“Just a cyberattack…”: An Evaluation of the Ethics of Western Cyber Operations using Just War Theory

van Hoeve, Simon

“Just a cyberattack…” An Evaluation of the Ethics of Western Cyber Operations using Just War Theory

(Resubmission)

August 23, 2021

Simon van Hoeve
S2725096
S2725096@vuw.leidenuniv.nl

Word Count: 14,957

Supervisor: Dr. L. Milevski

Submitted in partial requirements for the MA International Relations program, Leiden Universiteit

Contents

Chapter 1: Introduction

Over the past few years, the cyber domain has been finding its place within strategic studies and international relations. This increased appreciation of cyberspace as a unique domain of operations comes alongside an even stronger appreciation that the cyber domain is a viable avenue for foreign actors to target civilians and states. In fact, in only the last half year, the West has seen unprecedented intrusions into government systems in the SolarWinds incident (Weiss and Hunter, 2021), crippling ransomware attacks on critical energy infrastructure in the Colonial pipeline incident (Sanger and Perlroth, 2021), and renewed disinformation campaigns profiting off the COVID-19 pandemic (Ignatidou, 2021). These are not new trends: over the past years, more and more Western rivals have begun to adopt the cyber power to gain advantages over rivals. States such as China, Russia, Iran, and North Korea are especially prolific at using cyber capabilities as part of their 'grey zone' toolkits.

These trends have resulted in a world today where aggression in cyberspace is emerging as a distinct phenomenon which states must respond to. One avenue explored has been the diplomatic: today, many Western governments support recent international law advancements such as the *Tallinn Manual*, as well as even more recent advances in cyber norm formation, such as the UN OEWG processes and the Paris Call. However, this diplomatic route has been seen by some as too slow to achieve real affects. Thus, notably spurred on by the United States, many Western allies have begun turning to offensive cyber operations to either deter, respond to, or proactively defend against unwanted cyber aggression from rivals.

Yet, leaning into the offensive has its own issues. Notably, many observers ask whether it is ethical to launch such operations in cyberspace, especially given the potential consequences of these actions and the risks of escalation. This is especially punctuated by the lack of binding international agreements and law moderating cyber conflict and operations. After all, if governments solely justify launching military cyber operations on the basis of foreign cyber aggressions, citizens should make sure that their

governments are not exacerbating the danger of offensive operations by responding in a likewise manner. Simply put, it is reasonable to ask any state, and especially Western states who proudly display a tradition of human rights and justice, that they can justify their use force in any domain – including cyberspace. If they cannot, then changes in their doctrines should be demanded.

Perhaps the most potent lens to judge whether a conflict is just is the aptly-named Just War Theory (JWT). Stretching back hundreds of years to its start in the musings of Roman philosophers and first codified by early Christian theologians, modern JWT has grown and evolved from these roots to inspire and influence modern international law guiding the entrance into conflict (*Jus Ad Bellum*) and the behaviour of states during warfare *(Jus In Bello*). However, cyberspace and its unique characteristics and nature often impose unique challenges to the application of JWT to cyberspace. This is often seen in debates about whether concepts like 'war' and 'aggression' can really be applied to cyberspace.

Keeping these debates in mind, this thesis will focus on the *Jus Ad Bellum* principles of JWT and apply them to contemporary Western offensive cyber operations in cyberspace. Thus, the main thesis question to be answered is *"To what extent do modern, Western cyber operation abide by the Jus Ad Bellum principles of Just War Theory?"* Applying JWT to cyberspace is not a novel pursuit, but this thesis will stand out in two manners: first, it will update JWT principles in cyberspace using the most recent advances and thinking. Second, this thesis will conduct a broad overview of all notable Western cyber incidents, instead of other projects which only analyze individual case studies. This should allow this thesis to conclude with pressing and unique observations about the overall justness of Western cyber operations.

Guiding the journey to the conclusion will be two sub-questions, which also form the two substantive chapters within this thesis. First, this thesis asks "How can JWT be applied to cyber conflict?" This is partially outlined in the methodology chapter, and then each of the principles of *Jus Ad Bellum*

will be explored to determine whether they still apply for cyber conflict as they do for traditional spheres of conflict in Chapter 4. Using these established principles, this thesis then asks, “Using a JWT framework, are modern Western offensive cyber operations Just?” This is explored within a broad study of Western offensive operations, located in Appendix A, and analyzed in Chapter 5. Finally, an existent concluding chapter ties together the main lessons to answer the thesis question.

Chapter 2: Literature Review

To explore the identified research question and the two sub-questions, an extensive literature review should be conducted of contemporary and relevant literature. This literature review should do three key tasks. First, it should catalogue the evolution of academic discourse on aggression in cyberspace. Second, it should briefly detail the current situation in cyberspace, isolating why the study of aggression is important and also concurrently identifying a gap where ethics-based approaches such as Just War Theory can be of use. Third, previous attempts to explore this gap should be explored. A short conclusion to the literature review will thus clearly identify the theoretical gap in which this thesis will exist, as well as its relevance.

Aggression and War in Cyberspace

The concept of aggression in cyberspace has a vivid history, traditionally receiving the most focus when paired with the study of 'cyber war'. which stretches back to the 1970s. Many credit Thomas Rona, a US Science Advisor, with first coining the term "information warfare" in a 1976 report titled "Weapon Systems and Information Warfare." Herein, Rona argues that these emerging technological trends can enable what he calls 'information warfare' (Rona, 1976). However, in years to come, cyber war would emerge as a credible fear. This was most famously noted in a 1993 article written by John Arquilla and David Ronfeldt, provocatively titled "Cyberwar is Coming!" Here, they predict that the ongoing information revolution will cause shifts in how conflict happens. In particular, they identify netwar (information-based conflict between states and society) and cyberwar (military operations targeting information and communication systems or using information principles) as two key emerging and new forms of warfare and conflict (p. 144). Their observations highlight and emphasize the observation that cyberspace, and new information technologies, form new ways for states and actor to commit acts of aggression, violence, and war against each other.

Martin Libicki also emerged as an influential name in this subject with his 1995 publication "What is Information Warfare?" Libicki here analyzes the concept of 'information warfare,' finding that while it is an ongoing phenomenon that should be analyzed, the way previous scholars defined it can use elaboration and enhanced nuance (Libicki, 1995, pp. 4-6). Thus, Libicki proposes to split up this 'information warfare' into seven subcategories: notably including the subcategory of cyberwarfare. Yet, Libicki shows doubt about whether all seven categories of information warfare, including notably his subcategory of cyberwarfare, are likely to be relevant as forms of warfare and thus aggression (p. 92). These ideas are expanded upon by Libicki a decade later in his influential 2009 monograph "Cyberdeterrence and Cyberwar." Within this work, Libicki examines whether cyberdeterrence, or the disincentivizing of cyberattacks using tactics of punishment or denial, can be an effective policy approach to mitigate cyberthreats (p. 7-8). However, to do so, he notes that he also needs to explore what aggression in the cyber domain is. Thus Libicki proposes several overarching definitions of cyberattacks, aggression in cyberspace, and war in cyberspace, which have all been heavily cited by latter scholars.

First, Libicki defines 'cyberattack' as "the deliberate disruption or corruption by one state of a system of interest to another state" (p. 23). However, it should be noted that this definitional framework does not immediately presume that a cyber act is or can be equivalent to an act of war in more traditional domains. In fact, Libicki acknowledges that for the most part, cyber acts exist on a level of belligerence below physical force, yet above diplomatic and economic responses. This can be seen in Figure 1 (Libicki, 2009, pp. 28-29). Second, Libicki distinguishes between two potential types of cyberwar: strategic cyberwar, defined as "A campaign of cyberattacks launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior" (p. 117); and operational cyberwar, defined as "wartime cyberattacks against military targets

and military-related civilian targets." (p. 139). However, for both these influential definitions, Libicki remains hesitant to adopt an alarmist voice about the threat of strategic or operational cyberwar.

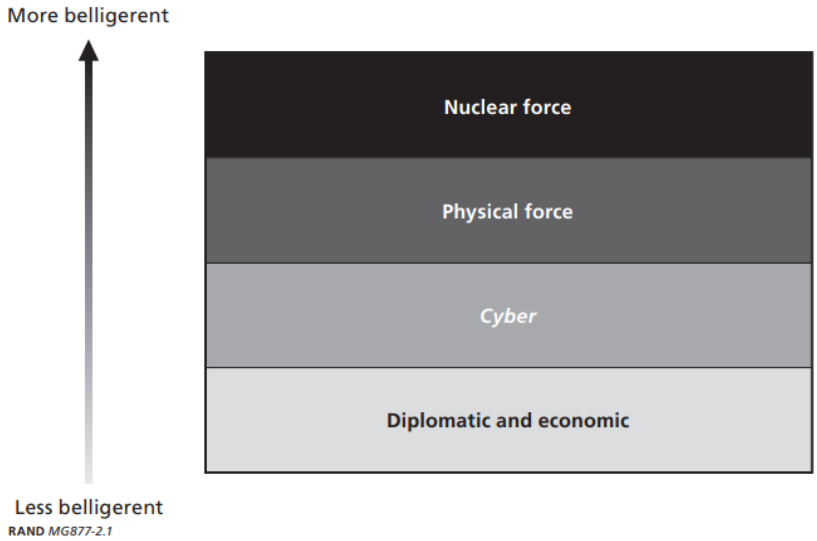

Figure 1: Responses by Rough Order of the Level of Belligerence

Libicki was not alone in approaching the concept of cyber war with some hesitation about its real-world applicability. Others, notably Thomas Rid in the early 2010s, were even more outright vocal about their disdain for the concept. Rid published in 2012 the article "Cyber War Will Not Take Place," which was later expanded into a 2013 book of the same name. Rid's work is summarized well by its central thesis, which argues:

> "Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage. That is improbable to change in the years ahead." (Rid, 2012, p. 6).

Rid develops this argument through comparing characteristics of cyberattacks and cyberconflict in 2012 to traditional definitions of war. In particular, he focuses on Clausewitzian thought, arguing that in order for something to qualify as an act of war, it must be violent, instrumental, and political (p. 7-9). Thus, Rid argues that "If the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria. But more than that, there are very few cyber attacks in history that meet only one of these criteria." (p. 10).

Rid's argument has met substantial pushback from fellow scholars. In 2013, John Stone wrote a response specifically to Rid, titled "Cyber War *Will* Take Place!" Herein, he argues that while Rid can use Clausewitzian ideas characterizing war as an act of force, Rid focuses too much on achieving these effects by focusing on lethality. As Stone notes specifically on Rid's category of sabotage, "Rid's distinction between war and sabotage rests solely on matters of targeting: war involves killing people, sabotage involves breaking things; war involves lethality, sabotage does not." (p. 106) This is an issue for Stone: he believes that an act of war does not require lethality to be present. As Stone concludes, "cyber war is possible in the sense that cyber attacks could constitute acts of war," and "Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character" (p. 107). Thus, for Stone, cyberattacks can and should be considered acts of war not because they are lethal, but rather because a non-lethal act can still meet Clausewitz's three characteristics of war (i.e. war must be violent, instrumental and political). This argument is compelling: it maps well onto contemporary views on cyber.

However, it is perhaps best to leave this debate on the note that while it is an interesting one to follow, many academics are growing increasingly frustrated with it. As Myriam Dunn-Cavelty, another leading expert on cyberspace, wrote in a special 2018 review of Rid's book "Cyber War Will Not Take Place," arguments like Rid's show more how "pointless this debate has become" in contemporary discussions on cybersecurity (p. 132). Namely, using the terminology of Libicki explored above, she states simply that "There is ample evidence that operational cyber-war […] has been a reality for many years, whereas strategic cyber-war is a mere thought construct. Indeed, no real expert takes stand-alone cyber-war scenarios seriously anymore – and it is even debatable whether they ever had as much of a mobilizing power as it is often claimed." (p. 132). Policymakers and experts today concern themselves less with the grand idea of 'cyberwar', but rather instead with how malicious state-level behaviour and aggression in cyberspace affects foreign policy and domestic goals. In this sense, strategic planners and

policymakers today accept that cyber aggression is real: however, the threat of a 'cyberwar' may be overstated and not practical to work with.

So, to briefly return to what should be a guiding question in this literature review: what is aggression in cyberspace? To summarize, there are two aspects of note. First, while it is currently not extremely applicable to cyber policy, a 'cyberwar' or 'cyber pearl harbour' type of incident would likely be aggression since it would carry effects similar to traditional conflict. Second, policymakers today are primarily concerned with the malicious uses of ICT technology by states, which is increasingly being considered to be akin to traditional views of aggression.

Cyberconflict in 2021

While there has never been a cyberwar, it is undeniable that states frequently conduct or are the victim or cyber operations: a trend that has only been growing in the past years. These operations, frequently falling into categories such as espionage, ransomware, sabotage, election interference, misinformation campaigns, and attacks on critical infrastructure, can pose legitimate threats to states and their populations. Often, these attacks occur in a 'grey zone of conflict' or use 'hybrid warfare tactics,' where states abuse clandestine behaviour to achieve strategic gains (Faesen et al., 2019). The nature of cyber conflict, particularly the wide proliferation of technology, easy access to such technology to a variety of actors, and technical difficulties with attribution (Sheldon, 2011), has made cyberattacks and cyberoperations a frequent feature of modern hybrid conflict. These trends have been influential in the past months and years: the headline-capturing cyber events of last year (the Colonial Pipeline attack, the SolarWinds hack, increased ransomware under COVID-19, etc.) have all been attributed as the work of a variety of APT groups. So, how has the West been responding to such challenges?

Response 1: Diplomacy

As the nature of cyberthreats facing states has become more defined, international efforts to address this behaviour via diplomatic means also evolved and has been becoming increasingly relevant. Most prominently, two ongoing United Nations processes called the UN Open-Ended Working Group (UN OEWG) and the UN Groups of Governmental Experts (UN GGE) regularly bring together national, industry, and civil society representatives from around the world to discuss what is acceptable state behaviour in cyberspace (Digwatch, 2021). These processes paint an appealing picture of what modern cyber diplomacy is and should look like. One key success would be the recent March 2021 UN OEWG *Final Substantive Report*, agreed to in a body including representatives from both the West and their traditional rivals including Russia and China. This report contained a number of affirmations, in particular outlining the role of international law in cyberspace, as well as what responsible state use of ICTs should look like (UN OEWG, 2021).

While these successes are certainly substantial, it should be noted that many still see normative and diplomatic processes as troubled. The UN GGE *Final Substantive Report* was significant because it featured positive contributions from traditionally absent actors like Russia and China: but it is still anyone's guess whether their contributions are but mere rhetoric. Similar issues plague the initiatives promoting cyber norms, where there exist examples of agreed-upon cybernorms, such as the 2015 U.S.-China agreement to stop IP theft, failing years later (Faesen et al., 2020, pp. 93-94).

Response 2: Offense

While cyber diplomacy is one pathway towards addressing contemporary threats facing the West in cyberspace, the other route that is embarking on a strategy of engagement, where states use military cyber operations to respond to, or pre-emptively deter, malicious cyber behaviour. Notably, the United States has pushed this agenda the furthest. This was especially thrust into public attention in 2018 when USCYBERCOM unveiled their new doctrine of "persistent engagement," which called upon the US to

"increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage" (USCYBERCOM, 2018, p. 4). This new Trump-era Persistent Engagement doctrine removed previous restraints and greatly increased the ability for USCYBERCOM to conduct offensive operations (Valeriano and Jensen, 2018, p. 4). This shift towards a more aggressive cyber stance is frequently linked to the ideas of deterrence and cyberdeterrence, where states need to demonstrate their abilities to ward off attacks or malicious behaviour from rivals.

As the dominant Western hegemon, if the U.S. goes somewhere, others will follow. Many American allies have been adopting offensive cyber capabilities and cyberdeterrence doctrines prominently in the past few years. For example, in 2020, the UK announced the creation of the National Cyber Force (NCF), specifically built to conduct offensive cyber operations against a variety of state, terrorist, and criminal actors (Steed, 2021). France was even earlier in this shift, having unveiled a doctrine for offensive cyber operations in January 2018, corresponding with large increases in funding and size for their cyber units (Laudrain, 2018). NATO has also been very active on the offensive cyber operations front, recently creating a cyberspace operations centre in Belgium and launching new units to coordinate the alliance's deterrence efforts in this domain (NATO, 2021). This enthusiasm by the "big actors" is also pulling smaller states to develop offensive cyber capabilities: as Alexander Klimburg wrote in 2020, "Instead of depending on the protective umbrella of their friends, many now have their own budding deterrence-by-punishment capability in the cyber domain, in addition to having become better able to resist the effects of a strategic cyber strike against themselves […] Any country not carrying out cyber attacks would, like those that did not test nuclear bombs, be excluded from the main table and left without a voice" (pp. 119-120).

It is within this identified offensive trend that this thesis finds its niche. While cyber diplomacy is evolving and can offer solutions, many Western actors seem determined that offensive cyber

capabilities are more necessary today than ever before. However, it is also clear that cyber operations can have effects on par with traditional military operations. Thus, questions should be asked about whether it is right – or just – for the West to resort to these measures. When Western actors have been using these offensive capabilities, does it abide to our conceptions of justice? How much do they do so, and where do the lapses lie? Thus, as will be justified in the methodology section, the Just War Theory (JWT) tradition can be a potent lens to examine contemporary behaviour by Western states in cyberspace and answer these questions. Before moving on to the exploration of JWT, it may be useful to first look at whether other scholars have also looked at the intersection of JWT and offensive cyber operations.

JWT in Cyber

Back in the early days of cyber emerging as a field of study from the late 1990s to the late 2000s, there was relatively little focus on it from JWT scholars. There is even one 2010 paper, "The Ethics of Cyberwarfare" by Randall Dipert, which makes the rather ambitious claim that it is only the third paper discussing cyberwarfare and ethics (p. 394). Many of these earlier papers proceeded in a similar fashion: looking at several of the principles of either *Jus ad bellum* or *jus in bello* and trying to see whether cyber conflict fit. Many of these papers had significant difficulties with this project. Consider Dipert, and his self-proclaimed 'third paper ever' on JWT and cyberwarfare. Most of this paper focused on the *Jus ad bellum* principle of Just Cause, which he argues is muddied significantly in cyberconflict (p. 395). As such, Dipert writes that a cyberattack more resembles a *casus belli*, which encompasses intrastate aggression like embargos, blockades, and harassment of citizens (p. 396). Yet Dipert notes that such aggression is typically neglected from JWT research, and thus not much help in situating Just Cause following a cyberattack. Ultimately, Dipert concludes that cyber power simply is too different from traditional powers to fit comfortably into a JWT lens. Other authors also had similar difficulties. Marco Roscini, in his 2010 paper "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force," notes that "there still

does not seem to be enough research on how the existing rules on the use of force apply, if at all, to cyber attacks" (p. 90). Throughout the remainder of the article, he especially notes that issues like anonymity and asymmetric capabilities in cyber posed legitimate difficulties to applying JWT principles such as Just Cause and Proportionality.

However, this pessimism was not shared by all authors – and, as the field of cyber has evolved and become better understood, more scholars began to note that JWT was a viable tool to analyze conflict in cyberspace. This shift is especially seen in Brian Orend's influential 2013 book "The Morality of War" wherein Orend dedicates a half chapter to analyzing the cyber operations using JWT (p. 153-184). Ultimately, he is able to map much of his JWT interpretation to cyber conflict, concluding the chapter by writing "After discovering the nature of (and cases) of […] cyber-warfare, argument was made that a just war analysis of both situations can offer action-guiding rules which are both plausible and principled." (p. 181). Other authors around this time also began viewing the relation between cyber and JWT more optimistically, such as Reese Nguyen, whose 2013 paper "Navigating Jus Ad Bellum in the Age of Cyber Warfare." Herein, he argues that cyber that while cyber poses unique difficulties for JWT, it is valuable to map behaviour in cyberspace to principled rules of behaviour. Others have built upon these works to offer more explicit guidance: including Christopher Finlay in his 2018 paper "Just War, Cyber War, and the Concept of Violence." Finlay writes: "If Violent Cyber-Attacks have the features of violence, as I define it, then they will also have the normative features associated with the concept of violence. Therefore, all else being equal, they can be treated in ethics the same way other cases of violence are—including kinetic violence" (p. 374). Doing this allows him to claim that JWT can then be applied to cyberattacks and similar operations.

However, scholars are not the only ones applying JWT to cyberspace. Notably, in recent years, various agreements and documents produced by state-level actors which reinforce the applicability of JWT to the cyber domain. Key among these are the *Tallinn Manuals* (both the original, published in

2013, and 2.0, published in 2017) (Schmitt, 2013; Schmitt, 2017). These documents outline specifically how *jus ad bellum* and international law principles should apply to cyberspace; and have been consequently very influential in state-level cyber diplomacy initiatives, such as the UN GGE processes. However, it should be noted that these documents are academic and non-binding in nature.

Given these trends, it should be clear that cyber is a domain whose operations can be analyzed via JWT, and doing so is a needed and relevant pursuit. This is especially due to both the increasing cyber capacities being built up by Western states, as well as the changing technological capabilities of states. However, the existing research does expose a few trends which also expose a niche where the research question of this thesis can fit in.

First, it is clear that cyberspace is a field which is rapidly changing. After all, the dominant research in the field went from a conclusion that JWT and cyber are largely incompatible to, less than 10 years later, documents like the *Tallinn Manual* emerging which seek to guide responsible state behaviour using explicit JWT thinking. In addition, a variety of governments have, over the past few years, released documents outlining their perspectives on the responsible use of cyberspace which both specifically and implicitly refer to JWT thinking and principles.[1]

Second, most prior scholars have focused on proving that cyber operations can and should be analyzed via JWT principles via largely theoretical terms. In doing so, they tend to use only a select number of notable cyber operations as case studies to support their principles. As such, no analysed studies were found which approach this subject from the opposite direction: i.e., looking at a broad range of case studies and then analysing how, if at all, they abide JWT principles and the lessons which that demonstrates. This is not an unexplored idea in the larger, parent field of JWT studies. One such

[1] Examples include New Zealand, the UK, Switzerland, and Australia. Many of these statements emerged as part of the OEWG talks, which called for states to voluntarily outline what they saw as the application of international law to cyberspace.

study was conducted by Walter Dorn, David Mandell, and Ryan Cross in 2014, titled "How Just Were America's Wars? A Survey of Experts Using a Just War Index." Herein, they first defined a set of JWT principles. Second, they then analyzed every major conflict America had been involved in to determine trends for both America and JWT in general. Such an approach would be especially valuable for cyber as Western states seek to expand their offensive cyber capabilities.

Literature Review Conclusion

This literature review has proceeded in three distinct sections, each containing several relevant insights which help isolate the need and value of this thesis's research question and focus. First, it was shown that aggression has been a long-studied and debated concept in cyberspace, particularly in the study of cyberwar. Ultimately while the debate on 'cyberwar' is important, it has less practical relevance to policymakers dealing with aggression in cyberspace, who prefer to focus on malicious behaviour. Second, this literature review set the scene of offensive operations in 2021. Here, it was identified that the increasing prominence of cyber deterrence and offensive cyber operations is worrying, and there is a role for observers to analyze whether such offensive operations are just or right. In this gap, the thesis question become pressing. Third, this literature conducted a review of prior attempts to analyze cyber operations using a JWT lens. This unveiled two key areas which this thesis can feasibly address: (a) updating prior research on JWT principles with new knowledge on cyberspace; and (b) a gap where there is no broad comparison between all Western cyber operations to determine whether their overall postures were in alignment with JWT concepts. Collectively, doing these two steps can supply an interesting and relevant addition to existing research on offensive cyber operations.

Chapter 3: Methodology and Data Selection

This chapter does three things: first, it identifies and determines both the theoretical lens and the methodological design used in this thesis. Second, it selects and justifies the relevant data sets that will be used. Third, this chapter justifies some research limitations.

Theoretical Lens and Methodology

This thesis focuses on analyzing the trend of offensive operations in cyberspace, seeking to explore how just this trend is. To do so, a clear theoretical lens is needed to guide this discussion and establish a framework to be used. As introduced briefly in the literature review, Just War Theory can apply this lens. As scholars have pointed out, while JWT is not perfect, given the lack of authoritative international legal agreements governing cyberspace, it may be the most potent lens available today to determine the ethics of entering cyberconflict (Thumfort, 2020, p. 2). This observation is supported by evidence presented in the literature review of JWT being used prominently on the international cyber stage.

So, what is JWT? JWT, in a nutshell, exists to determine both when it is right to use aggression, as well as how much aggression is acceptable to use. These are important questions: humanity has always been embroiled in conflict and war, so establishing rules for responsible, or just, behaviour is of tremendous importance. In this regard, JWT as known today has proven to be remarkably influential, serving as the undisputed cornerstone behind famous international agreements such as the Geneva Convention (Orend, 2013, pp. 4-5). Most modern interpretations of JWT draw the most from the work of Michael Walzer and his influential 1977 book *Just and Unjust Wars*. Therefore, the primary work used as a starting point for JWT in this thesis will be work of Brian Orend, a Canadian political philosopher, drawing primarily from his book *On War* and several publications. Orend's interpretation of JWT is based very heavily off Walzer's work, and proposes six principles to determine *Jus ad bellum*, seen in Figure (see Figure 2). Orend also stipulates that in order for a conflict to be just, all these six principles should

be met. This is, as Orend himself admits, a high bar to clear: but one he deems necessary considering the heavy nature of conflict. For the purposes of this thesis, this is also an acceptable stipulation: after all, the focus is to see what needs to be done to make cyber conflicts just, which requires a detailed examination of what principles modern cyber conflict struggles to deal with.

Principle	Explanation
Just Cause	To resort to violence, the state must be a victim of aggression, or come to the aid of a victim of aggression.
Right Intention	There should be no perverse incentives behind the resort to violence even if Just Cause does exist.
Public Declaration by Proper Authority	Violence should be publicly disclosed by a proper authority in a reasonable timeframe.
Last Resort	Violence should be only resorted to when all other reasonable options are exhausted.
Probability of Success	The violence should not be futile and have a reasonable chance of success.
Proportionality	The benefit of the violence should outweigh all other options, including taking no action.

Figure 2: Orend's Six Principles

In this thesis, Orend's six principles will be used to evaluate the selected cyber operations: but, first, it should be explained how these principles are relevant and applicable to acts in cyberspace. This will be done in Chapter 4; where each principle will be individually introduced and explored how they are applicable to acts in cyberspace. The methodological approach used for this chapter will be inductive process tracing. Inductive process tracing is a subgenre of process tracing, and relies on using identifying causal mechanisms between cases to establish theory (Trampusch and Palier, 2016, p. 439). This is an ideal pathway for this portion of this thesis since inductive process tracing is often used as a theory constructing form of process tracing; and this portion aims to test how existing JWT principles are relevant in today's environment. Ultimately, this will allow each subchapter in Chapter 4 to propose how a JWT principle is applicable in cyberspace.

Before moving on to the literature review, one key critique of the usage of JWT for cyber should be examined. Namely, JWT is typically a theory of warfare. However, there has not been a 'cyberwar', or even an offensive cyber operation commonly accepted as an act of war. At most, many of these acts are only aggression below the level of warfare. Thus, can JWT feasibly provide a lens to analyze contemporary Western cyber operations, especially those not considered acts of war? There are two ways to answer this critique:

First, it could be argued that in the cyber domain it is difficult to establish what is an act of war in the first place, and a variety of cyber acts are actually acts of war. Libicki notes this. He explains that unlike traditional physical force, there are no universally accepted definitions of what an act of war in cyberspace is. Thus, the duty is left up to individual states to declare cyber activity as an act of war. However, this is plagued by two key issues: first, the international community must collectively accept that designation as legitimate; and second, the victim state may (for variety of reasons) be dissuaded from calling a cyberattack an act of war (2009, pp. 179-181).[2] Thus, it should not be surprising that there have not been any 'official' acts of warfare in cyberspace. However, this does not mean that acts of aggression in cyberspace today may not, under other circumstances, be called acts of war. For example, while there is no academic consensus on this, operations like Stuxnet are convincingly argued by some to be an act of war (Singer, 2015). Thus, JWT may have a much wider application in cyberspace than initially appears: after all, there are obvious issues with asking states to define what an act of war is, and then limiting JWT to only cover those incidents. However, this thesis will not take this path, as it requires an in-depth case study for each incident: something not able to be delivered within the word constraints of this thesis.

[2] A non-exhaustive set of reasons can include hypocrisy, loss of reputation, diplomatic costs, and admission of weakness.

The second path would be to argue that the concept of aggression within JWT should be expanded to not only include acts of war, but also certain forms of cyber activity. This is a path taken by most JWT scholars exploring this issue: as shown in the literature review, many JWT scholars justify expanding the JWT framework to cyber aggression which technically falls below the threshold of warfare by arguing that the framework of aggression or violence behind JWT should be expanded. This is often justified by referring to the evolving nature of conflict and the unique characteristics of the cyber domain (Finlay, 2018, pp. 358-359; Orend, 2013, pp. 176-177). This thesis takes this position, arguing that the concept of violence should, and can reasonably be, expanded to incorporate a variety of behaviours in cyberspace. In specific, this would include acts of sabotage and destruction, as well as acts targeting electoral and critical infrastructure. This position is argued for and defined in the first subchapter of the next chapter; given the significance of this debate for the JWT principle of Just Cause.

Data selection

After having justified the JWT principles that will form the units of comparison, the data of modern cyber conflicts should be justified. Despite the notoriety of cyber operations and the almost daily discovery of new attacks from a variety of actors, databases collecting cyber operations are not as common as one may expect. In fact, only two databases of note emerge: The Council on Foreign Relations (CFR), who run a Cyber Operations Tracker (CFR, 2021); and a private dataset compiled by Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen called the Dyadic Cyber Incident and Dispute Data (Maness et al., 2021). This project will focus on using the data from the CFR dataset. This is for two primary reasons. First, it is by far the most reputable set. Over the years, it has grown to enjoy a significant status in the cyber community, often serving as the backbone for many other studies. Second, they are frequently updated with recent incidents and draw from a variety of datasets and databases. These incidents are also able to be filtered alongside a variety of categories.

Thus, the data collection done in Appendix A will apply the data on contemporary cyber conflict from the CFR cyber operations tracker. As mentioned, the CFR tracker sorts collected cyber operations into several categories. Of these, three are selected for this thesis to focus on: Sabotage (referring to "The use of malware that causes a disruption to a physical process"), Data destruction (referring to "The use of malicious software to destroy data on a computer or to render a computer inoperable"), and Distributed Denial of Service (referring to "The intentional paralyzing of a computer network by flooding it with data sent simultaneously from many individual computers") (CFR, 2021). These categories were chosen because they contain the clearest links to aggression in cyberspace and have the greatest and clearest potential to cause physical damage. Moreover, these are all behaviours that see condemnation in numerous contemporary agreements on state behaviour in cyberspace. The remaining categories (Espionage, Defacement, Doxing, and Financial Theft) are frequently not included in such agreements, and often have unclear connections to aggression.

Research Limitations

Given this research design, there are three key limitations to this project that should be mentioned:

Focus on Jus Ad Bellum*.* To be very explicit, this thesis will focus only on the *Jus Ad Bellum* principles of JWT: that is, the principles commonly understood as justice in entering conflict. The JWT principles of *Jus in Bello* (justice in conflict) and the occasionally included principle of *Jus ex Bello* (justice after war) are not included within this thesis and analysis. Including them were deemed to expand the scope too far; but are potent areas for future research.

Focus on Western States. This thesis focuses explicitly on the behaviour of states, and not non-state entities. There are two points to make about the scope of this thesis:

First, this thesis focuses primarily on the behaviour of Western states (which will be reasonably defined as NATO members and their strategic allies, most prominently Israel). This limitation exists for several reasons. Western states have been traditionally much more willing to present an image that whatever cyber operations they do launch should be just. Consider states like China, who officially do not claim to have any offensive cyber capabilities to begin with. Additionally, confining this focus allow the final observations and lessons to be more insightful in terms of policy implications for Western states. Finally, this limitation seeks to contain the scope of this thesis: while this research question is theoretically able to accommodate such an expansion, the word limit for the thesis would not be able to.

Second, a state-based focus, while ideal for this thesis, is not always ideal for the cyber domain in general. Notably, unlike traditional domains, much of the infrastructure of the internet is in private hands, which often necessitates the involvement of wide range of non-state actors and has led to the popularization of a mulitstakeholder model of governance in cyber diplomacy (Faesen et al., 2019). Thus, using a state-centric framework such as JWT can potentially ignore these additional, relevant, non-state actors. This ignorance can be justified here by pointing out that most offensive cyber operations are launched by states, and, since this thesis focuses on *Jus ad bellum*, the launcher is the prime focus. However, this is a trend that may change in the coming years: private corporations such as Microsoft are increasingly dabbling with the legality and practicality of conducting their own offensive operations against threat groups (Broeders, 2021, p. 6). While this is an emerging research field, it could be an interesting extension of the conclusions this thesis will hopefully determine. At the very least, the conclusions need to sympathetic towards the inherently private nature of the Western internet and the associated non-state actors.

Third, it should be noted that while this thesis focuses on Western states, several cyber operations from the dataset deal with Western responses to non-state behaviour (such as certain botnet takedowns and terrorist groups). These were kept in the analysis since the application of force was by the military branches of Western states, and thus constituted military operations. There is a risk that these operations were more readily disclosed by governments due to their largely successful nature (thus serving more as a boast or show of power of Western cyber power); however, this is deemed an acceptable risk as these operations could still demonstrate how JWT should be present in cyber operations.

No espionage. As mentioned, this thesis will not be focusing on certain cyber behaviours, such as vandalism, financial crimes, and espionage. The main category whose exclusion should be explicitly justified is espionage. First, as discussed briefly in the literature review, espionage using cyber capabilities is almost always excluded as a form of aggression. This comes primarily as no Western state is willing to do so given the hypocrisy which would ensue. Second, espionage in general is typically excluded from JWT: even when dealing with traditional aggression, something which Brian Orend stresses in his work on JWT (Orend, 2013).

Chapter 4: The Principles of *Jus Ad Bellum* in Cyberspace

Given this research design, this chapter will rely upon Orend's identification of the six principles of *Jus Ad Bellum*, and accordingly identify and argue how they can be applied to cyber operations. This should answer this thesis's first sub-question, "How can JWT be applied to cyber conflict?" This answer will then form the theoretical basis for the metrics used in Chapter 5.

Just Cause

JWT Principle

While the principle of Just Cause is typically the first principle of JWT listed – perhaps implicitly conveying that most theorists also consider it the most important principle – it is far from the most straightforward or the least contentious. To summarize, Just Cause deals with when it is 'just' to launch an attack on another state. After all, given the risk of destruction, death, and other such ethically unscrupulous aspects of warfare, it is quite evident that states should not simply attack each other. According to Orend, Just Cause in modern JWT consists of three main conditions which a state must fulfill in order to justly resort to using violence: (2013, pp. 35-42).

1. *It is the victim of aggression or is coming to the aid of a victim of aggression*. This aggression is usually interpreted to not just be some serious wrong against a state, but also traditional contain a serious, physical direct force against a state or its people.
2. *It is a minimally just or legitimate state*. This means they (a) are a recognized state by both their own citizens and the international community, (b) avoid violating the rights of other states, and (c) they make every reasonable effort to uphold human rights for their citizens.
3. *The state's resort to violence fulfills all aspects of the Core Principle of Aggression (CPA)*. Orend argues that the CPA states that the use of aggression by any aggressor entitles the victim to use of all means necessary, including lethal force, to stop them. This is, however, still constrained by *Jus in bello* principles.

In this regard, the "gold standard" of Just Cause would be a "kinetic physical attack, usually involving some kind of armed invasion across a border" (Orend, 2013, p. 176).

Just Cause in Cyber

However, this "gold standard" is hard to apply to cyberspace, largely because the concept of aggression in cyberspace is considered by many to be different than in traditional conflict. Simply put, the equivalent of launching a missile or invasion in cyberspace is often not accompanied with the same

direct physical damages. Cyber operations instead tend to aim to produce effects which fall into categories of subversion, sabotage, or espionage, as opposed to traditional effects like destruction and invasion (Rid, 2013, p. 15). This stems from the limitations in the inherent nature of cyber power, which, unlike traditional forms of power, cannot directly cause casualties (i.e. kill) or occupy territory (Steed, 2011, pp. 21-24). However, it should be noted that, for the most part, these are difficulties with the first condition that Orend identifies as part of Just Cause: the need to show that a state is a victim of aggression. So, what is aggression in cyberspace?

This question was examined in the literature review, with two conclusions being reached: first, there is a healthy, largely academic debate on whether or not 'cyberwar' is a valid term. Second, in the policy and strategic realm, the focus is very much on combatting the malicious use of cyberspace by states, often as part of hybrid campaigns or operations. So, can these be aggression, as defined by Orend in his first condition of Just Cause? There are two answers to be explored.

Cyberspace has direct, physical consequences.

Does cyberspace cause direct, physical consequences, such as traditional destruction of property or the loss of life, which closely mirror traditional conceptions of aggression? As explored within the literature review, scholars such as Arquilla, Ronfeldt, Rid, and Stone have long had conflicting views. Moving beyond their theoretical discussions, it is useful to look at reality today where states and individuals *actively do* see cyberattacks resulting in direct physical consequences which are very reminiscent of traditional, physical attacks. This can therefore be compatible with the traditional concept of aggression in Just Cause and JWT. A shortlist of prominent events can be easily be compiled which have had effects beyond simple criminal acts. For instance, there is a 1982 event where the CIA inserted code into the software of a Russian pipeline, which was then used to explode it resulting in, allegedly, a "3-kiloton blast" resulting in substantial destruction (Kettmann, 2004). Energy grids and similar critical

infrastructure, which are often the first targets in a conventional conflict, have also been attacked via cyber means: most prominently known are the frequent Russian intrusions and meddling in the Ukrainian power grid throughout the latter half of the 2010s (Greenberg, 2017), but China has also been accused of similar attacks in 2021 with their targeting of the Indian power grid (Sanger and Schmall, 2021). Even the infamous Stuxnet attack can be argued to be an example of a physically destructive attack, with some calling it the 'first kinetic cyber attack' (Singer, 2015, pp. 79-86).

Adding to this, many states have signalled that they view cyberattacks as having the possibility to warrant escalation; meaning they view cyber as having the capability and potential to cause substantial levels of physical destruction. Consider the March 2021 United Kingdom *Integrated Review of Security, Defence, Development and Foreign Policy*. Herein, they state that emerging technologies, such as cyber, can be destructive enough to warrant escalation up to the nuclear level (Jay, 2021). Other states and international bodies have vocalized these ideas more explicitly; most prominently being NATO, where Jens Stoltenberg, secretary-general of NATO, vocalized in 2015 that "NATO has made it clear that cyber-attacks can potentially trigger an Article 5 response" (NATO, 2015). There also exist demonstrated incidents where states responded to incidents in cyberspace using physical means, such as the US drone strikes targeting ISIS cyber operations in 2015 (Williams, 2015) and Israel using missile strikes to take out Hamas cyber operatives in May 2019 (O'Flaherty, 2019).

Thus, it should be clear that given the potential of cyberattacks, there can be instances where a cyberattack can directly threaten or cause substantial destruction, loss of life, or other effects on par or greater than conventional attacks – thus then forming Just Cause for the proportional use of offensive cyber operations.

The Concept of Aggression in Cyberspace Should be Expanded

As noted earlier, the traditional concept of aggression struggles to accommodate cyber behaviour: but perhaps the concept of 'aggression' itself is to blame rather than cyber itself. Perhaps cyber introduces new phenomena which 'aggression' as a concept cannot accommodate. This has been noted by several scholars: for instance, Orend argues, given the "new and pervasive" role computer and digital technologies play in everyday lives, it may be necessary to amplify and expand what is currently perceived as aggression to accommodate contemporary cyber behaviour (Orend, 2013, pp. 176-177). In this light, as society's reliance on digital technologies has only increased, a number of international forums emerged noting that these technological shifts require us to define what is and is not responsible state behaviour in cyberspace. These negotiations have often been spurred on by key incidents where traditional concepts, such as what is "aggression" or "attack", fails to successfully accommodate new, obviously malicious behaviour. While slow, there have been some successes in proposing norms which detail specific, novel limitations on what acceptable state behaviour is in cyberspace.

Most prominently, two ongoing United Nations processes called the UN Open-Ended Working Group (UN OEWG) and the UN Groups of Governmental Experts (UN GGE) regularly bring together national, industry, and civil society representatives from around the world to discuss what is acceptable state behaviour in cyberspace (Digwatch, 2021). One key success would be the recent March 2021 UN OEWG *Final Substantive Report*, agreed to in a body including representatives from both the West and their traditional rivals including Russia and China. This report notes both the real and increasing threats to states from cyber operations. One particular focal point of this report, and the discussions leading up to it, is the impact of cyber operations being conducted against a state's critical infrastructure. This includes sectors like electricity, power, and emergency services, and is often expanded to also include health care. Simply put, critical infrastructure is whatever is needed to run a state – which is nowadays often dependent on digital systems which can be targeted by a variety of cyber operations. Taking down these services and systems can result in dramatic implications for citizens: something the OEWG report

notes, writing about the potentially "devastating security, economic, social and humanitarian consequences" arising from targeting critical infrastructure. Based on these dangers, they ultimately recommend that "States should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." (UN OEWG, 2021, p. 5).

The UN OEWG is not alone in noting that contemporary discussions of cyberspace need to condemn attacks on critical infrastructure given the largely and potentially destructive impacts of targeting this sector. Several international initiatives have been proposing norms in cyberspace on this topic for years now. Most notable are the 2018 Paris Call and the 2019 Final Report of the Global Commission on the Stability of Cyberspace (GCSC) (Paris Call, 2021; GCSC, 2019). Both movements propose a set of norms or principles for responsible behaviour in cyberspace, and both have achieved substantial support in the international community.

Given these trends in recent cyber diplomacy, clearer boundaries are emerging of what is and is not acceptable state behaviour in cyberspace. Much of these discussions are based off the danger that a misuse of cyber operations can cause: for instance, attacks on critical infrastructure has real destructive and deadly consequences for citizens. Similarly, operations targeting electoral infrastructure and processes threaten the basic ability of a country to practice their rights to sovereignty and non-intervention.

So, for the purposes of this thesis, it is argues that Just Cause in cyberspace follows the same three basic elements proposed by Orend earlier in this subchapter. However, two explanatory points should be made:

First, some cyber operations or attacks can cause physical affects to the same extent as traditional means of warfare.

Second, due largely to the nature of cyber power, aggression in cyberspace can credibly be extended to also encompass attacks on critical infrastructure or electoral infrastructure and processes; where even if there is an absence of the direct violence or destruction typically associated with 'aggression', the nature and consensus about these targets do allow for Just Cause to be present.

Right Intention

JWT Principle

As noted from JWT scholars tracing back to Aquinas, Augustine, and Kant, just because you may have Just Cause to enter a conflict, it does not mean that 'anything goes' (Purves and Jenkins, 2016, p. 20). Simply, a Just Cause can be pursued through wrong intentions. This is where Right Intention exists, often as a partial extension of the principle of Just Cause. It states that a state needs not only the proper justification for resorting to aggression, but also the right intentions behind taking action. Too often there appear to be incentives behind conflict such as economic motivations, strategic gains, imperialist ambitions, or even xenophobia or racism existing alongside Just Cause as a factor for the resort to aggression – something that should not, for a just conflict, calculate into the decision making.

Since Right Intention deals with understanding the motivations behind a state's actions, this principle can often be very vague or subjective in practice. But some scholars have proposed some rough indicators to see if Right Intention is present. For instance, Orend builds off ideas first proposed by Emmanuel Kant that states should commit credibly to rules of conduct within warfare, with a specific emphasis on conflict resolution. This would include international commitments like the Geneva convention, and would therefore hold states against standards that they would only enter conflicts with proper intentions respecting JWT principles (Orend, 2013, pp. 50-51). Second, other scholars also

advocate that states should either publicly plan or 'call their shot' when resorting to violence (Purves and Jenkins, 2016, p. 23). This means that states should not only publicly declare their intention to enter a conflict, but also publicly state their plans and end goals. If states demonstrate such indicators in their rhetoric and actions before entering conflict, it can more credibly signal that they are action with Right Intention, helping guard against mission creep or secondary or ulterior motives creeping into play.

Right Intention and Cyber

The relationship between Right Intention and cyber is relatively straightforward. Since Right Intention deals with intentions and motivations, it should map onto cyber power and cyber conflict in the same manner it does as with traditional conflict: simply put, when conducting an offensive cyber operation, the actor must approach it with the proper intentions of primarily abiding by the identified Just Cause. Likewise, Right Intention in cyber still has issues with subjectivity. A cyber operation can, like an operation in a traditional domain, still be used to accomplish alternative goals beyond the scope of the initial Just Cause.

Fueling this fear is the lack of effective indicators which states can use to signal their Right Intention in cyberspace. Both indicators identified above for traditional conflict are largely absent from modern cyber operations. First on the indicator of abiding by international conventions on warfare, it is commonly known that in cyberspace, there is no equivalent to the Geneva Convention: in fact, there are no internationally agreed upon rules for warfare or offensive operations in cyberspace. While documents like the *Tallinn Manual* do exist and do provide guidance for some Western states, it is not comparable to international law and conventions on regular warfare. Second, as will be highlighted in the next subsection on Public Declaration, most states struggle to currently even disclose cyber operations, much less engaging in practices like 'calling your shot.' However, this is not to say that these indicators cannot be present. Even if there are no binding international agreements governing cyber

operations, states can still actively take part in ongoing cyber diplomacy negotiations, and use such discussions as rationale for their actions. Additionally, states can also be publicly clear and transparent about the extent and rationale of any offensive cyber operations conducted.

For the purposes of this thesis, Right Intention in cyber will be deemed to be present if an actor conducts a cyber operations that (a) abides by the identified Just Cause[3], and (b) is rationally justified, ideally with reference to emerging international law as well as clearly limited in scope.

Public Declaration by Proper Authority

JWT Principle

Just War theorists agree that a key component of just conflict is ensuring that conflict or war is declared not only by a proper authority, but also publicly declared. This ensures that all sides of a conflict, as well as the public and bystanders, are sufficiently informed of the threats they face. In addition, this also ensures that the citizens are aware of the actions committed by their government. Often, for major conflicts and wars, this formalized is seen in an official note or declaration; but this can also be done through press statements, speeches, publicized votes, etc. (Orend, 2013, pp. 52-53).

Public Declaration in Cyber

Despite the relatively strong norms for Public Declaration in traditional conflict, in cyberspace, there rarely are such public declarations (Orend, 2013, p. 178). Why is this?

Some point to the difficulty with attributing cyber operations to states, thus making them attractive for states to use to clandestinely achieve strategic goals. This is different than in traditional conflict, where attribution is often difficult to avoid or hide. However, recently, this is being increasingly challenged though the rise in popularity of 'grey zone conflict' or 'hybrid warfare tactics,' where states

[3] As a side note, this also means that for the data collection, this thesis will only judge cases for Right Intention if Just Cause was first deemed to be present.

abuse clandestine behaviour to achieve strategic gains (Faesen et al., 2019). Cyberoperations have become a frequent and prominent form of power used in such operations, largely because of some of the perceived characteristics of cyber power which makes it easy to conduct anonymously; such as the wide proliferation of technology, easy access to such technology to a variety of actors, and technical difficulties with attribution (Sheldon, 2011).

However, despite these characteristics, the issue may be less the lack of attribution and more the lack of political will to take action to punish offenders and enforce a standard of Public Declaration in cyberspace. Notably, many contemporary sources on cyber power have long been hinting that technical attribution of cyberattacks, while still difficult, is possible for virtually all cyberattacks (Pritchard, 2019, p. 51). Even back in 2013, the head of the U.S. Cyber Command stated that "We feel confident that foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response" (Alexander, 2011). Despite these advances in attribution, most cyber operations see little response. Consider the 2020 SolarWinds hack by Russia against American systems which entered the American public's consciousness in late 2020. Despite the magnitude of this hack, the only real punishments faced by the Russian government were some sanctions and diplomatic expulsions (Greenberg, 2021). This is especially scary considering the often less than responsible usage of cyber capabilities by non-Western states, such as the 2017 NotPetya attacks launched initially against the Ukrainian banking sector (presumably by Russia) which quickly – and presumably unintentionally – spread beyond the region to globally cause over $10 billion in damages (Greenberg, 2018). Public Declaration should be upheld as a norm not only for informing citizens, but also for holding states accountable for any irresponsible use of cyber capabilities.

One final note that should be mentioned in the cases where Public Declaration is present, it often comes months or years following an operation. In short, some declaration is better than no

declaration: occasionally, some governments justify this by saying that doing Public Declaration right away can undermine their operations. However, if an unreasonable amount of time has passed, then this declaration should not be sufficient.

Ultimately, the JWT principle of Public Declaration by Proper Authority can – and should – be actively applied to cyberspace. Not only do citizens have a right to know of and approve of their government's behaviour in cyberspace, ignoring Public Declaration also allows all states – including states like Russia, China, and Iran – to be held to a lower standard of responsibility in making sure cyberattacks are limited in their impacts and effects.

Last Resort

JWT Principle

Walzer argues that force should never be a last resort: simply put, he believes that there should always be another option than violence, except in the rarest 'supreme emergencies' (Waler, 1977, p. 72; 251-255). Some modern JWT scholars, such as Eamon Aloyo, also abide by this school of thought, going as far as to argue that Last Resort as a principle should be "jettisoned" from the just war tradition since what matters morally is not whether there were no other options available, but rather the harms of the action itself (2015, p. 187). However, this remains, arguably, a minority view, with most JWT scholars retaining Last Resort as a key tenant of JWT. For instance, Orend writes that "It seems much more plausible to contend not that war be the literal last resort – after all other imaginable means have been totally exhausted – but, rather, that states ought not to be hasty in their resort to force" (Orend, 2013, p. 60). As such, this project will retain the view Last Resort as a part of JWT. And thus, building off definitions from authors like Orend, Last Resort here entails that the resort to violence or aggression should only be done when all other reasonable alternatives are exhausted or have failed (Orend, 2000, pp. 534-535). Finally, while Last Resort appears relatively simple, determining whether it exists is far from an exact science. In essence, it relies on a largely subjective appraisal of whether all options have,

in fact, been exhausted. Look only at the classic JWT case study of the Second World War, where people today still occasionally debate whether more appeasement could have been possible to avoid conflict.

Last Resort in Cyber

Overall, Last Resort is not a very difficult principle to apply to cyber: simply put, the use of force in the cyber domain should only be used when all other diplomatic and economic means have been exhausted. Many scholars investigating cyber and JWT actually only state that and leave the discussion here.[4] However, an issue that should be explored is that many states, including Western leaders, view offensive cyber operations not as a measure of last resort, but rather as a means to achieve quick strategic gains.

This comes largely as offensive cyber operations have been, and currently continue to be, frequently used by Western states to achieve strategic gains: one needs only to look at incidents like the infamous American usage of Stuxnet to compromise Iranian uranium refinement, where the usage of a computer virus to covertly 'first strike' cyberattack against a sovereign state was far from the last option available. Spurring on such a usage of cyber power are a host of advocates who see the unique characteristics of cyberspace, such as the low-cost nature, dominance of the offense and the low risk for escalation as ideal for achieving strategic gains against rivals (Sheldon, 2011). Brandon Valeriano and Benjamin Jensen examined these trends, and found that only 32% of the cyberoperations conducted by the United States ever saw a response by the victim: and even if a response is given, the response tends to be at a level lower than or equivalent to the American cyber operation (Valeriano and Jensen, 2019, p. 5). Such trends have helped motivate the U.S. to adopt a cyber policy of 'Persistent Engagement', where intrusions against the U.S. are met with equivalent cyberattacks, in theory establishing 'cyber deterrence' (p. 7). This even spills over into using cyber responses to potentially respond to conventional

[4] For instance, see Dipert, *The Ethics of Cyberwarfare* and Pritchard, *Is Just War Theory a Credible Tool*.

threats, with some advocating that escalation via cyber means is preferable to escalation via traditional military operation, with most of these advocates simply pointing to cyberattacks being, by nature, less destructive. However, this is a dangerous way of thinking: given our modern societies' ever-increasing reliance on cyber technologies (especially within our critical infrastructure), coupled with the continued general consensus among academics that in cyberspace offense still dominates defense (Sheldon, 2011), it seems to be tempting fate to openly advocate offensive cyber operations as a risk-free component of cyber defense.

In summary, Last Resort, like Public Declaration, is a much-ignored JWT principle in cyberspace – but that does not stop it from being relevant and applicable. States should only resort to the usage of offensive cyber operations when all lesser means, such as diplomatic and economic measures, have been fully exhausted.

Probability of Success

JWT Principle

The principle of Probability of Success tends to receive the least attention among the six JWT principles, as it is often fairly easy to understand. Simply put, this principle aims to prohibit violence that is known in advance to be futile. Along these lines, some formulate it to read as the war (or violence) is "sufficiently likely to achieve its aims" (Lazar, 2016). Despite the general consensus on this definition amongst JWT scholars, Probability of Success has two key weaknesses that are often explored: first, like with the principle of Right Intention, there is a certain amount of general vagueness or subjectivity surrounding the calculation of likelihood of success; and second, Probability of Success struggles with cases of extreme power asymmetry (Orend, 2013, p. 61). In response, most scholars argue to link Probability of Success very closely to an understanding of when decisionmakers can reasonably be confident of success (Harbour, 2011, p. 238). While this itself is still subject to concerns about subjectivity, as a general principle Probability of Success can be cogently identified in conflicts.

Relation to Cyber

In cyber conflict, as in traditional conflict or acts of violence, the aggressor should also ask themselves if their cyber operation is sufficiently likely to achieve its aims; and, if the answer is negative, refrain from launching such an offensive cyber operation. This plays out not too much differently in cyberspace as in traditional spheres of operation or combat.

However, it should be noted that responsible states are largely incentivized only to use sophisticated cyberweapons when their success is guaranteed. Cyberweapons developed by most Western states have a much higher level of sophistication and complexity. For instance, leading US cyber officials such as Eric Rosenbach describe offensive cyber activity as “painstaking work” that “involves identifying a platform in another country, gaining access, and then remaining undetected, often for years, inside the system” (Halpern, 2019). Moreover, these cyberweapons rely upon the exploitation of previously unknown flaws in the systems used by their targets. However, once a cyberweapon is used, it is then also able to be discovered – which allows security researchers to identify the flaws it uses and patch them. Thus, cyberweapons are often a ‘one-shot’ kind of deal, where a weapon which cost years and millions to develop can only be used in one operation. This incentives states to only use their most potent cyberweapons when they are absolutely sure it is both necessary to be used, or that the operation will succeed (Rowe, 2009).

Modern states must endeavour that the cyber operations they launch are likely to succeed: a bar that requires both the careful construction of cyber weapons to achieve their goals and the removal of the urge to use cyber operations as simply a demonstration of power.

Proportionality

JWT Principle

Proportionality dictates that states, before entering conflict, need to reflect on or calculate whether the negative effects of conflict outweigh all other potential options – including the option of taking no action at all and accepting the current state of affairs (Brown, 2003, pp. 173-174). This includes reflecting on whether the stated cause for conflict is valuable enough to justify the potential effects of action: above all, this means determining that the "unchecked triumph of aggression" is greater than the evils of war (Orend, 2013, p. 62). Using a colorful example, some summarize Proportionality with the statement that "if the other side stole your cow, you can't justifiably nuke their city" (Singer, 2015, p. 84).

It should also be noted that Proportionality suffers from an inherent subjectiveness since there is no adequate mathematics or equation that is accepted by modern philosophers which can calculate to determine if and when aggression is a proportionate response. Instead, the path forwards favoured by many modern philosophers is instead focusing on what is *not* a proportional response. Orend advocates this approach, eventually concluding that "Proportionality, at best, provides some checks and balances, some outside constraints, on the drive to secure a just cause. In other words – and with some irony – we know much better what disproportionality is than proportionality" (Orend, 2013, p. 63).

Proportionality in Cyber

Like any other form of conflict, there should be some expectation upon decisionmakers to be able to justify why an offensive cyber operation is a proportional response to their current situation. However, unlike more traditional forms of warfare, many policymakers tend to justify offensive cyber operations due to their lower risks of escalation or retaliation. This has a key implication on the Proportionality of cyber: namely, that many strategic thinkers and decisionmakers view cyber as type of force that is 'less dangerous' than traditional, more physical actions – leading to an offensive cyber response being more proportional or justifiably applicable to a large variety of phenomena. On the one hand, this can be positive *if* offensive cyber operations do avoid escalation and keep damages limited. After all, even if

cyberattacks have the potential to be destructive or lethal, this does not mean all of them have to be. However, on the other hand, the ability for states to do this is far from guaranteed (as examined in multiple places throughout this chapter). As noted earlier, some states, such as Russia, seem uncaring about the potential fallout from the indiscrete use of cyber weapons. Others, such as the West who do tend to take care to try to limit the impact of their cyber operations, seem to forget or conveniently ignore that cyberspace is only really governed by norms. But this use of offensive cyber power by the West – even if it is largely done responsibly – still normalizes this behaviour: something their rivals can lean on to justify their own less responsible cyber behaviour.

In general, scholars who attempt to study the relation of JWT Proportionality to cyber do struggle. Lloyd Pritchard looked at this subject in his work, ultimately concluding that a "broader revisionist definition of proportionality offers greater application to cyberwarfare but, in doing so, becomes susceptible to even more subjectivity and incommensurables" (Pritchard, 2019, p. 49). Thus, Orend's suggestion to look not at what is proportional, but instead at what is not proportional may be most appliable to cyber behaviour as well. One looking for Proportionality in cyber behaviour should aim to conclude that the act outweighs not only the immediately visible negative effects, but also those that may emerge in the future. While there is no defined calculus for determining this, looking at what behaviour known to be disproportionate may be the optimal way forward, and is also included within this thesis as part of what it means to be proportionate in cyberspace.

Conclusion

This chapter has shown that, using Orend's interpretation of JWT, JWT principles can be used to create a distinct set of criteria which should be able to analyze Western offensive cyber operations.

Chapter 5: Applying the JWT Framework to Western Cyber Operations

Now that the applicability of has been established, it is now apt to turn to the data collection in this thesis. This will form the answer to the second sub-question, namely "Using a JWT framework, are modern Western offensive cyber operations Just?" The full data collection can be found in Appendix A. This chapter will extract and analyze the key takeaways and includes potential lessons for policymakers.

Introduction

In total, there were 13 applicable cyberoperations launched by Western states and allies which were either a form of sabotage, denial of service, or data destruction. Of those, only 3 operations satisfactorily met all 3 principles of *Jus ad bellum*.

Out of the other principles, Just Cause, Right Intention, and Public Declaration were the ones most absent, each appearing in only 4 out of 13 operations. The most prevalent principle was proportionality, appearing in 10 out of 13 operations. This is visualized in Figure 3. Figure 4 visualizes all cyber operations by their individual results.

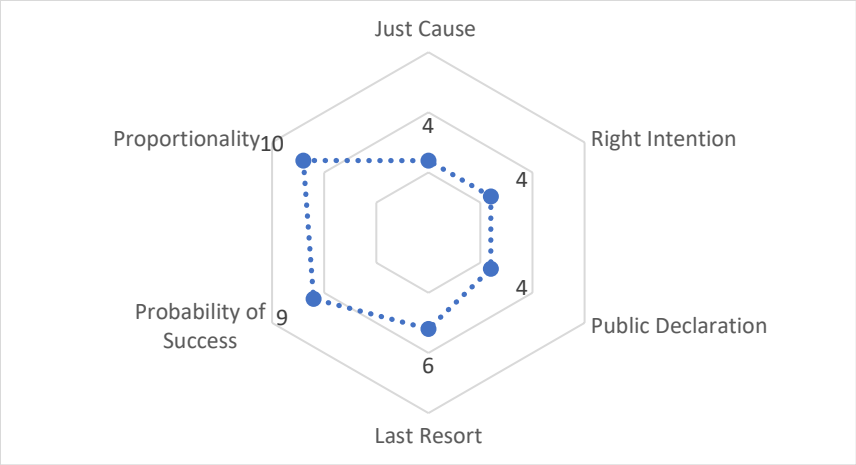

Figure 3: Prevalence of JWT Principles in Western Cyber Operations

	Just Cause	Right Intention	Public Declaration	Last Resort	Probability of Success	Proportionality	**Total Amount of Principles present**
UK targeting of the Islamic State group	Yes	Yes	Yes	Yes	Yes	Yes	**6**
Targeting of TrickBot computer networks	Yes	Yes	Yes	Yes	Yes	Yes	**6**
Operations against actors targeting Australians during COVID-19 pandemic	Yes	Yes	Yes	Yes	Yes	Yes	**6**
Targeting of the Islamic State group	Yes	Yes	No	Yes	Yes	Yes	**3**
Targeting of Internet Research Agency	No	n/a	No	Yes	Yes	Yes	**3**
Disruption of operations at Shahid Rajaee Port	No	n/a	No	No	Yes	Yes	**2**
Attack on Iranian computer systems	No	n/a	Yes	No	Yes	No	**2**
Targeting North Korea's Reconnaissance General Bureau	No	n/a	No	Yes	No	Yes	**2**
Attack on the Syrian Air Force	No	n/a	No	No	Yes	Yes	**2**
Compromise of the North Korean nuclear program	No	n/a	No	No	No	Yes	**1**
U.S. retaliation against Iran	No	n/a	No	No	No	Yes	**1**
Stuxnet	No	n/a	No	No	No	No	**0**
Flame	No	n/a	No	No	Yes	No	**0**

Figure 4: JWT in Cyber Operations

The following sections will briefly go over each result, and present the results and lessons.

Full JWT

For a cyber operation to be truly 'just' according to the JWT lens used in this thesis, it must demonstrate all six *Jus Ad Bellum* principles. Depressingly, only 3 out of the 13 analyzed Western cyber operations clear this bar. These 3 operations can all be sorted into two broad categories: operations targeting terrorist organizations and operations targeting transnational cybercriminals. There can be several reasons why these two types of operations were more likely to abide by JWT principles than others. First, these operations tend to target non-state actors. This vastly lowers the chance that this will be seen as aggression by strategic rivals as well as facilitating Public Declaration. In fact, these operations often mark the first time a government officially declared using cyber power (like with the UK targeting of ISIS). Second, many of the actors targeted (ISIS, criminal networks) were arguably less sophisticated than states thus increasing probability of success – especially as these campaigns were carefully prepared by the aggressors over the course of weeks to years. Third, these campaigns were all in response to consistent campaigns conducted by these actors, of which there was no potential of diplomatic negotiation or economic sanctions having any effect. Finally, these operations are often used by governments to 'show off' or justify their investments in cyber offensive capabilities. In recent years, the UK and Australia have been investing heavily in such capabilities, often pointing to these successes to justify the need for such investments.

Just Cause

For Just Cause, only 4 cyber operations were deemed to possess this principle. As mentioned in the discussion on Just Case, this is the most contentious principle of JWT and is often the bar most difficult to clear. Where many cyber operations struggled was with preventative or retaliatory operations: two forms of aggression which are very difficult to justify even when considering traditional conflict. Other operations (notably the American attacks on the Internet Research Agency) fell just short due to pre-existing international law; and some operations (such as the American operations against North Korean hacking) were too unclear or vague to make any conclusions on Just Cause. From the operations that did

meet Just Cause, they were all able to link their aggression as a response to ongoing campaigns targeting their states, civilians, and often critical infrastructure.

> **Lessons:** States need to clearly link targets of their offensive cyber operations to ongoing and persistent cyber campaigns aimed at their citizens or critical infrastructure. More research should be done on under what conditions, if any, it is acceptable to launch preventative or retaliatory cyber operations.

Right Intention

Since Right Intention is often linked to Just Cause, Right Intention was only analyzed when Just Cause was present. Interestingly, in each case of Just Cause, Right Intention was also present. This could be linked to three observations. First, this could be a by-product of the research design focusing specifically on Western states. Typically, Western rivals like Russia, China, Iran, and North Korea are much more notorious with using cyber operations to achieve a multitude of foreign policy goals (ranging from financial profit to testing weapons to silencing dissidents) (Valeriano and Jensen, 2019). Second, this could also be explained by the type of actors targeted by these cyber operations. After all, terrorist groups and cybercriminals arguably offer fewer other things of interest than, say, a similar cyber operation against a major strategic rival like Iran or Russia. Finally, it is likely that Just Cause is simply a lower bar than Right Intention: after all, there are few cases in even traditional JWT where an operation that fails to meet Just Cause does meet Right Intention.

> **Lessons:** States should continue to make sure their primary intentions behind a cyber operation are their identified Just Cause for resorting to the use of aggression.

Public Declaration

The principle of Public Declaration was tied for last with Just Cause and Right Intention, with only 4 cases deemed to demonstrate this principle. This number would have been dramatically lower if a looser definition of this principle for cyber was not followed (where declaration is allowed in a reasonable time following the incident). Timing of the declaration proved to be very important: most cases discussed here that declared in a reasonable time following the operations noted that they did not declare prior or during as that would greatly inhibit the objectives and probability of success of the incident. Yet, some cases were cut off even if declaration was in place. For instance, the US claimed responsibility for the 2018 operations targeting the Internet Research Agency – albeit a year later and apparently invertedly in an interview of Donald Trump, which was deemed to be an unreasonable time following the initial launch of the operation. Beyond these cases, most other cases, as predicted and explored in Chapter 4, lack any form of Public Declaration or responsibility.

> **Lessons:** States need to hold themselves accountable for offensive cyber operations. Public Declaration is largely absent in most modern Western cyber operations. States should also discuss or establish – perhaps in international fora – guidelines for reasonable public disclosure of offensive cyber operations and uphold any resulting norms or standards.

Last Resort

Last Resort was deemed to be present in 6 cyber operations launched by Western states. As seen, often when dealing with either very closed off regimes (such as North Korea) or actors outside traditional diplomacy (such as ISIS) an offensive cyber operation can be the most reasonable response to continued threatening cyber behaviour. There are also other cases that clearly meet definitions of Last Resort: most notable is the American operation against the Russian Internet Research Agency. There, failing traditional economic and legal sanctions coupled with a clear and urgent threat to American democratic processes emerging, formed a credible case for Last Resort.

But, for more than half of the offensive cyber incidents within the dataset, Last Resort was not deemed to be present. For most of these cases, such as Flame or the Israeli attack on the Syrian Air Force, it was disputed at the time of their launching whether there was sufficient or credible enough information to necessitate the operation. This might be due to a lack of information being made publicly available – which realistically should not be an excuse given the ask of other JWT principles like Public Declaration. Additionally, for many of these operations, it is not immediately clear that the action chosen is better than taking no action at all – especially as some seem to exist as purely retaliatory responses.

> **Lessons:** States need to ensure that when they seek to launch an offensive cyber operation, all other available options have been sufficiently exhausted. This is not an unattainable standard, and more care should be taken to demonstrate this urgency to the public.

Probability of Success

Most of the analyzed cyber operations (9 out of 13) were deemed to demonstrate Probability of Success. This is perhaps best attributable to the focus on purely Western states, who tend to commit considerable development and funding into designing highly sophisticated and targeted cyber weapons. This, in turn, translates to a much higher degree of confidence by policymakers that their cyber operation will succeed at accomplishing its goals. This is especially prevalent given most operations analyzed had months of preparation, development, and investment prior to be launched. By contrast, many cyber operations launched by Western rivals tend to have lower levels of sophistication, reducing chance of success and increasing potential fallout or unpredicted proliferation of effects.

This is not to say that sophistication is the only benchmark for Probability of Success – in fact, most of the operations who failed to meet this principle did appear to have an adequate level of sophistication. Simply put, many of the failing operations seemed to use their cyber operation more to

'test the waters' and see what happens. For instance, the American operations against North Korean hacking had many factors which likely would inhibit its success – something that should have been known to American decisionmakers before the operation was launched. Similarly, Stuxnet can also be critiqued along these lines: while the operation was undoubtedly highly sophisticated, the end impacts were fairly limited and more exploratory of the options available to policymakers.

> **Lessons:** Western cyber operations tend to demonstrate a high level of sophistication, allowing them to be highly targeted and thus increase the likelihood of success. Policy makers should, however, resist the temptation to use cyber operations to simply see the potential affects.

Proportionality

Proportionality saw the most uptake of any other JWT principle, with 10 out of 13 operations abiding by the principle. The majority of cyber operations analyzed were responses to other cyber operations, avoiding rampant escalation. Some operations also explicitly used cyber after deeming it as the least destructive option available. Moreover, the best proportional responses not only responded in reasonably limited means, but also responded in ways which reinforced accepted norms of international behaviour. For instance, the operations targeting cybercriminals supported international norms condemning attacks on critical infrastructure, and the American operations against the Internet Research Agency supported norms condemning election interference.

But, there were outliers. Stuxnet and Flame are two of the more difficult cases for proportionality, which others could potentially argue were proportional. While government officials (if they acknowledged these operations) could feasibly argue that they were somewhat proportional to Iran's nuclear threat, the larger difficulties come when considering the legacy of these actions. Notably, operations like Stuxnet served as justification for American rivals to also develop and launch cyber weapons – and this seems like a cost that perhaps would not be worth the potential gains from causing

some disturbances for the Iranian nuclear program. This follows the more holistic perspective on Proportionality argued for in Chapter 4.

> **Lessons:** States should continue to use cyber power in a proportional manner to the situation that presents itself. This should include a holistic view, where long-term and normative impacts are also considered.

Chapter 6: Conclusion

This thesis attempts to cover a lot of ground. First, it conducts an extensive literature review into three areas (war and aggression, cyberspace in 2021, and previous attempts to analyze cyber via JWT). Next, this thesis turns to the first sub-question – How can JWT be applied to cyber conflict – and answers it via updating existing JWT principles. This then allows this thesis to turn to the second sub-question – Using a JWT framework, are modern Western offensive cyber operations Just – and answer it via an extensive study of cases and accompanying analysis. Now, this thesis will provide several final insights, and use those to shape an answer to the guiding thesis question.

First, despite this thesis's admittedly high bar for considering an offensive cyber operation Just, several cyber operations were found that abided by all 6 JWT principles and, thus, met this bar. This should be an optimistic note: given that there exist real-world examples of JWT being fully realized in cyber operations, it proves that not only can JWT be adequately applied to the cyber domain, but also that full realization of JWT should be a gold standard that all Western states should strive to meet when conducting offensive cyber operations.

Second, on a more pessimistic note, only a small subset of cases analyzed actually met full JWT requirements. Across the operations analyzed, there was a vast fluctuation between how upheld the principles were. For instance, the principle of Proportionality was upheld in the most incidents; where as several principles (Just Cause, Right Intention, and Public Declaration) were only upheld in four cases. This reasons why each principle is upheld or not was explored in further detail in chapter 4; however, this trend of fluctuation is significant in and of itself. Namely, it suggests that oftentimes meeting JWT obligations in cyber is at best an afterthought done only when favourable. More worryingly, coupled with the few cases where full JWT was realized, it also implies that most policymakers do know what their obligations should be when it comes to conducting just operations: however, apparently, they are galvanized into acting unjustly through a myriad of potential incentives.

Third, each JWT principle had a number of differing reasons why they may fail. Accompanying insights were also explored in Chapter 5, and Figure 5 provides a summary relevant for this conclusion.

Principle	Common reasons for not meeting the principle	Insights
Just Cause	Lack of clear connection to prior aggression; need to justify a clear and present danger to civilians or critical infrastructure.	States need to clearly link targets of their offensive cyber operations to ongoing and persistent cyber campaigns aimed at their citizens or critical infrastructure.
Right Intention	Few states abided by Just Cause, which this thesis considered a prerequisite for establishing Right Intention. Generally, there is a need to clearly disclose mission objectives.	States should make sure their primary intentions behind a cyber operation are a clearly identified Just Cause for resorting to the use of aggression.
Public Declaration by Proper Authority	Many states did not publicly declare cyber operations, often due to fear of receiving retaliation, setting undesirable trends, undermining mission success, or appearing hypocritical. Other times, disclosure happened via non-official sources or an unreasonable time following the operation.	States need to hold themselves accountable for offensive cyber operations. Public Declaration is largely absent in most modern Western cyber operations.
Last Resort	Some operations were launched when internal analysts openly advocated other solutions to be explored. Many operations appeared to be more retaliatory than preventative.	States need to ensure that when they seek to launch an offensive cyber operation, all other available options have been sufficiently exhausted.
Probability of Success	Some operations seemed more exploratory than a path toward an explicit end.	Policy makers should, however, resist the temptation to use cyber operations to simply see the potential affects.
Proportionality	Some cyber operations set adverse normative trends (such as normalizing reckless or frequent offensive cyber behaviour) or caused escalation outweighing benefits.	States should continue to use cyber power in a proportional manner to the situation that presents itself. This should include a holistic view, where long-term and normative impacts are also considered.

Figure 5: Reasons why JWT principles failed

In summary, looking now at the starting thesis question of "*To what extent do modern, Western cyber operation abide by the Jus Ad Bellum principles of Just War Theory?",* it can be noted that: (a) JWT can provide an adequate perspective to analyze cyber operations, and realizing all JWT principles can be a gold standard states should strive to (if they accept the underlying JWT framework); (b) there is a wide range of variation amongst cyber operations in terms of respect of JWT principles, with only a few

meeting all 6; and (c) the reasons why cyber operations fail are diverse and varying, but there do exist feasible policy solutions which could address these. Ultimately, it was determined that only three examples of Western offensive cyber operations satisfactorily met the full definition of JWT in this thesis.

Finally, where should the future lead us? As explored within the literature review, there are two key Western responses to the threats from the cyber domain: the diplomatic, and the offensive. This thesis has mainly focused on isolating issues with the offensive trends from a moral perspective. However, it should also be noted that much of the progress that can happen on the moral aspect in the offensive response will primarily come from and be actualized by the diplomatic threads. This thesis can help isolate where more guidance is needed from the diplomatic realm on the offensive realm, and any future such projects expanding on the scope or arguments of this thesis could also prove informative. In particular, applying this JWT lens to either rival states cyber operations or non-state cyber operations would be an ideal next step.

Appendix A: Case Comparison

Data Tables 1: Acts of Sabotage

Suspected Sponsor	Year Reported	Just Cause	Right Intention	Public Declaration	Last Resort	Probability of Success	Proportionality
Israel	2020	No	n/a	No	No	Yes	Yes
Disruption of operations at Shahid Rajaee Port		A retaliatory attack against Iran for Iranian cyber operations targeting Israeli critical infrastructure. Generally, the pursuit of retaliation is not allowed under Just Cause.		Israel has not claimed responsibility, despite credible links to them.	Tit-for-tat escalation is typically not last resort.	Highly targeted.	This Israeli response reinforces norms condemning operations targeting critical infrastructure.
Additional Sources: Gross, J. (2020). *Cyberattack on port suggests Israeli tit-for-tat strategy, shows Iran vulnerable*. The Times of Israel. https://www.timesofisrael.com/cyberattack-on-port-suggests-israeli-tit-for-tat-strategy-shows-iran-vulnerable/.							
USA	2020	Yes	Yes	Yes	Yes	Yes	Yes
Targeting of TrickBot computer networks		Disabled an operation which had targeted critical services when evidence suggested it was preparing to re-emerge.	No ulterior motives other than disable a malicious botnet.	Did publicly assume responsibility within a reasonable time after the operation.	No other options existed, and it was deemed a pressing matter.	Highly targeted.	Proportionate response to protecting critical infrastructure.
Additional Sources: Nakashima, E. (2020). *Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election*. Washington Post. https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.							

USA; Israel	2010	No	n/a	No	No	No	No
Stuxnet		Did the Iranian nuclear program pose a legitimate threat to American/Israeli security? Arguably, not yet: thus Stuxnet was primarily a first strike.		No suspected sponsors have claimed responsibility.	While Iran was about to upgrade their centrifuges, arguably options like sanctions were not fully explored or realized yet.	Highly targeted: but, overall, only about 1000 out of 8000 Iranian centrifuges were affected. Uranium enrichment also did not drop. Sources have claimed that internal officials were not convinced that Stuxnet would have the desired effect before launching.	Believed by the US and Israel to be proportional to the Iranian nuclear threat. However, it did lead to norms of reciprocal cyber engagement and offensive cyber capacity building. Iran also greatly upgraded their offensive cyber capabilities.
Additional Sources: Jenkins, R. (2013). Is Stuxnet Physical? Does it matter? *Journal of Military Ethics* 12(1), 58-79. https://doi.org/10.1080/15027570.2013.782640; Singer, P.W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. *Case Western Reserve Journal of International Law* 47(1), 79-86. https://scholarlycommons.law.case.edu/jil/vol47/iss1/10/; Zetter, K. (2014). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon.* Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.							

UK	2018	Yes	Yes	Yes	Yes	Yes	Yes
UK targeting of the Islamic State group		A cyberoperation launched to destroy the capabilities of ISIS to spread content online and target foreign citizens.	These operations were done solely to disrupt ISIS capabilities.	Did publicly assume responsibility within a reasonable time after the operation.	Least destructive of options available.	Highly targeted.	Proportionate response to tackling extremism.
Additional Sources: Bond, D. (2018). *UK reveals Isis target of first military cyber attack*. Financial Times. https://www.ft.com/content/cea9d608-3e3f-11e8-b7e0-52972418fec4.							

USA	2019	No	n/a	Yes	No	Yes	No
Attack on Iranian computer systems		Retaliatory response to an Iranian attack on an American drone.		USA publicly assumed responsibility and discussed it as a non-armed response (instead of a drone strike President Trump contemplated).	Retaliation is not a last resort, other options could have been explored.	Highly targeted, anonymous sources claim it was planned for weeks.	Was done instead of a proposed conventional missile strike due to cyber being perceived as below the threshold of armed conflict. However, it did reinforce norms of using cyber as retaliation.
Additional Sources: Barnes, J. and Gibbons-Neff, T. (2019). *U.S. Carried Out Cyberattacks on Iran. NYTimes*. https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.							

USA	2017	No	n/a	No	No	No	Yes
Compromise of the North Korean nuclear program		There were Korean nuclear threats against the U.S., but arguably the threat was not yet imminent.		No actor has claimed responsibility.	Lack of demonstrated urgency.	No successes in preventing nuclear capability development. North Korea poses a number of structural challenges to cyber operations.	Attack generally limited to only nuclear capabilities, which pose a legitimate danger when in the hands of the North Korean regime.
Additional Sources: Sanger, W. and Broad, W. *Trump Inherits a Secret Cyberwar Against North Korean Missiles*. NYTimes. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.							

USA; UK	2016	Yes	Yes	No	Yes	Yes	Yes
Targeting of the Islamic State group		ISIS cyber operations were being used to directly advance ISIS goals and spread ISIS content; as well as physically threaten American civilians.	These operations were done solely to disrupt ISIS capabilities, little evidence of ulterior motives.	Details were released after the successful operations.	No other diplomatic or economic tools were viable alternatives. Cyber is less destructive than drone/missile strikes.	Highly targeted.	Used cyberweapons to proportionately disrupt ISIS exploitation of the internet.
Additional Sources: Sanger, D. (2016). *U.S. Cyberattacks Target ISIS in a New Line of Combat*. NYTimes. https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.							

USA	2019	No	n/a	No	Yes	Yes	Yes
Targeting of Internet Research Agency		While the Russian IRA was directly conspiring to influence American elections, the U.S. was responding to their disinformation: something allowed under international law.		Confirmed by U.S. President Trump several years after the operation happened. Before, official attribution was not clear.	On the short notice USCYBEROM had, coupled with the failure of several other tools, a short-term cyber event temporarily disrupting the IRA was the last feasible option to stop election interference.	Highly Targeted.	The limited nature of the strike (only was intended to temporarily disable the IRA during the midterm election) made it largely proportional. Reinforced international norms against democratic election interference.
Additional Sources: Nakashima, E. (2019). *U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms*. Washington Post. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html/.							

Data Tables 2: Data Destruction

Suspected Sponsor	Year Reported	Just Cause	Right Intention	Public Declaration	Last Resort	Probability of Success	Proportionality
Australia	2020	Yes	Yes	Yes	Yes	Yes	Yes
Operations against actors targeting Australians during COVID-19 pandemic		Directly done to stop cybercriminals targeting Australian citizens and critical infrastructure.	No evidence to support any alternative motives.	Public statements were released by the Australian government.	No other options existed.	Worked alongside a variety of actors to ensure success.	A clear and justified response that was limited to only targeting the cybercriminals via cyberspace.
Additional Sources: Reynolds, L. (2020). *On the offensive against COVID-19 cyber criminals*. Department of Defence Ministers. https://www.minister.defence.gov.au/minister/lreynolds/media-releases/offensive-against-covid-19-cyber-criminals.							
USA	2019	No	n/a	No	No	No	Yes
U.S. retaliation against Iran		A retaliatory strike against Iran for a Sept. 2019 incident where Iran attacked Saudi oil facilities.		No official statements or attribution.	Retaliation is generally not last resort for action.	It is not clear that there would not have been equivalent affects from taking no action at all.	A relatively limited attack in terms of destructive capability. Reinforced norms against targeting critical infrastructure.
Additional Sources: Ali, I. and Stewart, P. (2019). *U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials*. Reuters. https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-say-idUSKBN1WV0EK.							

USA; Israel	2012	No	n/a	No	No	Yes	No
Flame		Similar malware/virus to Stuxnet designed to undermine Iranian nuclear and critical infrastructure capabilities (not to prevent an active threat).		No official declaration or attribution (only unofficially attributed to USA and Israel).	It was unclear whether the Iranian nuclear program would be effectively deterred by programs like Flame: thus, Last Resort is not fully in play.	Highly targeted; arguably had less ambitious (more achievable) targets than Stuxnet.	Believed by the US and Israel to be proportional to the Iranian nuclear threat. However, it did lead to norms of reciprocal cyber engagement; offensive cyber capacity building.
Additional Sources: Nakashima, E. (2012). *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*. Washington Post. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.							

Data Tables 3: Denial of Service

Suspected Sponsor	Year Reported	Just Cause	Right Intention	Public Declaration	Last Resort	Probability of Success	Proportionality
USA	2017	No	n/a	No	Yes	No	Yes
Targeting North Korea's Reconnaissance General Bureau		Targeted North Korea's active cyber warfare unit. Sought to disable their internet connections. While North Korea has attacked critical infrastructure, it is currently unclear in response to what these American attacks were launched. Thus, Just Cause could potentially be in place.		No public responsibility claimed.	This operation was likely the least destructive way to stop Korean hacking, especially as diplomatic and economic measures were already taking place and largely ineffective.	Unclear whether the operation would actually disable North Korean hacking.	North Korea has shown no signs of halting their predatory cyber warfare program; cyberattacks aimed at stopping their ability to do so appear proportional.
Additional Sources: Gallagher, S. (2017). *As US launches DDoS attacks, N. Korea gets more bandwidth—from Russia*. Ars Technica. https://arstechnica.com/information-technology/2017/10/as-us-launches-ddos-attacks-n-korea-gets-more-bandwidth-from-russia/.							

Israel	2007	No	n/a	No	No	Yes	Yes
Attack on the Syrian Air Force		This attack was launched to knock out Syrian air defenses to allow Israel to bomb a Syrian nuclear reactor. Largely a first strike.		No public responsibility claimed.	Many analysts were unsure at the time whether the attack should proceed.	Fairly sophisticated attack; which also greatly increased the chance of success of the accompanying Syrian bombing raid.	In terms of the means used, cyber was arguably the power with the lowest risk of escalation and destruction to disable Syrian air defenses; as well as avoiding unnecessary casualties.
Additional Sources: Farley, R. (2019). *Syria Wanted a Nuclear Bomb, but in 2007 Israel's Air Force Destroyed Their Reactor*. National Interest. https://nationalinterest.org/blog/buzz/syria-wanted-nuclear-bomb-2007-israels-air-force-destroyed-their-reactor-86486.							

Reference List

Arquilla, J. and Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy* 12 (2), 141-165. https://doi.org/10.1080/01495939308402915.

Alexander, K.B. (2011). Building a New Command in Cyberspace. *Strategic Studies Quarterly* 5(2), 3-12. https://www.jstor.org/stable/26270554.

Aloyo, E. (2015). Just War Theory and the Last of Last Resort. *Ethics & International Affairs* 29(2), 187-201. https://doi.org/10.1017/S0892679415000064.

Broeders, D. (2021). Private active cyber defense and (International) cyber security – pushing the line? *Journal of International Cyber Security* 7(1), 1-14. https://doi.org/10.1093/cybsec/tyab010.

Brown, G. (2003). Proportionality and Just War. *Journal of Military Ethics* 2(3), 171-185. https://doi.org/10.1080/15027570310000667.

Council on Foreign Relations. (2021). *Cyber Operations Tracker*. CFR. https://microsites-live-backend.cfr.org/cyber-operations.

Digwatch. (2021). *UN GGE and OEWG.* Digwatch. https://dig.watch/processes/un-gge.

Dipert, R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics* 9(4), 384-410. https://doi.org/10.1080/15027570.2010.536404.

Dunn-Cavetly, M. (2018). Cyber War Will Not Take Place by Thomas Rid. *European Review of International Studies* 5(1), 131-134. https://www.jstor.org/stable/26593685.

Faesen, L., Torossian, B., Mayhew, E., and Zensus, C. (2019). *Conflict in Cyberspace: Parsing the Threats and the State of International Order in Cyberspace.* HCSS. https://hcss.nl/report/conflict-in-cyberspace-parsing-the-threats-and-the-state-of-international-order-in-cyberspace/.

Faesen, L., Sweijs, T., Klimburg, A., MacNamara, C., and Mazarr, M. (2020). *From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict*. HCSS. https://hcss.nl/news/new-report-from-blurred-lines-to-red-lines-countermeasures-and-norms-in-hybrid-conflict/.

Finlay, C. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology* 31 (3), 357-377. https://doi.org/10.1007/s13347-017-0299-6.

Global Commission on the Stability of Cyberspace. (2019). *Advancing Cyberstability*. HCSS. https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf.

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

Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, A. (2021). *US Sanctions on Russia Rewrite Cyberespionage's Rules*. Wired. https://www.wired.com/story/us-russia-sanctions-solarwinds-svr/.

Halpern, S. (2019). *How Cyber Weapons Are Changing the Landscape of Modern Warfare*. The New Yorker. https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.

Harbour, F. (2011). Reasonable Probability of Success as a Moral Criterion in the Western Just War Tradition. *Journal of Military Ethics* 10(3), 230-241. https://doi.org/10.1080/15027570.2011.608497.

Ignatidou, S. (2021). *The COVID-19 pandemic and trends in technology*. Chatham House. https://www.chathamhouse.org/2021/02/covid-19-pandemic-and-trends-technology/04-infodemic-and-covid-19-disinformation.

Jay, J. (2021). *Britain may deploy Trident missiles in response to destructive cyber attacks.* TEISS. https://www.teiss.co.uk/britain-may-deploy-trident-missiles-in-response-to-destructive-cyber-attacks/.

Kettmann, S. (2004). *Soviets Burned By CIA Hackers?* Wired. https://www.wired.com/2004/03/soviets-burned-by-cia-hackers/.

Klimburg, A. (2020). Mixed Signals: A Flawed Approach to Cyber Deterrence. *Global Politics and Strategy* 62(1), 107-130. https://doi.org/10.1080/00396338.2020.1715071.

Laudrain, A.P.B. (2018). *France's New Offensive Cyber Doctrine*. Lawfare. https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.

Lazar, S. (2016). *War*. The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/.

Libicki, M. (1995). *What is Information Warfare?* National Defense University. https://apps.dtic.mil/sti/pdfs/ADA367662.pdf.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html.

Maness, R., Valeriano, B., and Jensen, B. *The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5.* Ryan C. Maness [Website]. https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.

NATO. (2015). *Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar*. NATO. https://www.nato.int/cps/en/natohq/opinions_118435.htm.

NATO. (2021). *Deterrence and defence*. NATO. https://www.nato.int/cps/en/natohq/topics_133127.htm.

Nguyen, R. (2013). Navigating Jus Ad Bellum in the Age of Cyber Warfare. *California Law Review* 101 (4), 1079 – 1129. https://www.jstor.org/stable/23784325.

O'Flaherty, K. (2019). *Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First.* Forbes. https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/?sh=12a90f87f895.

Orend, B. (2000). Michael Walzer on Resorting to Force. *Canadian Journal of Political Science* 33(3), 523-547. https://www.jstor.org/stable/3232581.

Orend, B. (2013). *The Morality of War*. Broadview Press.

Paris Call. (2021). *The 9 Principles*. Paris Call. https://pariscall.international/en/principles.

Pritchard, L. (2019). *Is Just War Theory a credible tool to explain contemporary war, globally*? EuroISE. https://www.euroisme.eu/images/Documents/Price2019/Pritchard_2019_ENG.pdf.

Purves, D. and Jenkins, R. (2016). Right Intention and the Ends of War. *Journal of Military Ethics* 15(1), 18-35. https://doi.org/10.1080/15027570.2016.1170385.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies* 35 (1), 5-32. https://www.jstor.org/stable/26593685.

Rona, T. (1976). *Weapon Systems and Information War.* Boeing Aerospace Company. https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf.

Roscini, M. (2010). World Wide Warfare – Jus ad bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law* 14, 18-130. https://ssrn.com/abstract=1683370.

Rowe, N. (2009). The Ethics of Cyberweapons in Warfare. *International Journal of Cyberethics* 1(1). https://faculty.nps.edu/ncrowe/ethics_of_cyberweapons_09.htm.

Sanger, D. and Perlroth, N. (2021). *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*. NYTimes. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

Sanger, D. and Schmall, E. (2021). *China Appears to Warn India: Push Too Hard and the Lights Could Go Out*. NY Times. https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Operations*. Cambridge University Press. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

Schmitt, M. (2017). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Sheldon, J. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly* 5 (2), 95-112. https://www.jstor.org/stable/26270559.

Singer, P.W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. *Case Western Reserve Journal of International Law* 47(1), 79-86. https://scholarlycommons.law.case.edu/jil/vol47/iss1/10/.

Steed, D. (2011). Cyber Power and Strategy – So What? *Infinity Journal* 1 (2), 21-24. https://www.militarystrategymagazine.com/article/cyber-power-and-strategy-so-what/.

Steed, D. (2021). *The National Cyber Force: directions and implications for the UK.* Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/cybersecurity/ari18-2021-steed-the-national-cyber-force-directions-and-implications-for-the-uk.

Stone, J. (2013). Cyber War *Will* Take Place. *Journal of Strategic Studies* 36 (1), 101-108. https://doi.org/10.1080/01402390.2012.730485.

Thumfort, J. (2020). Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius*. Internet Policy Review* 9(3). DOI: 10.14763/2020.3.1500.

Trampusch, C. and Palier, B. Between X and Y: how process tracing contributes to opening the black box of causality. *New Political Economy* 21(5), 437-454. http://dx.doi.org/10.1080/13563467.2015.1134465.

UN OEWG. (2021). *Final Substantive Report*. United Nations. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

USCYBERCOM. (2018). *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.* https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

Valeriano, B. and Jensen, B. (2019). The Myth of the Cyber Offense: The Case for Restraint. *Cato Institute Policy Analysis* 862, 1-16. https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint.

Walzer, M. (1977). *Just and Unjust War: A Moral Argument with Historical Illustrations*. Basic Books.

Weiss, J. and Hunter, B. (2021). *The SolarWinds Hack Can Directly Affect Control Systems*. Lawfare. https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems.

Williams, K. (2015). *Drone strike kills ISIS hacker*. The Hill. https://thehill.com/policy/cybersecurity/252102-drone-strike-may-have-killed-isis-hacker.