (2007) 'Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid'. *CNN* [online] 26th September. Available from:

http://edition.cnn.com/2007/US/09/26/power.at.risk/

[Accessed 31 January 2019]

Metz, S. (2012) 'The Internet, New Media, and the Evolution of Insurgency'. *Parameters*, (2008): 80–90.

Miller, R. (2011) 'Cyber War and the Dangers of Preemption'. *International Journal of Critical Infrastructure Protection*. 4(1): 22–23.

Milton-Edwards, B. (2010) *Contemporary Politics in the Middle East*. 2nd ed. Cambridge: Polity.

Miskimmon, A., and O'Loughlin, B., (2017) 'Russia's Narratives of Global Order: Great Power Legacies in a Polycentric World'. *Politics and Governance*. 5 (3): 111-120.

Mobasherat, M. and Yan, H. (2013) 'Iran marks 'National Nuclear Day' with a New Uranium-Processing Site'. *CNN*. (online). April 9th. Available from:

https://edition.cnn.com/2013/04/09/world/meast/iran-nuclear/index.html

[Accessed 5 February 2018]

Moran, N. (2009) 'A Historical Perspective on the Cybersecurity Dilemma'. *Insecure*, (209): 112–116.

Muller, R. (2019) *Report on the Investigation Into Russian Interference In the 2016 Presidential Election*. US Department of Justice: Washington DC. Available from: https://heinonline-org.ezproxyd.bham.ac.uk/HOL/Page?handle=hein.congrec/mueller0001&id=1&collection=presidents&index=congrec/mueller

[Accessed 25 June 2021]

Munkler, H. (2005) *The New Wars*. Polity: Cambridge. Translated by Patrick Camiller

Nath, S. (2012) 'What Military Deterrence Cannot Do, Cyber Deterrence Can Do To Iran: Exploring the Implications of Manipulative Incessant Usage of the Term 'Preemptive.'' *International Journal of Social Sciences and Humanity Studies*, 4(1): 313–323.

Naughton, J. (2016) 'The Evolution of the Internet: from Military Experiment to General Purpose Technology'. *Journal of Cyber Policy*, 1(1): 5–28.

Nickel, T. (1974) 'The Attribution of Intention as a Critical Factor in the Relation Between Frustration and Aggression'. *Journal of Personality*. 42 (3): 483-492.

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. (2012) 'SCADA Security in the Light of Cyber-Warfare'. *Computers and Security*, 31(4): 418–436.

NPT (1968) *Treaty on the Non-Proliferation of Nuclear Weapon*s. 1 July. Available from: https://www.un.org/disarmament/wmd/nuclear/npt/text

[Accessed 2 January 2018]

Noor, S. (2015) 'Cyber (In) Security: A Challenge to Reckon With'. *Strategic Studies*, 1–20.

Nye, J. (2004) *Soft Power: The Means To Success In World Politic***s**. New York: Public Affairs.

Nye, J. (2011) 'Nuclear Lessons for Cyber Security?' *Strategic Studies Quarterly*: 18–38.

Nye, J. S. (2013) 'From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?' *Bulletin of the Atomic Scientists*, 69(5): 8–14.

Nye, J. S. (2017) 'Deterrence and Dissuasion in Cyberspace'. *International Security*, 41(3): 44–71.

O'Connell, M. E. (2012) 'Cyber Security Without Cyber War'. *Journal of Conflict and Security Law*, 17(2): 187–209.

Office of General Counsel Department of Defense (2015) 'Weapons'. In *Law of War Manual*. Washington, DC: United States Department of Defense: 340.

Ohlin, J. Govern, K and Finkelstein, C. (eds.) *Cyberwar: Law and Ethics for Virtual Conflicts*. Oxford: Oxford University Press.

Oppenheim, L. (1935) *International Law: A Treatise Volume II*. Longmans, Green and Co: London.

Osanaiye, O., Choo, K. and Dlodlo, M. (2016) 'Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework'. *Journal of Network and Computer Applications*. 67: 47-165.

Osawa, J. (2017) 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?' *Asia-Pacific Review*, 24(2): 113–131.

Osgood, R. (1970) *Limited War*. University of Chicago Press: London.

Ottis, R (2018) *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Center for Excellence Estonia: Tallin. Available from:

https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[Accessed 25 June 2021]

Owens, W., Dam, K. and Lin, H. (2009) *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington DC: National Academies Press.

Paine, M. (2001) Crusades, Pocket Essentials, Harpenden. Available from: ProQuest Ebook Central. [10 July 2021].

Pawlak, P., and Barmpaliou, P.-N. (2017) 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity'. *Journal of Cyber Policy*, 2(1): 123–144.

Payne, K. (1996) *Deterrence in the Second Nuclear Age*. Lexington University Press: Lexington.

Payne, C., and Finlay, L. (2015) 'Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack'. *George Washington International Law Review*, 49(3): 535–569.

Perlroth, N. Sanger, D and Schmidt, M. (2013) 'As Hacking Against U.S. Rises, Experts try to pin Down Motive'. *New York Times* [online] 3rd March. Available from: https://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html

[Accessed 4 December 2019]

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., and Apostolopoulos, T. (2018) 'A New Strategy for Improving Cyber-Attacks Evaluation in the Context of Tallinn Manual'. *Computers and Security*, 74: 371–383.

Posen, B. (1982) 'Inadvertent Nuclear War?: Escalation and NATO's Northern Flank'. *International Security*. 7 (2): 28-54.

Posen, B. (1991) *Inadvertent Escalation: Conventional War and Nuclear Risks.* New York: Cornell University Press.

Poulson, J. (2020) 'Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated'. *Tech Inquiry*. 7th July. Available from:

https://techinquiry.org/SiliconValley-Military/#company-summaries

[Accessed 21 June 2021]

Poulson, Kevin (2007) 'Cyberwar' and Estonia's Panic Attack'. *Wired* [online] 22nd August. Available from https://www.wired.com/2007/08/cyber-war-and-e/

[Accessed 17 October 2017]

Preciado, M. (2012) 'If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare'. *Journal of Law and Cyber Warfare*, 1: 99–154.

Radin, A. (2017) *Hybrid Warfare in the Baltics.* RAND: Santa Monica.

Radu, R. (2013) 'Negotiating Meanings for Security in the Cyberspace'. ***Info***, 15(6): 32–41.

Reynolds, M. (2016) 'Welcome to E-stonia, the world's most digitally advanced society'. Wired [online] 20th October. Available from: https://www.wired.co.uk/article/digital-estonia

[Accessed 20 September 2017]

Rid, T. (2012) 'Cyber War Will Not Take Place'. *Journal of Strategic Studies*. 35 (1): 5-32.

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

Rid, T. and Buchanan, B (2018) 'Hacking Democracy'. *The SAIS review of international affairs*. 38 (1): 3-16.

Riyadh Diplomatic Cable I (2008) Saudi King Abdullah and Senior Princes on Saudi Policy Towards Iraq20th April. Available from: https://wikileaks.org/plusd/cables/08RIYADH649_a.html

[Accessed 2 January 2018]

Robb, C. and Wald, C. (2014) *Evaluating a Nuclear Deal with Iran. Bipartisan Policy Center*. Available from: https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/BPC-Evaluating-an-Iran-Nuclear-Deal.pdf

[Accessed 22 June 2021]

Roberts, P. (2011) 'New York Times: Stuxnet a Joint US-Israeli Operation'. *ThreatPost: The Kaspersky Lab Security News Service* [online] 16 January. Available from: http://threatpost.com/en_us/blogs/new-york-times-stuxnetjoint-us-israeli-operation-011611

[Accessed 4 December 2018]

Romanosky, S. (2016) 'Examining the costs and causes of cyber incidents'. *Journal of Cybersecurity*, 2(2): 121–135.

Romanosky, S., and Goldman, Z. (2016) 'Cyber Collateral Damage'. *Procedia Computer Science,* 95: 10–17.

Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Roscini, M. (2015) 'Evidentiary Issues in International Disputes' in Ohlin, J. D., Govern, K. and Finkelstein, C. (eds.) *Cyberwar: Law and ethics for virtual conflicts.* Oxford, Oxford University Press. 215-248.

Rovner, J., and Moore, T. (2017) 'Does the Internet Need a Hegemon?' *Journal of Global Security Studies*, 2(3): 184–203.

Russell, A. L., and Russell, A. L. (2017) 'Implications for Deterrence and Coercion'. *Strategic A2/AD in Cyberspace:* 53–73.

Rustici, R. (2011) 'Cyberweapons: Leveling the International Playing Field'. *Parameters*, 41(3): 32.

Saltzman, I. (2013) 'Cyber Posturing and the Offense-Defense balance'. *Contemporary Security Policy*, 34(1): 40–63.

Sanger, D. (2012) *Confront and Conceal*. New York: Crown Publishing.

Sauter, M. (2014).*The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic. Available from: http://dx.doi.org.ezproxyd.bham.ac.uk/10.5040/9781628926705

[Accessed 25 June 2021]

Schelling, T. (1966) *Arms and Influence*. Yale University Press: New Haven.

Schmitt, M. (2010) 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts'. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*: 151–78.

Schmitt, M. N. (2013) 'Cyberspace and International Law: The Penumbral Mist of Uncertainty'. *Harvard Law Review*, 126: 1–5.

Schwedler, J. and Gerner, D. (eds.) (2008) *Understanding the Contemporary Middle East*. 3rd ed. London: Rienner.

Schwedler, J. (2008) 'Religion and Politics in the Middle East' in Schwedler, J. and Gerner, D. (eds.) **U***nderstanding the Contemporary Middle East*. London: Lynne Rienner. 373–396.

Securing CyberSpace for the for the 44 Presidency (2008) 'Securing CyberSpace for the for the 44 Presidency'**.** *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, (December).

Shachtman, N. (2008) 'Under Worm assault, Military bans disks, USB drives.' *Wired* [online] 19th November. Available from: https://www.wired.com/2008/11/army-bans-usb-d/

[Accessed 23 May 2018]

Shachtman, N. (2010) 'Insiders doubt 2008 Pentagon hack was foreign spy attack' (updated). *Wired* [online] 25th August. Available from:

https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/

[Accessed 23 May 2018]

Shackelford, S. (2009) 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law'. *Berkeley Journal of International Law.* 27 (1): 192-251.

Shackelford, S. (2010) 'Estonia Three Years Later: A Progress Report on Combating Cyber Attacks'. *Journal of Internet Law*. 22-29.

Shah, S., and Mehtre, B. M. (2013) 'A Latest Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing'. *International Journal of Electronics Communication and Computer Engineering*, 4(6): 47–52.

Shaji, R. S., Sachin Dev, V., and Brindha, T. (2019) 'A Methodological Review on Attack and Defense Strategies in Cyber Warfare'. *Wireless Networks*, 25(6): 3323–3334.

Sharma, A. (2010) 'Cyber wars: A Paradigm Shift From Means to Ends'. *Strategic Analysis*, 34(1): 62–73.

Sharoni, S. and Abu-Nimer, M. (2008) 'The Israeli-Palestinian Conflict' in Schwedler, J. and Gerner, D. (eds.) *Understanding the Contemporary Middle East*. London: Lynne Rienner. 117–220.

Sharp, T. (2017) 'Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony'. *Journal of Strategic Studies*, 40(7), 898–926.

Shui, Y., Tian, Y., Guo, S. and Wu, D. (2014) 'Can We Beat DDoS Attacks in Clouds?' *IEEE transactions on parallel and distributed systems*. 25 (9): 2245-2254.

Shusterman, R. (1992) 'Interpretation, Intention and Truth' in Iseminger, G. (ed.) *Intention and Interpretation*. Philadelphia: Temple University Press. 65-75.

Shusterman, R. (1992a) 'Interpreting with Pragmatist intentions' in Iseminger, G. (ed.) *Intention and Interpretation*. Philadelphia: Temple University Press. 167-182.

Siers, R. (2017) 'North Korea: The Cyber Wild Card 2.0'. **J***ournal of Law & Cyber Warfare*, 6(1): 155–165.

Simmons, N. (2014) 'A Brave New World : Applying International Law of War to Cyber-Attacks'. *Journal of Law & Cyber Warfare*, 4(1): 42–109.

Simon, S. and Martini, J. (2004) 'Terrorism: Denying Al Qaeda its popular support'. *The Washington Quarterly*. 28 (1): 131-145.

Singer, D. (ed.) (1979) *The Correlates of War Volume I*. Free Press: London.

Singer, P. (2010) *Wired For War***.** Penguin: London.

Singer, P. and Friedman, A. (2014) *Cybersecurity and Cyberwar: what everyone needs to know*. Oxford: Oxford University Press.

Sklerov, M. (2009) *Solving the Dilemma of State Responses To Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Protect*. Thesis from Judge Advocat General's School, United States Army .

Slayton, R. (2017) 'What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment.' *International Security*, 41 (3): 72-109.

Sleat, M. (2018) 'Just Cyber War?: Casus belli, Information Ethics, and the Human Perspective'. *Review of International Studies,* 44(2): 324–342.

Smeets, M. (2018) 'A Matter of Time: On the Transitory Nature of Cyberweapons'. *Journal of Strategic Studies*, 41(1–2): 6–32.

Smith, P. (2006) *Why War?* London: University of Chicago Press.

Smoke, R. (1977) *War: Controlling Escalation*. London: Havard University Press.

Spector, L., & Cohen, A. (2008) 'Israel's Airstrike on Syria's Reactor: Implications for the Nonproliferation Regime'. *Arms Control Today***.** 38(6): 15-21.

Strachan, H. and Scheipers, S. (eds.) (2014) *The Changing Character of War*. Oxford University Press: Oxford.

Stadnik, I. (2017) 'What is an International Cybersecurity Regime and How We Can Achieve it?' *Masaryk University Journal of Law and Technology*, 11(1): 129–154.

Steiger, S., Harnisch, S., Zettl, K., and Lohmann, J. (2018) 'Conceptualising Conflicts in Cyberspace'. *Journal of Cyber Policy*, 3(1): 77–95.

Stevens, T. (2012) 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace'. *Contemporary Security Policy,* 33(1): 148–170.

Stockburger, P. (2016). 'Known unknowns: State operations, Cyber Warfare and the Jus Ad Bellum'. *American University International Law Review*, 31(4): 545–591.

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

Suganami, H. (2001) *On the Causes of War*. Oxford University Press: Oxford.

Sullivan, J. E., and Kamensky, D. (2017) 'How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid'. *Electricity Journal*, 30(3): 30–35.

Taddeo, M. (2018) 'Deterrence and Norms to Foster Stability in Cyberspace'. *Philosophy and Technology,* 31(3): 323–329.

Tarock, A. (2016) 'The Iran Nuclear Deal: Winning a Little, Losing a Lot.' *Third World Quarterly*. 37 (8): 1408-1424.

Taylor, C. (1979) 'Action as Expression' in Diamond, C. and Teichman, J. (eds.) *Intention and Intentionality: essays in honour of G.E.M. Anscombe*. Hassocks, Harvester Press. 73-90.

Tétreault, M. (2008) 'The Political Economy of Middle Eastern Oil' in Schwedler, J. and Gerner, D. (eds.) *Understanding the Contemporary Middle East*. London: Lynne Rienner. 225-280.

Thomas, T. (2014) 'Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?' *Journal of Slavic Military Studies*, 27(1): 101–130.

Thornton, R. (2008) *Asymmetric Warfare*. Polity: Cambridge.

Thornton, R. (2015) 'The Changing Nature of Modern Warfare: Responding to Russian Information Warfare'. *RUSI Journal*, 160(4): 40–48.

Tikk, E., Kaska, K. and Vihul, L. (2010) *International Cyber Incidents: Legal Implications*. Cooperative Cyber Defence Centre of Excellence: Talinn

Travis, A. (2003) Support for War falls to new low. **Guardian** [online] 21st January. Available from: https://www.theguardian.com/politics/2003/jan/21/uk.iraq2

[Accessed 7 September 2017]

Traynor, I. (2007) 'Russia Accused of Unleashing Cyberwar to Disable Estonia'. *Guardian*. [online] 17th May 2007. Available from: https://www.theguardian.com/world/2007/may/17/topstories3.russia

[Accessed March 19, 2018].

Trenta, L. (2016) *Risk and Presidential decision-making*. Oxon: Routledge.

Valeriano, B. and Maness, R. (2016) *Cyber War versus Cyber realities: cyber conflict in the international system*. Oxford: Oxford University Press.

Valeriano, B., and Habel, P. (2016) 'Who are the Enemies? The Visual Framing of Enemies in Digital Games'. *International Studies Review*, 18(3): 462–486.

Valeriano, B., and Maness, R. C. (2018) 'How We Stopped Worrying About Cyber Doom and Started Collecting Data. *Politics and Governance*, 6(2): 49–60.

Valeriano, B., and Maness, R. C. (2014) 'The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11'. *Journal of Peace Research*, 51(3): 347–360.

Van Evera, S. (1999) *Causes of War: Power and the Roots of Conflict*. New York: Cornell University Press.

Valuch, J., Gábriš, T., and Hamul'ák, O. (2017) 'Cyber Attacks, Information Attacks, and Postmodern Warfare'. *Baltic Journal of Law and Politics.* 10(1): 63–89.

Vasquez, J, (1998) *The Power of Power Politics*. Cambridge: Cambridge University Press.

Veebel, V. (2018) '(Un)justified Expectations on Nuclear Deterrence of Nonnuclear NATO Members: the Case of Estonia and Latvia?' *Defense & Security Analysis*. 34 (3): 291-309.

Ven Bruusgaard, K. (2016) 'Russian Strategic Deterrence'. *Survival.* 58(4): 7–26.

Vick, K. (2005) 'Iran's President Calls Holocaust 'Myth' in Latest Assault on Jews'. *Washington Post*. (online). 15th December. Available from: http://www.washingtonpost.com/wp-dyn/content/article/2005/12/14/AR2005121402403.html

[Accessed 21 May 2018]

Waltz, K. (2001) *Man, the State, and War*. New York: Cornell University Press.

Walzer, M. (2006) *Just and Unjust Wars*. 4th ed. New York: Basic Books.

Warrick, J. (2011) 'Iran's Natanz Nuclear Facility Recovered Quickly From Stuxnet Cyberattack'. *Washington Post*. 16th February. Available from:

http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021506501.html

[Accessed 2 January 2018]

Washington Times Wire (2007) 'McConnell Fears Iran Nukes by 2015'. *Washington Post* [online] 27th February. Available from:

https://www.washingtontimes.com/news/2007/feb/27/20070227-112340-4811r/

[Accessed 2 January 2018]

Weber, S. (2017) 'Coercion in Cybersecurity: What Public Health Models Reveal'. *Journal of Cybersecurity*, 3(3), 173–183.

Weber, V. (2018) 'Linking Cyber Strategy with Grand Strategy: The Case of the United States'. *Journal of Cyber Policy*, 3(2), 236–257.

Wendt, A. (1999) *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Whyte, C., Valeriano, B., Jensen, B., and Maness, R. (2018) 'Rethinking the Data Wheel: Automating Open-access, Public Data on Cyber Conflict'. *International Conference on Cyber Conflict, CYCON*, 2018-May, 9–30.

Wiener, A. (2015) 'Virtual Crimes , Actual Threats : Cyberspace'. *Journal of Law and Cyber Warfare*, 4(2), 109–149.

Wlodarska, A. (2016) Ethnic Russian Minority In Estonia. **International studies**. 18 (2): 153-164.

Wrange, J., and Bengtsson, R. (2019) 'Internal and External Perceptions of Small State Security: The Case of Estonia'. *European Security*. 28 (4): 449-472.

Wrangham, R. W. (1999). 'Evolution of Coalitionary Killing'. *American Journal of Physical Anthropology*, 110(S29), 1–30.

Wright, Q. (1942) *A Study of War.* Volumes 1 and 2. Chicago: University of Chicago Press.

Yarhi-Milo, K. (2013) 'In the Eye of the Beholder'. *International Security*. 38 (1): 7-51.

Gibney, A. (2016) *Zero Days.* Magnolia Pictures: USA.

Zetter, K. (2014) *Countdown to Zero Day*. New York: Broadway Books.

Zetter, K. (2014a) 'Countdown to Zero Day.' *Wired* [online] 3rd November. Available from: wired.com/2014/11/countdown-to-zero-day-stuxnet/

[Accessed 30 July 2015]

Zetter, K (2014b) 'Hacker Lexicon: What is a Zero Day?' *Wired* [online] 11th November. Available from: https://www.wired.com/2014/11/what-is-a-zero-day/

[Accessed 13 June 2021]

Zhang, L. (2013) 'A Chinese Perspective on Cyber War'. *International Review of the Red Cross*. 94(886): 801–807.

Zrahia, A. (2018) 'Threat Intelligence Sharing Between Cybersecurity Vendors: Network, Dyadic, and Agent Views'. *Journal of Cybersecurity*, 4(1), 1–16.