The Moral Limits of Cyberwarfare: How Should States Respond to Cyber-Attacks?

Valk,

N.A. Valk

The Moral Limits of Information Warfare

How Should States Respond to Cyber-Attacks?

Master's Thesis, June 2022

Supervisor: Prof. Dr. T.R. Wells

Institute for Philosophy, Leiden University

Word Count: 18309
S1970968
July 31, 2022

ABSTRACT: This thesis engages with the question: how should states deal with information warfare? To begin with, this question will be discussed from the perspective of Just War Theory. The analysis will demonstrate that solely the *jus in bello* category of JWT, as opposed to *jus ad bellum*, is relevant for information warfare. Furthermore, scholar alternative ethical framework designed by Taddeo will be critiqued. According to Taddeo, the application of Just War Theory to information warfare causes a problem because physical harm and harm in the cyber domain are in different ontological domains. Her theory strives for ontological equality by merging information ethics with Just War Theory. However, our analysis will show that the resulting theory is unsatisfactory in several ways. As an alternative, I will suggest to distinguish four categories of harm and six forms of information warfare. These forms of information warfare can be associated with the categories of harm in order to determine to what extent *jus in bello* is suitable to assess the justifiability of IW attacks by looking at their consequences.

Table of Contents

1. Introduction

There used to be four domains in warfare: the naval, land, air, and space domain. Recently, a new domain has been added to these four: the cyber/information domain. The traditional domains of warfare have in common that they all occur within the physical realm. This means that these domains and their consequences, in warfare, are all physically perceptible. Bullets are shot by infantry soldiers on the ground (land), rockets are launched by ships that sail on the seas (naval), bombs are dropped by fighter planes (air), and satellites are used for communication and intelligence (space). Cyberspace, however, as a fifth domain, 'is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies' (Kuehl 2009, p. 29). The use of information communication technologies (ICTs) on the battlefield has thereby changed the ways wars are fought. Fewer risks have to be taken and supposedly warfare can be fought without directly causing any physical harm to the adversary.

Some noteworthy examples of information warfare (IW) are the following: the cyber-attack in 2010 on the nuclear program of Iran with a cyber-worm, 'Stuxnet'. This worm – a method of a cyber-attack – was designed to infiltrate and disrupt computer systems. The consequence of this attack was that about one-fifth of the nuclear centrifuges in Iran were destroyed and their nuclear program was set back about two years (Kelley 2013). More examples of acts of IW occurred in the Russo-Ukrainian war. Since 2013 there have been cyber-attacks from both sides. The first cyber-attack was 'Operation Armageddon' from the Russian side (Weedon 2015, p. 73). The last cyber-attack from Russia against Ukraine has been during the end of January and the beginning of February 2022. Just before the full-scale war on Ukraine started, Russia attacked and took down several government and banking websites (Kramer 2022). A final example concerns the Israeli-Palestinian conflict. With these attacks, however, 'hacking and social media, particularly Facebook, are among the most important tools of Palestinian-Israeli cyber conflict, where Israel is much superior to Palestinians, mainly due to its control over the telecommunications and internet infrastructure in Palestine' (Abu Saada & Turan 2021).

This relatively new kind of warfare brings crucial moral dilemmas for policymakers that call for answers. To begin with, it is not always clear who the perpetrator of a cyber-attack is. Furthermore, it is difficult to determine in advance which attacks will be effective and proportional to the military advantages they will bring. In addition, it is difficult and sometimes even impossible to distinguish between combatants and non-combatants. All these dilemmas are made worse by the fact that there are no conventions, treaties or exact legal rules yet that outline the morality of cyber-attacks.

These dilemmas are not new and play a significant role in conventional warfare (CW) as well. Issues such as attribution, necessity, discrimination, and proportionality are not new issues within the context of CW, but they have different implications in IW. However, for CW, a theory has been designed to assess these problems and determine whether acts of war are justifiable or not. This theory is called Just War Theory (JWT). However, it is questionable to what extent JWT is applicable to IW. This question emerges because of the following reasons: firstly, it is debatable to what extent the distinction between peace and war can genuinely be made in the case of IW. In JWT, there is a distinction between the questions whether it is right to resort to war (*jus ad bellum*) and whether a war is fought in a just way (*jus in bello*). However, as the distinction between war and peace in IW is opaque, the question is whether the distinction between *jus ad bellum* and *jus in bello* is possible in the case of IW. The second question about the use of JWT as an instrument for IW follows from the first problem. When there is no clear distinction to be made between war and peace, we may nonetheless evaluate IW through *jus in bello*. However, *Jus in bello* is derived from certain principles, such as proportionality, necessity, and discrimination. The question is whether these principles are also relevant and applicable to IW.

There has been an attempt to resolve these questions regarding the justification and moral assessment of IW. Mariarosaria Taddeo argues that JWT is 'a necessary but not sufficient instrument for considering the ethical implications of information warfare' (Taddeo 2014, p. 213). According to Taddeo, the only suitable ethical analysis of IW would be by merging JWT with information ethics (IE). She calls this approach Just Information Warfare (JIW). She has a two-pronged approach for devising JIW. First, she tries to fill the 'theoretical vacuum' on the phenomenon of IW. She differentiates between different kinds of IW activities: cyber-attacks, robotic weapons, and the management of communications among the fighting units. The ICTs have an offensive or a defensive purpose of destroying, disrupting

or controlling the enemies' resources. (Taddeo 2011). Subsequently, she tries to provide the conceptual basis for establishing new ethical rules for IW. This is done by merging the macro-ethical framework of IE – a form of ethics that is concerned with the whole realm of reality which provides an analysis of moral issues from an informational perspective - with JWT (Taddeo 2014). As a consequence of this merging, JIW is designed. JIW is grounded on three ethical principles that are able to assess whether certain actions within IW are justified or not.

Taddeo's theory is a thought-provoking addition to the literature on IW. Her theory, however, is unsatisfactory in assessing the justifiability of acts in IW for a few reasons. First, the approach of Taddeo suffers from terminological issues. The term 'information warfare' is a broad term that can refer to multiple things. Over time, this concept has undergone many transitions with regard to meaning and complexity. The term, especially used in the way by Taddeo, is 'less straightforward to determine what is covered by this definition of IW and what is not' (Stevens 2012). This makes the definition of information war too broad. Secondly, Taddeo aims for a certain 'ontological equality'. This means that all kinds of consequences and harm caused by acts of war should be evaluated in the same way. It is questionable if harm to a human being and damage to a computer can be considered the same kinds of harm. Thirdly and related to the other problems of Taddeo's approach, Taddeo introduces the terms 'well-being' and 'destruction' of the *infosphere*. This notion, however, raises questions. For instance, she does not define how this well-being or destruction is caused, and consequently it is hard to know how this well-being can be achieved or protected. Finally, Taddeo uses the term 'victory' in the context of IW. As it is difficult in IW to determine whether it is a time of war or peace, it is impossible to know if there even can be a thing such as victory in IW.

Once we consider all of this, the question remains: how should states deal with IW - or cyberattacks? In this thesis, I try to bring a solution to this question closer by first going deeper into the different forms of cyber-attacks that can be part of IW and then showing that each form of cyber-attack involves different kinds of harm and thus different types of dilemmas. These dilemmas subsequently ask for different types of moral evaluation. Thus, some of the categories and principles of JWT can still be applied to some types of attacks that take place in the context of IW. Other types of attacks in the sphere of IW should rather be considered outside the scope of JWT and therefore also require different types of evaluation. We will thus show that it is not feasible to claim that a single theory can be devised on the justifiability of all types of acts within IW.

2. A Traditional Approach for Modern Warfare

Not everyone thinks that war can be morally evaluated. Realists and pacifists, for example, do not think so. But those who believe it can be done usually turn to JWT. JWT is a doctrine of military ethics studied and used by military strategists, policymakers, and ethicists. This theory claims that there is a way to assess whether acts of war are morally justified or not. (Lazar 2020). JWT presupposes the belief that war can be justified when it pursues some greater good and prevents more undesirable outcomes, such as atrocities or collateral damage. This chapter will focus on JWT only because the other two paradigms do not even question the justifiability of war.

Just War Theory was initially designed as an ethical framework for CW in the traditional domains. Information war, however, is a new kind of war, fought in a different - non-physical - domain. The question that therefore arises is whether JWT is still relevant with regard to IW and cyber-attacks. This chapter will explain which challenges arise with the application of traditional JWT falls for assessing acts of IW. First, the two main components of JWT, *jus ad bellum* and *jus in bello*, will be discussed. We will see that the dichotomy between these two domains of JWT has, for several reasons, already become opaque in conventional warfare. Yet we will see that in information warfare this distinction has wholly disappeared. Secondly, we will see that when we try to apply the principles of *jus in bello* to IW, the conditions of this category are relevant but turn out not to be applicable 1-on-1 to IW.

2.1 The Traditional Categorical Distinction Between *Jus ad Bellum* and *Jus in Bello*

JWT separates the moral evaluation of war into two categories. First, there is the category of *jus ad bellum*, translated as the right to (go to) war. This category addresses the question whether it is justified to resort to war. Secondly, there is the category of *jus in bello*, translated as the right (conduct) in war. This category considers the question whether the war is waged in a just manner. The two categories have their own conditions that should be met in order for a war to be just. The point of this distinction is to separate different stages of warfare and give a framework to determine whether an act of war is just or not. International law also makes this distinction.

On the one hand, *jus ad bellum* describes the circumstances under which states may resort to war or the use of force in general. Both the prohibition on the use of force between

states and the exceptions to it are enshrined in the 1945 United Nations Charter. *Jus ad bellum* prescribes certain conditions that ought to be met before resorting to war. When these conditions are all met, the resort to war can be considered just.

On the other hand, *Jus in bello* governs the conduct of the parties involved in an armed conflict. International humanitarian law looks a lot like *jus in bello* and it can thus be considered as a foundation for law. International humanitarian law (IHL) aims to reduce the suffering of war by protecting and assisting victims wherever possible. It thus views conflict as a reality, without looking at the reasons or legality of resorting to violence. It rules only on the humanitarian aspects of the conflict. It applies to all parties in a conflict, regardless of the reasons or the legitimacy invoked by any party. *Jus in bello* is meant to determine whether a war is waged justly and directs how combatants of a war should act by indicating boundaries that should not be crossed when a war is in progress. The *jus in bello* conditions, according to Frowe, are enshrined in 'two sets of conventions. The Hague Conventions of 1899 and 1907 […] and the subsequent Geneva Protocols of 1977' (2015, p. 105).

2.1.1 Fading Boundaries for the Distinction in Conventional Warfare

However, the distinction between these two categories within CW has been under pressure for some time. Thus, in today's world, it is more challenging than before to make this distinction. The Russo-Ukrainian war is a case in point. According to President Putin, Russia did not start a war but instead, as he addressed on Russian national television on the 24th of February 2022, he launched a 'special military operation'. This immediately led to the invasion of Ukraine by Russian troops. Although it is forbidden in Russia to consider this military act as an act of war, most Western states (NATO) recognized this as an act of war. After the first attacks on the same day of Putin's speech, Ukraine mobilized its army and declared martial law (Reuters 2022). The response of NATO can also be considered as noteworthy and something that demonstrates that it is hard to say what the dividing lines are for the traditional categories of JWT. NATO does not actively participate in this war. However, it seems that they are waging a proxy war against Russia at the moment. Instead of sending troops, they send equipment and weaponry to support the Ukrainians. By doing this, they are not actively fighting and risking the lives of their own military personnel, but they do participate on another level in the war. In addition, next to sending this support to Ukraine,

most NATO countries are also boycotting Russia. Through the use of sanctions, they try to weaken Russia and show their support to Ukraine.

This contemporary example illustrates that the categories of JWT are already a grey area within CW. In this particular war, there are three active actors: Russia, Ukraine and the Western World. In accordance with the categories of JWT, only one country, namely Ukraine, meets both categories. This, however, does not necessarily apply to NATO and Russia. Russia does not consider itself to be at war. Russia claims that it is on a peace mission to help the Ukrainian people from the Kyiv regime (The Spectator 2022). The result of this position is that *jus ad bellum* becomes less relevant. The Western world also does not consider itself to be at war. They provide help to Ukraine, but they want to avoid direct conflict with Russia. When one of the states of NATO gets into direct conflict with Russia, this means that NATO is in conflict with Russia, which could lead to disastrous consequences. Mainly for this reason, both parties, NATO and Russia, avoid direct conflict with each other.

2.1.2 Disappeared Boundaries for the Distinction in Information Warfare

As we have seen, the distinction between *jus ad bellum* and *jus in bello* in a conventional war is already a grey area. However, the distinction can still be made in some cases, and it can be helpful to use the categories of JWT to assess whether conventional war is waged in a just way. However, the categorical distinction between *jus ad bellum* and *jus in bello* is even harder to make for IW. For IW, the distinction has arguably completely disappeared. This is the case for several reasons: first, in IW, there is usually no conflict that takes place through continuous attacks. It is usual in CW that a conflict consists of frequent attacks from both sides. States need to defend themselves in order to subsist. When they do not defend themselves, the enemy can cross the border and occupy territory. There are cases where the country attacked does not respond to an enemy attack and surrenders — an example is the capitulation of Denmark. After multiple attacks from different German armed forces, the Danes surrendered to the Germans after six hours. However, most of the time states are attacked, there is some kind of resistance from the side of the aggressed state. So, when a state does not immediately surrender, it is highly probable that there are frequent attacks from the aggressor and frequent responsive attacks from the aggressed state. Examples of frequent attacks during CW are the attack on Pearl Harbor by the Japanese, their attacks on the UK by Germany and the responses of both countries. Both the US and the UK attacked executed counterattacks

against their aggressors and stayed in active conflict till the end of World War II. The US sent troops to Europe and Asia, and the UK did the same to help their allies and defend their own state. However, the events that indicate the distinction in CW do not always apply to IW with respect to a few reasons.

These immediate responses and the possibility of a counterattack are not usual in IW. An attack in the cyber domain usually requires a lot of preparation, time, and money. This is also true for conventional war, but when a state is attacked in conventional war, there is an immediate need for a response. This causes frequent and fast consecutive reactions in CW. This is not the case when considering IW. In IW, an attack does not necessarily mean that the aggressed state would immediately be occupied. An immediate counterattack, therefore, is less urgent. Another point that decelerates the speed of retaliation in the cyber domain is that it usually is more time-consuming to execute one. Most of the time, a cyber weapon is developed based on an information system of the attacked party. The development of such a weapon 'involves identifying a platform in another country, gaining access, and then remaining undetected, often for years, inside the system' (Halpern 2019). According to IBM's 'Cost of a Data Breach Report 2021', in 2021, it took an average of 212 days to identify a data breach – or cyber attack – and another 75 days to contain it (IBM 2021). This means that attacks also go undetected sometimes, and when something stays undetected, it is impossible to even give a response to such an attack. Even when the attack is detected, it should be taken into consideration that it already took about a year to find out and contain the breach; an actor then also has to start preparing a counterattack before it can actually be executed. This takes a tremendous amount of time. It is questionable whether a vengeance would still be useful. Once the cyber-attack is performed, all this valuable time and money are spent. The point is that, unlike CW, IW does not consist of continuous conflict. Generally, there are more kinds of isolated attacks against each other than consecutive attacks. An example is the cyberwarfare between Ukraine and Russia. The attacks within this 'cyberwar' are isolated and do not necessarily respond to each other.

Secondly, the involved actors are not constantly occupied with the thought of responding to an attack in the cyber domain. There is no immediate need for any defensive counterattacks. An attack within IW does not mean that enemy troops are crossing the border and the state needs to protect itself. This is different within CW, where attacks lead to direct physical harm to a state. In addition, unlike as within CW, where retaliation for the (physical)

harm done is not unusual, this is less relevant for IW. Because there is not necessarily a question of physical harm to casualties within IW, the urge for retaliation is less. In general, states consider an attack within the cyber domain less severe than a conventional attack for the reason that with these kinds of attacks, usually no human harm is directly involved.

Third and in line with the former argument, there is not necessarily a fundamental change within the diplomatic arena when an informational attack is executed. The kind of harm done by such attacks is different than that of a conventional attack. Because it is not necessary for IW that there is any physical damage or human casualties, it is often considered to be less serious than a conventional attack. When a conventional attack is executed and combatants or civilians are hurt, there often is an immediate need from the diplomatic arena to call for direct response in the same form as the conventional attack. Because the harm that is suffered is not considered to be as serious, there is not always an immediate need to oppose the other side of the diplomatic arena. For the reason that the harm is most of the time considered to be less severe than the harm done by a conventional attack, the diplomacy would not change fundamentally after an attack in IW, while this does typically after a conventional attack.

2.2 Evaluating Information Warfare through *Jus in Bello*

We have seen that the distinction between *jus ad bellum* and *jus in bello* is no longer helpful in the case of IW. This does not apply to *jus in bello* and the relevance of this category and its conditions will be addressed in this subchapter. The *jus in bello* category comes with certain conditions that determine whether separate attacks in a war should be considered just or not and gives combatants a direction on how they are supposed to act when they want to act justly. These conditions have been designed to assess acts of conventional warfare and not IW. The conditions are discrimination, proportionality, and necessity. When these three conditions are met, according to JWT, a war is fought in a justifiable manner. This subchapter will explain the conditions and assess their suitability for IW.

2.2.1 Distinction

According to Brian Orend (2013), the condition of discrimination and non-combatant immunity – or distinction - are the most critical requirements of *jus in bello*. This requirement

is also the strictest and most frequently enforced requirement of *jus in bello* within the international laws of armed conflict. The essence of the condition is as follows, according to Orend (2013, p. 113): 'soldiers charged with the deployment of armed force may not do so indiscriminately; rather, they must exert every reasonable effort to discriminate between legitimate and illegitimate targets'. He continues by asking himself how soldiers should know such a thing. Who or what is a legitimate target or not? Legitimate targets are targets that somehow have an engagement in harming during wartime. This means that all persons, objects, or institutions that are not engaged in harming should thus be ethically immune from direct attacks done by either soldiers or their systems. Soldiers on the enemy side clearly take part in the war and thus in the harming. This means that these enemy soldiers are allowed to be directly and intentionally attacked. This also applies to their equipment, supply routes and sometimes even their civilian distributors. The attacking of civilians that are engaged within the harming process of warfare, however, is problematic for this condition. Commonly civilians may not be attacked. However, when civilians are supplying the army, they indirectly take part in the harm, and they may be attacked. Yet the category of civilians that are engaged with harm can be considered very broadly. It would mean that it is ethically allowed to attack the electricity network, bridges, and other kinds of communal used facilities. This is the so-called dual-use problem. Yet, according to Orend, it is only justifiable to attack civilians that directly contribute to warfare.

The discrimination requirement has been designed for CW and not for IW. This brings up the question whether it is also applicable to IW. The relationship between the discrimination of combatants and civilians is similar in IW. However, when the cyber domain is used as a battleground, it causes obscurity with the distinction between different parties. When a cyber-attack is executed, civilians that are not engaged in any kind of harming should not be attacked. Cyber operations should only be directed against legitimate targets, which are the military and any other parties that are engaged in harming. There are some problems, however. Within traditional warfare, it is mandatory according to the rules of the Geneva convention that soldiers and people that are engaged in warfare have a particular dress code. Soldiers wear their uniforms, and for most equipment, it is evident, because of the color or just because of the system itself, that it is used for military ends. This is not so obvious for cyberwar and the direction of cyber-attacks. Cyber-attacks are easier to use anonymously than traditional kinetic attacks. This, however, is a matter of degree. There are examples of

conventional attacks that could not necessarily be attributed to one state or another. An example is the Abqaiq–Khurais attack on Saudi Arabia's oil infrastructure in 2019. Saudi Arabia still cannot say for sure who carried out these attacks (AP 2019). A traditional attack usually shows who the source of an attack is. A cyber-attack can be executed through a whole infrastructure of different IP addresses, which makes it difficult or even impossible for the other party to unveil who the attacker is. This, on the one hand, makes it hard to trace the aggressor, but on the other hand, it is also challenging to find the target of the attack. Therefore, it is easier with a cyber-attack to attack multiple targets that are not all relevant in order also to hit the right one. This, however, can put other people, like non-combatants, in danger, which is not justifiable according to the JWT (Lin, et al. 2012). This eventually means that it is more difficult to be sure the distinction is made in IW and that acts are executed with the distinction condition as a guideline.

In addition, the harm of an attack in the cyber domain does not necessarily have consequences that concern physical harm. Because there are no necessary physical consequences of harm, it is more effortless for states to execute such an attack on civilians or civilian systems. The risk of any severe consequences is less, which makes it less problematic to launch an IW-related attack on civilians than a conventional attack. This means that the distinction condition is less relevant for the moral assessment of IW.

We have seen that the distinction between *jus ad bellum* and *jus in bello* is no longer helpful in the case of IW. This does not apply to *jus in bello* and the relevance of this category and its conditions will be addressed in this subchapter. The *jus in bello* category comes with certain conditions that determine whether separate attacks in a war should be considered just or not and gives combatants a direction on how they are supposed to act when they want to act justly. These conditions have been designed to assess acts of conventional warfare and not IW. The conditions are discrimination, proportionality, and necessity. When these three conditions are met, according to JWT, a war is fought in a justifiable manner. This subchapter will explain the conditions and assess their suitability for IW.

2.2.2 Proportionality

The second condition of *jus in bello* is proportionality. This condition obligates soldiers, when the legitimate targets are known, to only use proportionate force against those targets. According to Orend (2013, p. 125), this requirement does not concern the war as a whole; it

instead is about the tactics of attacks in warfare. The condition requires that harm is done to achieve a benefit proportional to this harm. Singer (2015, p. 84) gives the prime example that 'in other words, if the other side stole your cow, you can't justifiably nuke their city'.

Proportionality is rather about the consequences of an action than about its intention. This means that proportionality in relation to cyber is only relevant when the consequences of a military operation within cyberspace end with kinetic or physical harm to civilians—for example, targeting an online military infrastructure to disrupt the communication systems between different units. This could cause military disadvantages but also a disruption in civilian communication systems as it is difficult just to target one system, and there is a chance that military and civilian systems are connected. This disruption of the civil system could lead to physical effects on the civil population, such as hospitals that cannot function as they are supposed to. These indirect effects of the cyber-attack could be considered disproportional. Jensen (2012, p. 207) puts it in contrast with the direct effects of a cyber-attack and explains indirect effects as 'effects [that] are the delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms. In the cyber domain, this would include damage that was not the intent of the attack, but that resulted from elements of the attack'. These indirect effects are hard to manage in practice, and this shows the difficulty of the application of the *jus in bello* proportionality condition in relationship to the high-tech emerging military technologies within cyberspace.

Another problem that illustrates why it is not possible to use the *jus in bello* condition on IW is that it is complicated to quantify the harm that is caused or will be caused by an IW-related attack. It is particularly difficult to determine for attacks that take place in the digital communication systems, such as disinformation. Such attacks are attacks that are used to change public opinion and manipulate the people of a state to put them against the same state. The consequences of such attacks are difficult to assess, as it is hard to tell in advance how people will deal with such things. It could be that nothing happens, but it could also happen that the people revolt against their own state.

2.2.3 Necessity

The last condition of *jus in bello* concerns necessity. The principle of necessity distinguishes which measures the military or state may use to accomplish an objective. The condition has both constraints and permissions. The permission is that it is allowed for the military to use whatever means necessary to attain a legitimate end. The constraint, on the other hand, is that whatever means that are not necessary for the use of attaining the legitimate end are unjustified in using (Blanchard & Taddeo 2022, p. 6). The condition governs that not every necessary action is permissible but that every permissible action should be necessary. With this is meant that it could be permissible – and thus justifiable – to perform actions that usually in war are not permissible. This could mean that when a state is under a direct existential threat by another state, it is permissible for the state that is under threat to not comply with the other conditions like proportionality and discrimination. For example, a warship seeking to avoid combat is unlikely to stop to help shipwrecked sailors, a surrounded force will find it difficult to fully comply with the rules governing the treatment of prisoners of war, and a small force retreating may have to destroy civilian communications facilities or buildings. However, when the legitimate end is accomplished, the loss of lives, the affected harm, and the damage to property must be kept to a minimum. For example, torturing and letting prisoners of war live under deplorable conditions. This kind of treatment serves no purpose for achieving any military advantages and therefore is not necessary.

It is challenging to apply this condition to IW. In CW, the general goal of the war and the attacks in the war is a victory upon the enemy. However, this does not seem to be so easy for IW. Since it is hard to determine whether a cyber-attack occurs in times of war or peace, it is also difficult to know what then the very legitimate end of a cyber-attack is. Usually, a cyber-attack or other IW-related kind of attack cannot be the decisive factor for ending a war and claiming victory like within CW. Most of the time, within IW, such a strategic target is still missing.

3. An Alternative Approach by Taddeo

As we have seen, new dilemmas and challenges arise when JWT is used as a tool to assess the justifiability of actions and attacks in IW. Mariarosaria Taddeo shares this position. Taddeo has written multiple articles on IW in which she undertakes a conceptual investigation of the matter and proposes an approach to the moral evaluation of IW (Taddeo 2011). In the article Just Information War (2014), she offers this approach based on an earlier conceptual investigation with the aim 'of filling the theoretical vacuum surrounding this phenomenon and of providing the conceptual grounding for the definition of new ethical regulations for IW' (2014, p. 213).

This chapter will provide critical analysis of Taddeo's views on how we should assess the justifiability of IW.

She argues that JWT is a necessary but not sufficient tool for the ethical analysis of IW. Taddeo's conclusion relies on two arguments: first, she argues that there is an ontological difference between the domains wherein contemporary warfare is waged. The traditional domains are all located in the physical realm, while the – new – cyber domain is not. Second, she argues, based on the former argument, that some principles from JWT cause problems when they are applied to IW. The reason for these problems is the ontological hiatus between IW and JWT. It is a characteristic of JWT and CW that warfare is violent with physical damage and bloodshed, while this is not the case for IW. She uses three conditions to substantiate her claim: last resort, more good than harm, and non-combatants immunity.

Subsequently, her solution to this problem will be discussed. According to Taddeo, the key to the deficiency of JWT in the application to IW is to merge JWT with information ethics (IE). In order to get a better understanding of her approach, Taddeo's account of IE will be explained in two steps: first, the goals of IE in this particular context will be explicated. Second, the relevance of the four introduced principles concerning IE for IW will be explained. Next, the merger of these two conceptual theories will be analyzed as a solution to the presented problem. This new theory is called Just Information Warfare (JIW). This theory is, as IE, based on three principles. The principles will be outlined to see how Taddeo thinks this approach is a better one than JWT.

Finally, Taddeo's approach will be considered from a critical perspective. There are a few major issues within the theory that demonstrate that the theory is unsatisfactory. The

approach is lacking for a few reasons: the first reason is that Taddeo tries to offer a solution to a broad range of problems with just one theory. In the approach, Taddeo suggests giving all kinds of entities the same ontological status. This, however, seems odd. In particular, it does not seem right to consider humans as occupying the same ontological domain – and therefore the same moral domain – as physical or informational objects. Secondly, it is questionable what Taddeo exactly means by her claim that the well-being of the *infosphere* should be the main criterion for assessing acts of IW. Thus, the principles she suggests as a solution for the problem rely on this terminology. However, the terminology seems to be ambiguous and hard to grasp. Thirdly, at one point, Taddeo writes: 'For it may be argued that, since IW can lead to victory over the enemy without incurring casualties, it is a kind of warfare (or at least the soft, non-violent instances of IW) that is always morally justified, as the good to be achieved will always be greater than the evil that could potentially be caused' (2014, p. 218). It, however, is dubious if there can be any question of victory within the constraints of IW.

3.1 Taddeo's Interpretation of Information Warfare

Taddeo uses the term IW to refer to a broad spectrum of different phenomena. These can range from cyber-attacks, and robotic weapons, to the use and management of communication systems. All these kinds of methods for waging IW have one thing in common, and that is that they rely on information or information systems. Taddeo chooses to endorse the concept of IW through a wide spectrum because it provides methodological benefits (Taddeo 2014, p. 214). From that perspective, she gives IW the following definition:

'Information Warfare is the use of ICTs within an offensive or defensive military strategy endorsed by a [political authority] and aimed at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging across the physical and non-physical domains and whose level of violence may vary upon circumstances' (Taddeo 2012, p. 114).

3.2 Taddeo's Problem

To give a solution, a problem is required. In the first chapter we have seen that there is a problem with the application of JWT to IW. The scholar Mariarosaria Taddeo has got the same

view. However, Taddeo's approach to this problem is different. There are two reasons why Taddeo thinks JWT falls short for IW.

3.2.1 The Ontological Problem

The first problem of the application of JWT on IW is an ontological problem, according to Taddeo. She claims that 'the problem arises because JWT mainly focuses on the use of force in international contexts and surmises sanguinary and violent warfare occurring in the physical domain. As the cyber domain is virtual and IW mainly involves abstract entities, the application of JWT becomes less direct and intuitive. […] and for this reason it does not provide sufficient means for addressing the case of IW.' (2014, p. 216). Taddeo claims that this so-called hiatus adversely affects the ethical analysis of IW for the reason that JWT is a theory that follows an anthropocentric approach, and it disregards all kinds of non-human entities.

In her own words, she states that 'the transversality of the ontological status of the entities involved in IW is particularly relevant as we try to shed some light on IW's novelty. Traditional warfare concerns human beings and physical objects, while IW involves artificial and non-physical entities alongside human beings and physical objects' (2014, p. 216). In simple words, this means that CW is waged in the traditional physical domain, and IW is waged in the nontraditional cyber domain. She considers this difference a problem. Taddeo supports the view by using Dipert, who argues that it is necessary for IW to identify and distinguish the different kinds of objects that are relevant; in this case, he calls them 'information objects' (Dipert 2013, p. 36). IW, or cyberwarfare in the words of Dipert, in this sense, surpasses traditional characteristics of conventional warfare.

The following example, according to Taddeo, shows why the ontological aspect is of importance and asks for further research. There are cases of autonomous computer viruses, like Trojan horse viruses. These viruses do not need any supervision or control once they are programmed for a purpose. They can individually identify their targets with only the help of the internet – and the programming in the first place. Once the target has found the objective, however, it can autonomously attack the objective without any authorization of the designer of the code or any other human agent. Based on this computer virus example, Taddeo explains that there are three questions that arise when considering the ontological distinction and the case of an autonomous computer virus.

In this moral scenario, there are a few things differently from a conventional attack. The first question Taddeo asks is about the moral agent. In CW it is, most of the time, clear who executes an attack. Especially when there are witnesses, it is hard to doubt who pulled the trigger or pushed the so-called red button. There can be a discussion about the guilt of the trigger puller and the one that commanded the individual to pull the trigger, but we can assume in that case that the one who pulls the trigger is responsible for the consequences of pulling that trigger or pushing that red button. This, however, is not the case for an IW-related question in Taddeo's view. She questions who can be seen as the responsible moral agent in such a case 'for it is unclear whether the virus itself should be considered the moral agent or whether this role should be attributed to the designer or to the agency that deployed the virus, or even to the person who actually launched it' (2014 p. 217).

The second question, which is also more evident in CW, addresses the question of who can be considered the 'moral patient' in a cyber-attack. In CW, the ones who suffered any kind of damage and are harmed can be regarded as moral patients. Taddeo, however, questions if, in IW, computer systems next to people can be considered moral patients. It is an interesting question, but when the answer is yes and computers should be taken into such consideration as being moral patients, this would have significant implications. It could mean that we, as humanity, should also apply other kinds of moral reasoning to computer systems and other types of non-biological beings. The third question is in line with the former two questions and asks to what extent rights should be attributed to such systems and their users.

The third question is in line with the former two questions and asks to what extent rights should be attributed to systems attacked in IW and their users. Taddeo is not completely clear about this last distinction. Indeed, it is quite important that the users of information or users of computer systems should have rights in IW. However, it seems in the last question that Taddeo considers the systems and the users more or less the same. This is problematic because it is debatable whether moral value can be ascribed to physical objects. As we have seen, on the basis of these questions, intangible objects and entities are brought into the moral domain.

3.2.2 Conditional Problems of Just War Theory

As discussed in chapter 2, there are multiple categories in JWT. These categories subsequently have their own conditions, which should be met in order to know whether a war is fought

justly or not. Taddeo has her own approach to these conditions. According to her, there are only three tenets of JWT. Taddeo does not give a reason why only these three conditions are 'tenets' of JWT and others or not. These are the conditions: last resort, more good than harm and non-combatant immunity. If these conditions, or tenets as Taddeo calls them, are compared to the *jus in bello* conditions, there are some similarities. Last resort is a condition that is not addressed yet since it is a condition that falls under the *jus ad bellum* category, which was considered to be less relevant for the evaluation of IW. This condition entails that warfare should always be considered the last in a range of options. Only when all the options before starting a war are exhausted and there is no other way of solving certain serious problems a war is justified to be started. The last resort condition is similar to the possibility of excessive use of self-defense. When one is cornered, and one's life is threatened, the law allows you to use lethal force against the aggressor. It could be said that this also applies to war. Only when there is no other option left war may be initiated. The second condition, more good than harm, can be considered the equivalent of proportionality and necessity. The third condition, non-combatant immunity, can be regarded as the same as the distinction principle. With the ethical analysis of these conditions, Taddeo argues that 'that the nexus of the ethical problems posed by IW rest on the ontological hiatus between IW and JWT' (2014, p. 217).

Taddeo argues that the application of the condition of 'last resort' is problematic for IW. IW is not necessarily a bloody and violent kind of warfare, and therefore it may be a better option that averts a kinetic attack that could lead to conventional warfare. But, because the attack of IW is considered to be an act of war, this would not be allowed, according to JWT. This could mean that it is better to allow and justify soft and non-violent cases of IW in order to prevent worse. Taddeo, however, does not give any guidelines on how IW would be better when a related attack is launched than the words 'soft and non-violent'. This seems to be ambiguous for the reason that it is, just like with other forms of attacks, difficult to foresee any consequences of an attack. Even when an attack may seem to be 'soft and non-violent', it could turn out to have catastrophic consequences. Although that Taddeo argues that IW should not always be a last resort, this is questionable because the implications of an IW-related attack are difficult to foresee.

The second condition Taddeo addresses is the 'more good than harm' condition. This condition also creates a problem. Taddeo states that 'according to this principle, before declaring war, a state must consider the universal goods expected to follow from the decision to wage war, against the universal evils expected to result, namely the casualties that the war is likely to produce. The state is justified in declaring war only when the goods are proportional to the evils. This is a fine balance, which is straightforwardly assessed in the case of traditional warfare, where evil is mainly considered in terms of casualties and physical damage that may result from a war. The equilibrium between the goods and the evils becomes more problematic to calculate when considering IW' (2014, p. 218). This raises a problem because it is, according to Taddeo, not necessary for IW to be a war where there would be any casualties. When there are no casualties or any other kind of physical harm, this would mean that such warfare would always be morally justified for the reason that the good achieved will always be more significant than the evil that potentially could be caused.

However, she argues that it is possible for IW to have unethical actions as a consequence. Despite the fact that the condition only takes physical harm into consideration as an 'evil' that can outweigh the 'good' that can be achieved, Taddeo thinks tout court that destroying a digital resource containing vital records is deemed to be an ethical action, despite the fact that it does not constitute physical damage. It is questionable that Taddeo argues tout court that this kind of harm is a 'harm' that can outweigh the goods it creates. CW focuses on physical damage, and it is disputable just to say that this kind of damage – the destruction of digital resources – can be considered wrong.

The third condition Taddeo queries in relation to IW is the requirement of 'discrimination and non-combatant immunity'. In traditional warfare, this condition entails the distinction between the military and civil society. This condition in CW, however, has become more ambiguous in the last few decades with the emergence of guerrilla warfare and terrorism. For IW, this distinction has wholly disappeared. Almost everyone globally has access to a computer and can execute IW-related attacks from their homes while continuing with their civil lives. This does not only apply to human beings but also to objects and systems. What can be considered to be a civilian target, and what as a military target in the contemporary world?

3.3 Taddeo's Solution

For every problem, there is a need for a solution. Taddeo also designed a solution to solve the problem that has been considered in the previous. According to Taddeo, the ontological problem that arises can be solved by merging two theories. These theories are Just War Theory and Information Ethics. This subchapter will be concerned with explaining, on the one hand, the purposes of IE and, on the other hand, the principles associated with it, the way that Taddeo exhibits them and how she applies them on IW.

3.3.1 The Goals of Information Ethics

In general, IE can be defined as a branch of ethics that 'that focuses on the relationship between the creation, organization, dissemination, and use of information, and the ethical standards and moral codes governing human conduct in society' (Joan 2010). Taddeo considers it as fulfilling a blind spot that should be perceived as a kind of macro-ethics. This blind spot taken into account by IE is the shift from an anthropocentric moral view to an ontological moral stance that is necessary to understand morality when assessing things as information. This object-oriented view is more applicable in modern society, where information is the common thread of living our lives. This kind of approach, therefore, can help us understand moral questions better, have a better look at the right or wrongfulness of human actions, and so on, could give us a better understanding of the ethical and moral values or theories we would want to foster. The justification of information warfare depends on IE because it answers inevitable questions concerning the moral status of informational entities involved within information warfare, such as who the moral agents are, who the moral patients are, and what the rights are of those two.

One of these questions that emerge is about the ontological status of agents in IE and how they differ from those moral agents in traditional ethics. According to Taddeo (2014, p. 219-220), IE is a macro-ethics. It concerns the realm of reality and analyzes ethical issues looked at from an informational perspective. This means that IE is primarily about considering the always radically changing contexts of information where specific ethical issues emerge. This forces us to look different at new problems that appear because of the technological developments within the information domain and to rethink, methodologically, certain ethical positions that were formerly considered to be correct. She defines IE as "a patient-oriented, ontocentric, and ecological macroethics." (p. 220). It is patient-oriented because it looks at

the morality behind an action with respect to the receiver of the consequences of that specific action. The 'patient' of the information action is the most important agent. Marco-ethics is ontocentric because it does not take humans as a central aspect in its approach for analysis. All existing things or entities are taken into consideration instead of just humans. An entity in this context should be considered as a "consistent packet of information, that is an item that contains no contradiction in itself and can be named or denoted in an information process" (Floridi 1999, p. 43). The existing entities are to be considered from an informational standpoint and thus as informational entities. They all have the same nature due to this principle of ontological equality. Every form of entity has got its own informational value.

Taddeo explains this on the basis of the level of abstraction (LoA). A LoA, according to Taddeo, is 'a finite but not empty set of observables accompanied by a statement of what feature of the system under consideration such a LoA stands for. A collection of LoAs constitutes an interface. An interface is used when analysing a system from various points of view, that is, at varying LoAs. It is important to stress that a single LoA does not reduce a car to merely the aerodynamics of its parts or to its overall look. Rather a LoA is a tool that helps to make explicit the observation perspective and constrain it to only those elements that are relevant in a particular observation' (Taddeo 2014, p. 214). The LoA, however, does not matter for the informational value an entity has. It still has got informational value. This applies to a grain of sand, giving information about its existence within our reality, as to a radio frequency, which is the actual sender of information. According to IE, an anthropocentric approach would not be sufficient for an effective moral analysis of information. The level of abstraction would prevent the analysis from adequately considering the nature and the role of the other than biological entities within the reality. This, however, does not mean that every entity has the same kind of information value. They can differ in the amount of information that is given. The moral value of an informational entity within the information sphere or *infosphere* is determined by the potential informational contribution it can provide within the *infosphere*. This *infosphere* includes every entity, digital or analog and physical or nonphysical. According to IE, the blooming within this *infosphere* is the ultimate good. The destruction or corruption of it is considered absolute evil. This destruction is also called entropy. The moral agents acting to let the *infosphere* flourish are thus moral actors, while the agents that try to destroy the *infosphere* are to be considered as instances of evil.

According to this approach, IE gives four principles that distinguish right and wrong and the duties of a moral agent. The principles are (Floridi 1999, p. 47):

0. entropy ought not to be caused in the infosphere (null law);
1. entropy ought to be prevented in the infosphere;
2. entropy ought to be removed from the infosphere;
3. the flourishing of informational entities as well as of the whole infosphere ought to be promoted by preserving, cultivating and enriching their properties.

3.3.2 The Application of IE and JWT to IW; Just Information Warfare

According to Taddeo, JIW relies on IE. The different entities within warfare– or the ontological status of these – should be demarcated to determine the status of the moral agents involved. While this is more difficult to do within IW, the ontological status of those entities should be determined. As discussed in the last chapter, every entity in reality, physical or nonphysical, human or artificial, has got a certain ontological status and an informational value. These values can override each other based on their moral status, but they still have a certain kind of informational value within reality.

According to Taddeo, all entities that may be affected by an act of war should be considered moral patients. This means that a human being, as a software or hardware system, could be an entity that should be considered as a moral patient affected by war. The actual moral value of an action in war depends on the value of the moral patient within the *infosphere* and how it contributes to the flourishing of this *infosphere*. It is, for example, less destructive to the *infosphere* when an empty USB stick is destroyed in comparison with a whole data center that provides an informational structure for a government. Taddeo argues for three principles within JIW (p. 221):

(A). IW ought to be waged only against those entities that endanger or disrupt the well-being of the infosphere.
Two more principles regulate just IW, they are:
(B). IW ought to be waged to preserve the well-being of the infosphere.
(C). IW ought not to be waged to promote the well-being of the infosphere.

The first principle (A) provides the condition under which it is justifiable to resort to IW. The resort to war is only justifiable when there are entities that endanger or disrupt the well-being of the *infosphere*, and the war is only meant to be directed at those entities. This means that an information war could be directed at multiple kinds of entities as all kinds of physical or nonphysical objects, in reality, are informational entities. Accordingly, information warfare could also be in the physical or nonphysical domain. In practice, however, this would probably be mostly about people using certain kinds of software to disrupt the *infosphere* or the software or viruses itself that should be attacked.

The second (B) and third principle (C) are there to regulate the first principle. They prescribe how to be sure that the first principle is complied with. The second principle is there to preserve the well-being of the *infosphere*. When a malicious entity attacks the *infosphere* with the goal of targeting a strategic goal, the consequence is the entropy of the *infosphere*. The second principle assures that the damage, or entropy, caused by the malicious entity is repaired and restored to let the *infosphere* flourish again. Taddeo uses an analogy of the police force in society to make this second principle clearer. The police (IW) in society (*Infosphere*) are not there to pro-actively coerce people to do the right thing. The police are there to ensure that malicious things are prevented or reduced within society. They do not actively want society to flourish as much as it could. The police have an executive role in countering undesirable practices. This state of political order, however, is something that, especially in times of war, cannot be assumed. Other people, like policymakers, are the ones that try to let society flourish. This second principle, however, is like the police. IW is just when it tries to prevent entities from acting maliciously within the *infosphere*.

The third principle (C) prescribes IW should not be undertaken to promote the well-being and flourishing of the *infosphere*. IW should only be used as a deescalating measure and as a last resort. The analogy of the police or the army could also be applied with the third principle. Those entities or forces should only be used to prevent things from happening or when it is the last resort and to defend themselves and prevent worse things from happening. It should not be used to promote the flourishment of the *infosphere* actively.

According to Taddeo, the application of these three principles – (A), (B) and (C) - overcome the 'ontological hiatus' by endorsing 'an informational ontology, which allows for including in the moral discourse both non-living and nonphysical entities. The principles also

prescribe respect for the (minimal and overrideable) rights of such entities along with those of human beings and other living things, and respect for the rights of the *Infosphere* as the most fundamental requirement for declaring and waging a just IW.' (2014, p. 222). Taddeo demonstrates the use of the principles according to the application to the mentioned conditions from chapter 3.1.2. In this way, she also illustrates how IE and JWT go together and thus solve the problems introduced earlier.

The condition of last resort can, with the help of IE, be used for IW because the first principle (A) of JIW prescribes that an entity that dangers or disrupts the *infosphere* loses its rights and becomes a licit target. A state then, according to the second principle, is allowed to repair the *infosphere* and re-establish the harm that is done. According to Taddeo, this means that the traditional and problematic approach of the last resort condition is overcome because such an action can avoid CW, which could even be a more significant threat to the *infosphere* than IW. In this case, Taddeo says that it would be allowed to use IW, even when there are other options possible, and this is not necessarily a last resort.

The second problem concerning the condition 'more good than harm', is avoided, according to Taddeo, when harm to nonphysical entities is considered as well as physical damage. This, however, is hard to imagine because physical damage can only occur in the physical war and thus through kinetic attacks or attacks that in some way have implications for the physical world. Taddeo explains this consideration by claiming that the assessment of 'good' and 'harm' can be determined by considering the state of the *infosphere* as a 'before and after' waging war. From this approach, the condition of 'more good than harm' is a corollary of the second JIW principle (B). In this way, IW only restores the state of the *infosphere* before the war and does not raise the amount of entropy or disorder in the *infosphere*. It is, however, the question of how the second principle takes care of this. Taddeo does give any tangible methods of how this restoration is done.

The three principles, and in particular the first principle (A), also help to overcome the problem of 'discrimination and non-combatant immunity'. In IW, the distinction between military targets and civil targets is blurry because recognizability is not a necessary condition for a military status in IW. This makes the condition problematic for the application in IW. However, the distinction still is a necessary one because it is required for a just war to target licit and not non-licit targets. The first principle (A) says that IW can justify attacks against malicious entities, being military as civil. When an entity is disrupting the *infosphere*, it is

necessarily evil, and it is justified, according to Taddeo, to attack these entities. This means that all evil entities, civil and military, are justified to attack if we should believe the first principle (A). In her own words, Taddeo states that 'the social status ceases to be significant in this context, because any entity that contributes to increasing the evil in the *Infosphere* loses its initial rights to exist and flourish and therefore becomes a licit target. More explicitly, it becomes a moral duty for the other entities in the *Infosphere* to prevent such an entity from causing more evil' (2014, p. 222).

3.4 The Shortcomings of Taddeo's Solution

Taddeo's article, 'Just Information Warfare', is a valuable addition to the literature on IW and JWT. However, her theory does not seem to be entirely satisfactory and to solve all of the problems that arise when thinking about a guiding ethical framework for IW. It is questionable if the ontological problem she explains, really is a problem. In addition, it seems that Taddeo's theory itself has problematic consequences. She tries to solve all the issues that are accompanied by IW with a single theory. It is the question if this is even possible. In this subchapter, three issues of Taddeo's Just Information Warfare theory will be introduced and discussed.

3.4.1 A Terminological Issue

Taddeo correctly addresses the fact that IW is not a single form of warfare but rather an 'umbrella' that consists of the different forms of ICTs. However, she nonetheless aims to find a theory to evaluate these different kinds of ICTs and their consequences in the same way. But IW is a term that needs to be diversified because it is too broad. Thus according to Stevens (2012), the term IW has fallen apart in the last few decades. It is hard to distinguish and know what exactly falls under the terminology, and therefore governments and militaries have stopped making use of the term. The definition of Taddeo in chapter 3.1 makes it even more challenging to determine what is covered by the definition of IW and what is not because it is so broad. Because the use of this terminology is in some sense outdated, it is questionable if it is useful to continue using it. What is the benefit of using an obsolete term when significant institutions such as the government and the military do not use it anymore because it is too broad?

3.4.2 The Concept of Harm

Next to the terminological issue, there also is the issue of different kinds of harm. In the context of warfare, harm is usually considered to be a kind of physical damage or injury towards an object or person. There are different kinds of harm and different kinds of attacks. Other than physical harm, there is information, espionage, and disinformation harm. However, it seems that Taddeo makes no distinction between these kinds of harms and considers them all to be the same. In her view, just one theory solves all the problems that are related to the different kinds of harm. This approach relies on the principles she introduced for a just IW. According to Taddeo, all the entities that endanger or disrupt – or malicious entities – the so-called *infosphere* cause the same implications to the *infosphere*. The outcome of JIW is, therefore, that harm to people – human beings – is evaluated in the same way as harm to digital objects.

The concept of the *infosphere*, however, is vague and raises questions. The *infosphere*, according to Floridi, 'includes all existing things, be they digital or analogue, physical or non-physical and the relations occurring among them, and also between them and the environment. The blooming of the *Infosphere* is the ultimate good, while its corruption, or destruction, is the ultimate evil' (2014, p. 220). This means that the introduction of just one concept, namely the *infosphere*, implies that all entities can be considered to be entities that coexist with each other in the same domain. It is questionable if this concept is right. The consequence is that all entities are related and thus can be compared to each other on the basis of their informational value to the *infosphere*. It seems to be against intuition, however, to compare a human being and software. A human being has a certain moral value in life which has a certain appreciation in our society and asks for an ethical consideration. This is not always the case for software or any other kind of digital entity. People clearly would care less, in general, when software is destroyed than when a human is killed. The software can be created again; the human being cannot. The call for ontological equality by Taddeo, therefore, has questionable repercussions. Intuitively, physical harm is a different and more severe type of harm than the harm done in the digital domain. Thus, the harm done is different and also should be treated otherwise. In addition, Taddeo explains the ontological problem based on three conditions of JWT, which she calls the 'tenets'. She, however, never explains why she uses exactly these three conditions and not the others. It is unclear why these conditions are

the fundament of JWT and others are not. Most scholars, for example, consider the just cause condition as the most critical condition of JWT.

3.4.3 Well-Being and Destruction of the *Infosphere*

Another problem of this theory of Taddeo is the ambiguity of the concepts 'well-being' and 'disruption or destruction'. The *infosphere* already is a vague concept, but how should we understand its well-being or destruction? She never explains what she means by these two concepts. How are we supposed to know what is good or bad for the flourishing of the *infosphere* when there are no guidelines what the actual well-being or destruction is? The only thing Taddeo says about the destruction or disruption is a quote from Floridi: 'In particular, any form of corruption, depletion or destruction of informational entities or of the *Infosphere* is referred to as entropy. In this case, entropy refers to ''any kind of destruction or corruption of informational objects (mind, not of information), that is, any form of impoverishment of being, including nothingness, to phrase it more metaphysically'' and has nothing to do with the concept developed in physics or in information theory' (2014, p. 220). This tells us that the destruction of the *infosphere* is called 'entropy', but it does not tell us what it really entails. What should be considered as the corruption or destruction of informational objects? This is not clear. In addition, nothing is said about the well-being of the *infosphere*. Should the well-being of the *infosphere* be considered as the absence of corruption or destruction? It is difficult to know what Taddeo exactly meant because she did not elaborate on it. This incompleteness causes questions that are not answered in her article.

In addition, according to Taddeo, the *infosphere* is a kind of domain in which everything exists. She writes about the well-being and disruption of the *infosphere*. To demonstrate the ambiguity and subjectivity of this concept, these can be compared to the different kind of forms of state worldwide. The Western world clearly has another view on how the world should be put together than Russia or China. Where the west thinks capitalism and free-market thinking work best, Russia and China prefer socialism and communism. When countries are not even on one line according to these views, what should the *infosphere* look like? With this example, I try to illustrate that a concept as well-being is subjective and that different people have different ideas of how this *infosphere* should be furnished. This is also the case for politics.

3.4.4 An Impossible Victory

In Taddeo's analysis and application of the three conditions of JWT on IW, Taddeo writes about victory in IW: 'For it may be argued that, since IW can lead to victory over the enemy without incurring casualties, it is a kind of warfare (or at least the soft, non-violent instances of IW) that is always morally justified, as the good to be achieved will always be greater than the evil that could potentially be caused' (2014, p. 218). It is questionable, however, if there can be any question of victory for IW. Since IW is not a continuous kind of battle, as is discussed in Chapter 2, and the attacks in relation to IW should be considered as separate stand-alone attacks, it is not right to state that there can be any victory after such an attack. These attacks lead to advantages or military gain in IW and CW, but the chance of ending a war is slight. Therefore, the use of the term victory is not correct in this context.

4. A New Approach to Information Warfare

This thesis proposed and analyzed two theories that may provide a solution to the question of the justifiability of the conduct of IW. These two theories, JWT and JIW, however, did not offer entirely satisfactory answers to the question of how IW may be morally evaluated. They were not satisfactory in their aim to create a moral framework for IW as one thing. IW, however, is not just one thing; it is a broad concept that consists of multiple different things. From this starting point, we will consider to what extent JWT, particularly the *jus in bello* condition, is applicable to different kinds of attacks that are part of the broader concept of IW. What both the theories did do, however, was show us the problems that arise when trying to morally evaluate IW. This chapter will revisit these problems to try and bring the solution closer.

The aim of this chapter will be to demonstrate that IW is a broad concept that needs to be divided into different categories of harm and forms of attacks. In this chapter, we will take a closer look at the individual types of attacks and their consequences in order to see how we can morally assess each type of attack individually. And whether it is possible to use JWT as a starting point to evaluate these types of attacks. For determining the different kinds of attacks, the perspective of Libicki (1995) will be used. He distinguishes between seven forms of IW. These forms are command-and-control, intelligence-based, electronic, psychological, hacker, economic information and cyber. In addition, Nichiporuk (2002) came up with other forms of IW. These are operational security, electronic warfare (EW), psychological operations (PSYOPs), deception, physical attacks on information processes, and information attacks on information processes. Of all these forms, the following will be used: command and control warfare, intelligence-based warfare, electronic warfare, psychological warfare, information attacks on information processes and operational security. Subsequently, different kinds of harm will be introduced and discussed. The response to an attack will depend on the damage done to the affected party. Depending on this damage, it can then be determined how a state should respond. The different kinds of harm are physical harm, information harm, espionage harm and disinformation harm.

In order to demonstrate the necessity and utility of the partitioning of the concept of IW, a few steps will be followed. First, the different forms of attacks will be considered and categorized on the basis of the harm they do. Secondly, the various categories of harm will be

introduced. The last and final step is using the categories of harm and the different forms of IW attacks to determine how a state could best consider an attack in order to find an appropriate response to such an attack. This will be done by putting the different forms of attacks to the test based on the conditions of JWT. This kind of approach does not necessarily give states a moral guideline on how to respond to IW-related attacks, but it brings the solution to this dilemma closer.

4.1 Different Forms of Information Warfare

In 1995, Martin C. Libicki wrote the book 'What Is Information Warfare?'. The reason for writing this book at the time was the emerging popularity of the concept of IW. Information technologies became more important for national security in general and especially for warfare. He predicted that these information technologies would become more and more relevant in the war domain and those who would master the techniques would have a military advantage over the ones who did not. He was right. Because the definitions, at the time, of IW, were too broad, Libicki suggests dividing the concept into seven different forms. The reason he does this is because one approach can take over the whole interpretation of the concept, while it may have more to offer. And, by giving a concept a too broad definition, it could cause an impossibility of finding the conceptual thread of the concept other than that IW is about information and about warfare. When the definition is more specific, the conceptual thread might be easier to find (Libicki 1995, p. 3). Another author that wrote on the same subject is Nichiporuk (2002). Nichiporuk gave five forms of IW. For the analysis, the most relevant forms of IW of the works will be used.

Despite the fact that these works are almost thirty years old, they present in a nuanced way why it is important not to approach a concept like IW in its generality but rather to break it down and deal with the specific aspects instead. This is also of importance when addressing the question concerning the morality of IW. Especially in this context, it is particularly relevant to use four of Libicki's forms of IW and two of Nichiporuk's. As we have seen in the former chapter, IW should not be considered as just one broad concept, but it should be assessed piece by piece, and one theory is not enough for assessing the different kinds of attacks. Not every attack in IW is the same, and different kinds of attacks ask for different kinds of responses. In the following, however, these forms of IW will be considered as attacks since the main question is about how states should respond to attacks in the spheres of IW. To

determine what form of IW – or attack – should be categorized in what category of harm, the attacks will be briefly discussed in this subchapter. The implications of these attacks and the dilemmas that come with them will be addressed in the following subchapter.

Command and Control Warfare

The first form of IW-related attack is command and control warfare (C2W). This kind of warfare, and especially the attacks that come with it, are not a new phenomenon that only occurs in IW. In CW, the use of these attacks has also been common. The aim of such an attack is to fully disable the command and control by killing, in CW, or destroying, in IW, the commander or the commanding systems of the military unit. The place of the command, however, shifted in CW, and it was not necessary anymore for the command to be part of the battlefield. This meant that the command was able to control the warfare from a location where it could not be targeted anymore by the enemy. This stopped when missiles and airplanes were developed, and the command could be targeted globally. However, IW shifted the accessibility of targeting the command again. In the contemporary world – and this is an adequate point of Libicki, especially for the time he wrote this – the command and control are shifted from the commander to a command center. These centers are a strategic place behind enemy lines where the strategy of a war is determined based on electronic communication systems. This is not a new aspect of war, but the size of the communications load is a new aspect. War in the contemporary age relies on communication systems. When a fighter jet cannot rely on its communications systems, it will not be allowed to justify an attack. When a C2W attack is executed, this can be through information systems, for example, a computer virus that shuts down the command center of the enemy. It can also be a physical attack. A bomb does the same job as a computer virus and probably even better. A computer virus does not physically destroy other computers, while bombs do. It is easier to reprogram a computer than to acquire new ones. C2W can be considered as attacks on systems (Libicki 1995).

Intelligence Based Warfare

The second form of IW is intelligence-based warfare (IBW). This kind of waging warfare and executing attacks is a direct form of intelligence that is ‘fed directly to operations’ (Libicki 1995, p. 19). This means that in contrast to other kinds of attacks, these intelligence attacks are used to gather the information that results in direct physical attacks on humans, objects

or information systems. The use of intelligence in warfare is different for CW and IW. In traditional warfare, intelligence is used so that the command knows the disposition, location, and intention of the enemy. When this information is known by the command, the command will not be surprised by enemy attacks and can anticipate on the plans of the enemy. It creates situational awareness. In IW, however, a shift takes place. Because the information systems are able to do a lot more than before, in CW, there is a lot more information that can be stolen and so on used to create more situational awareness than before. The goal of IBW, however, stays the same as in CW, but the means are different. Now that information and computer systems have taken a significant part in the battlefield; there is less risk to be taken into consideration. This makes it easier to execute IBW attacks. IBW can be considered as attacks by systems (Libicki 1995).

Electronic Warfare

Electronic Warfare (EW) is an operational kind of warfare in comparison to the former two kinds of attacks. EW entails operational techniques, i.e., it concerns the war in the realm of communication. This can be done through (radio)electronic systems or cryptography. A form is antiradar. This is manipulating radar technology of the enemy. Although this kind of attack seems to be outdated, it is not. In contemporary warfare, radar systems – more advanced than before – still are very important for secret attacking or being aware of the enemy. Another kind of EW is by attacking and communication systems of the enemy. This is more complex than radar jamming, but when it works, it can be even more effective. The last way of EW is cryptography. Cryptography is also still very relevant in contemporary warfare. Although computer systems are more developed since it is still imperative that states protect their own communications by scrambling their own messages. And as a part of IBW, states can unscramble the communication of enemy states in times of war.

Psychological Warfare

Psychological warfare (PW) is the use of information against the human mind. This means that propaganda or disinformation can be used by a state to influence the civilian population or other information that can demoralize the military troops. This can be done through multiple methods. One of the methods is creating an image of a war that shows the people of the country wrong information, which could lead to the loss or rise of support by the people of a

state. In this way, the people of a state can be manipulated by information. When the state has no support of its people, most of the time, it is not sufficient to continue a war. Another way of using PW is by using (dis)information to discourage the enemy forces or their people. This is in line with the former use of PW. What also can be considered a PW attack is the misleading of the command of the military. The command could refer to a commander, command center, diplomats and even spies (Libicki 1995). These can all be misled using PW. An excellent example is operation Mincemeat. The allies misled the Germans by throwing a body in the sea with documents that said they would land on Sardinia instead of Sicilia. The Germans believed this, and the invasion of Sicilia by the allies was successful (Beard 2013).

Information Attacks on Information Processes

Information attacks on information processes (IAIP), in contrast to physical attacks, almost solely refer to attacks targeted at computer networks. The goal of HW is to breach these networks through knowable holes in the computer networks' security system. This means that for a hacker, the degradation of a system almost always lies in the system itself, which the hacker tries to exploit. The intents and implications of IAIP can vary from a shutdown of the system to stealing information from another network. Examples of attacks are a simple breach of a system – guessing the correct password – to Trojan horses, logic bombs and other viruses (Nichiporuk 2002, p. 188). This kind of warfare and the attacks are very similar to C2W.

Operational Security

This last form of IW is not a kind of attack in the direct sense. Operational security (OS) can be a form of an attack when a state is attacked by another state, but it is primarily preventive. Operational security consists of a few things. First, there is literal security. When the door is closed, it is difficult to get in. When the door is locked, it is even more difficult. And when there is no door, it is almost impossible to get in. This is also how security works in operational security and IW. A state can determine itself, dependent on the knowledge and the amount of money they are able to spend, how developed and up-to-date its ‘cybersecurity’ is. This, however, is expensive because other states also tend to develop further and further, and the keys for the door change continuously.

Another form of security, which is also common in CW, is deterrence. This kind of security has worked well in the past in CW as other kinds of warfare that are not conventional,

like biological and nuclear warfare. Nuclear deterrence helped to ensure that the cold war between the Western world and the Soviet Union did not escalate to a third world war. (Robinson & Janicke 2015, p. 88) While there is one part of defense that is concerned with the actual holding back of attacks, cyber deterrence is occupied with discouraging the enemy from striking in the first place. Cyber deterrence is a security because it ensures that enemies know that when they launch some kind of IW-related attack, they can expect a response to the same attack.

OS is relevant to all kinds of harm. Since OS is occupied with defending a state from all kinds of harm that can be done, OS is applicable to all kinds of harms that will be discussed in the following. Harm is something that should be prevented, and this is the goal of OS.

4.2 The Partial Breakdown of Harm

If a state wants to know what responses are right to what kind of attacks, they should take the consequences of an attack – or the harm done to them – into consideration. Attacks are not always successful, and when an attack is not successful, it is questionable whether it is even justifiable to respond to such an attack. However, it is necessary to make a distinction between different kinds of attacks in order to categorize them into different categories of harm. Because when an attack is successful, one can think about what response is appropriate. Now we know what sorts of attacks there are in IW, we can have a look at the consequences of these. This approach is an answer to some of the problems that arise when directly applying the conditions of JWT to IW.

I distinguish four categories of harm. These categories are physical harm, information harm, espionage harm and disinformation harm. The distinction between these is made because the main implications of attacks in IW concern the destruction of objects or injury to living beings, the destruction or disruption of entities in the digital domain, the theft of (crucial) information by other states and the deceiving of systems or people. In this subchapter, the different categories of harm will be discussed individually, and the different forms of attacks in IW will be attached to the categories of harm. The different kinds of harm, however, also bring specific dilemmas with them. These different dilemmas that arise need different kinds of answers to solve them. Based on the *jus in bello* category of JWT, the dilemmas will be addressed and will be assessed to what extent the category of *jus in bello* can contribute to the assessment of these harms. We will see whether this category can help

states in helping to provide a proportionate response to specific attacks or harm. To find that out, we can one by one try and apply the conditions on this kind of harm in relation to IW. Because the different forms of attacks are attributed to the categories of harm, it can be known whether the *jus in bello* conditions works or not.

4.2.1 Physical Harm

To this category, the following forms of IW can be attributed: C2W, EW and OS. C2W can be attributed to this category because these kinds of attacks are directly focused on targeting information systems. This can be through informational harm and putting down the system, but this can also be done by physical attacks. Putting down a power grid in order to disrupt a command center is an example. What also could be done is using robotic weapons to kill a person who is in command directly.

Electronic warfare can also be considered to cause physical harm because the jamming of radar or communication systems can result in the disruption of the navigation of vehicles which in order could lead to the destruction of these or the injury of humans.

The first category of harm is physical harm. Physical harm is the most obvious kind of harm. All types of harm that have direct physical negative implications to the outer world should be considered physical harm. Within this category, there are two forms of physical harm that should be scrutinized. The first form of physical harm is harm to physical objects that are not human. The second kind of harm is the harm to human beings due to a physical attack. The consequences of such an attack on humans, however, do not necessarily have to be physical.

The first kind of physical harm, the harm that is inflicted on objects, is relatively straightforward in CW. An example of this physical harm is a missile attack. When a missile is launched and it reaches its target, it explodes and destroys everything in its immediate surroundings. However, attacks in IW may also cause physical harm. An example of physical harm done by such an attack is the Ukraine power grid hack in 2015. The information systems of three energy distribution companies were compromised, which resulted in disruption of the electricity supply for consumers. About 230.000 people could not use the electricity for one to six hours (Zetter 2016). This example shows that it is possible that a combination of different IW attacks can cause physical harm to, in this case, a physical object. In this example, the consequences were not necessarily disastrous to the object, the power grid, but it could

have caused the power grid to stop working. One can imagine that there is actual physical damage when a power grid is not working for several hours or days. When the power grid of a nuclear plant is targeted, for example, the nuclear elements cannot be cooled anymore, which would cause a meltdown with the disastrous consequences that go with it. This may be considered sabotage.

In CW, physical harm to people is common. Troops are deployed for the purpose of eliminating other forces. They do this with various kinds of weapons. These weapons are primarily weapons that have direct physical consequences, like guns and other military equipment. That this harm is straightforward for CW does not mean it is always straightforward for IW. In IW, there is also a possibility of physical harm to human beings in multiple ways. The first way is in line with that of physical sabotage. When a power grid is affected by IW, this could lead to consequences that affect people. The disruption of a power grid can cause a hospital to be out of power. When a hospital is out of power, people die. Another cause of physical harm to humans could be robotic weapons. An autonomous drone could target people, and when it strikes, this may damage objects as people.

JWT Conditions

The goals of physical harm in IW are the same as the goals of physical harm in CW. The only difference is that the methods for achieving these goals are different. The question now is whether the conditions of JWT and specifically *jus in bello*, can also assess the justifiability of these attacks.

Physical harm can be considered the same in CW and IW. The only difference is the method for causing physical harm. This means that the proportionality condition can be applied in the same way. Before launching an IW-related attack, the executor should take into consideration the consequences of the attack. When the effects outweigh the goal in a negative sense, the attack should not be executed. Here applies the same as in CW; more good than harm must arise from the attack. When the consequences of an attack are only physical, it is possible to quantify the outcome of the attack and make the comparison between good and bad. However, one problem is that one cannot always foresee this outcome and collateral damage is possible. This, however, is also a problem in CW.

For the condition of distinction, the same applies. Because the consequences concern physical harm, the distinction between combatants and non-combatants can be made easier

than with other forms of harm. When it is clear who executed an IW-related attack, it is clear who to attack. Because the attack is a physical one, there is usually a possibility of discovering who committed the attack. This can be done based on the material that is used for the attack or satellite images, for example. However, when executing a counterattack, the same problems come to the surface as within CW. It is not always possible as well for an IW-related attack to distinguish between combatants and non-combatants. It is hard to foresee the consequences of such an attack and know who is exactly going to be targeted.

The condition of necessity as well can be applied in the same way for IW as for CW in the case of physical harm. When the strategic target of an IW attack is clear, the condition of necessity can be applied to assess whether the attack is justified or not. Since a physical attack, in CW as in IW, usually is a strategic target that can help to gain military advantages, it is possible to use this condition. Because physical harm is a consequence of an attack that is equal for CW and IW, the same condition, necessity, can be used to make the assessment of whether an attack is justifiable or not.

4.2.2 Information Harm

Forms of IW, or attacks, that can be attributed to information harm are IAIP, EW, and OS. IAIP is the most obvious kind of attack that can lead to information harm. The goal of IAIP is to attack information processes with information. As noted in the brief description of IAIP, this can be done through multiple methods.

EW is occupied with jamming radio or communication systems and the use of cryptography. These attacks are relevant for information harm because they directly concern the harm of information. When a communication system is jammed, this disrupts the flow of information. When the flow of information is disrupted, this can be considered as harming the information because it is used as it is intended to be used. Cryptography has the goal of coding or decoding information, and this not necessarily harms the information, but when the information is decoded by the enemy, this could be considered as harming the information of the enemy since it falls in the hands of the wrong party.

Information harm is the second category of the four categories of harm. Information harm is harm done by information systems against other information systems without the necessary consequence of causing physical harm. This form of harm is not always directly noticeable by

humans, which makes it less straightforward than physical harm. Because there are no direct implications to the physical world, it can be challenging to observe harm that is done to the own information or information systems. It is, therefore, not unusual that attacks that concern information harm are detected much later and with more effort than the more usual physical attacks that are more common for CW.

JWT Conditions

Proportionality can be applied if we can assess the harm relative to the human experience. This assessment relies on the consequences of such an information attack. The information attack itself is difficult to quantify. There is no direct concern for people when data or information is deleted or an information system is destroyed. The concerns arise only once the destruction of the information or information systems will have noticeable effects on people. This could be through different kinds of observable effects, such as economic harm or damage to morale. Another effect could be strategic damage in times of war. When strategic information systems are damaged by information harm, communication is disrupted, which leads to disadvantages in battle. When this kind of harm is visible, the proportionality condition can also be applied, and it may be assessed whether an attack that caused the harm was proportional.

The condition of distinction is harder to apply in the case of information harm. When information harm is done or suffered, it is not always directly detected, which causes the problem that it is not necessarily known who is targeted by the attack. However, when this is evident, it is easy to tell whether the condition of distinction has been adhered to or not. In addition, when an information attack is launched, it may be difficult for the attacker to know what systems are actually getting targeted. This is dependent on the method, but the collateral damage of an attack is difficult to foresee.

The condition of necessity is more troublesome to apply in the context of information harm. As this condition is about achieving military objectives while complying with the other two conditions, it is hard to say if information harm can be the exact strategic target. Usually, the consequences of such an attack are causing harm to the strategic target and not the consequence of information harm itself. Unless data is directly destroyed, and this has consequences because the enemy cannot act anymore as they wanted to, it is a direct consequence of the harm to information. Other consequences, however, are consequences

that are a result of information harm, but not the harm caused directly by attacking information.

4.2.3 Espionage Harm

The forms of IW that can be attributed to this kind of harm are IBW and OS. Clearly, IBW is a form of IW that causes espionage harm. Although the means of getting to the goal – gathering enemy intelligence – are different between CW and IW, this does not mean that the implications are different.

The third category of harm is espionage. The harm caused by espionage is another kind of harm than the former two. This kind of harm, however, is not particularly new. The harm that is inflicted on a state that is attacked through espionage is the loss of important strategical intelligence to another state and thus the disadvantage in battle. Espionage is of all times and is also a kind of harm that is inflicted in CW or outside warfare. The goal of espionage is to gather intelligence about the enemy. Secret or confidential information – or intelligence – is obtained from non-disclosed sources or without the permission of the owner of the information. This is done with the aim of gaining benefits for having an advantage over the enemy, in this context, in war. In war, espionage is considered permissible for the reason that states can acknowledge that it is inevitable that the opposing side, the enemy, tries to gather intelligence about the plans of the other. There are, however, rules about the capturing of the people executing espionage, also known as spies. Because the spies disguise themselves behind enemy lines to not get caught, they are not considered as prisoners-of-war. This means that they can be subject to the prosecution of the corresponding state.

Espionage in IW, however, is different than that of CW. In IW, there is no necessity to use people for gathering intelligence since computer systems can also be used to breach other computer systems and gather intelligence through that method. The benefit of using this method is that fewer risks need to be taken when executing an espionage attack.

JWT Conditions

It is questionable whether the conditions of *jus in bello* can be applied to espionage in IW. Since espionage already is a grey area in the domain of CW, this is vague as well in the context of IW. It does not seem that the condition of proportionality is relevant for the assessment of

the justifiability of an attack that concerns espionage because the harm that is done only concerns expropriating information for the own gain of a state. This certainly is a kind of harm, but it does not destroy or damage physical objects or information.

The second condition also does not really seem to be relevant for espionage since attacks of espionage are always goal oriented. An attack or operation of espionage usually is well prepared and aims at just one purpose: gathering intelligence of the other. There is no need for distinction because this goal usually is straightforward and can be acted upon.

Necessity is probably the most relevant condition because espionage could be one of the least harmful options for gathering intelligence. A state could also send all its troops to gather intelligence, but that probably defeats the purpose of the attack. The goal most of the time is to gather intelligence without the enemy knowing in order for the information to be helpful in battle. This also applies to the use of espionage in IW.

Since the conditions of JWT are not that useful for this kind of harm, the question emerges of how states should consider this kind of harm. Another kind of framework than JWT would be better for viewing espionage harm.

4.2.4 Disinformation Harm

Attacks that can be attributed to disinformation harm are C2W, IBW, PW and OS. C2W can be attributed to information harm because these kinds of attacks can consist of deceiving and misleading the enemy.

IBW can also be attributed to disinformation harm because next to the gathering of information, information can also secretly be given to the enemy in order for them to believe false information.

Attacks of PW are the most convincing attacks that can be attributed to disinformation harm. Disinformation harm clearly is a result of propaganda or disinformation that is used by a state to influence the civilian population or other information that can demoralize the military troops.

The final category of harm concerns disinformation. Disinformation can be considered a form of propaganda. The use of disinformation in war is not a new phenomenon and can also be seen in CW. Before the advent of television and other forms of mass media, oral disinformation and pamphlets etc., already existed. In the contemporary world, however, the

use of disinformation has become much more prevalent. There is no need anymore to be in a position of power to make use of disinformation. With the emergence of social media, people can assemble and create and spread their own disinformation if they wish to. The use of disinformation in times of war, however, can differ. There are multiple places and subjects that can be the target of disinformation. The means of using disinformation can vary, but the harm essentially stays the same. The harm of disinformation is caused by misleading people by giving them the wrong information.

In IW, this can have multiple goals. The first is that of creating ill will among the people of a belligerent. An example is that of a disinformation campaign orchestrated by Somalian warlord Mohammed Aidid. In a confrontation between Aidid's troops and that of the US, the US lost about nineteen men, while Aidid lost about fifteen times that number. However, because he had made images of Somalis dragging the American soldiers through the streets of Mogadishu, it seemed to the American people that they were losing the fight. This eventually led to the revulsion against the war by the American people, which in turn led to the withdrawal of troops and Aidid eventually winning the (information) battle (Libicki 1995, p. 35-36). Another use of disinformation in times of war is the use of psychological methods against the other side's forces. This could be by telling the troops that they will die within the war or by creating resentment against the home front. The third way of deceiving the enemy in the war with the use of disinformation is by deceiving the command. An illustrating example is that of operation Mincemeat, which is discussed in the former subchapter.

One can imagine that new technologies make it easier to spread disinformation. With the use of social media and algorithms, it is much easier to deceive people than it was before. An example of the contemporary use of disinformation in war is the Russo-Ukrainian war. Both sides use disinformation to keep the soldiers on their feet, letting the people of the state believe that they are winning the war. This happens through traditional media as through relatively newer methods such as social media.

JWT Conditions

It is questionable to what extent the conditions of *jus ad bellum* can be applied to disinformation harm. Since the harm of disinformation is not any physical harm but rather harm that gives a state an advantage in battle, it is difficult to speak about proportionality. Because the harm that disinformation can cause is mainly about misleading the enemy, it can

cause physical harm by extension. However, for the attack itself, this is not the case. Therefore, the proportionality condition is not relevant to take into consideration.

The distinction condition is also not applicable. As the goal of spreading disinformation is to only spread to a specific group or to as many people as possible, the distinction condition is not relevant. When a specific group is targeted, the goal is only to target this group and no one else in order for the attack to succeed. And when as many people as possible are targeted by disinformation harm, this is precisely the goal. A state wants to let as many people as possible believe their disinformation and stand on their side. This means that distinction is not applicable because there is no need for distinction, or the distinction is part of the plan, and there is no risk of harming non-combatants.

The condition of necessity is relevant for disinformation harm. This kind of harm can be quite serious and a real game changer in warfare. When it is not necessary to use disinformation harm, states should not. The side effects can be long-term and demanding to be taken away when considering significant propaganda attacks. On a smaller scale, however, the necessity principle is of less importance because only a few people are misled.

5. Conclusion

The aim of the first chapter was to show the problems that arise with the application of JWT to IW. We saw that if IW (as a whole) is to be assessed through JWT, a number of problems/dilemmas arise. These problems are mainly related to the fact that the consequences of attacks in IW often have no physical consequences, as in CW. The first problem concerns the distinction between the categories *jus ad bellum* and *jus in bello*. This distinction is already a grey area within CW but has completely disappeared with regard to IW. This is because there is no continuous conflict with frequent subsequent attacks in IW as there is not always a question of responses or retaliation, and an individual IW attack does not necessarily lead to a state of war, as there is not necessarily a fundamental change within the diplomatic arena.

The second argument showed that when IW is evaluated with the help of *jus in bello*, the principles of this JWT category can be useful but cannot be applied 1-on-1 to the kind of warfare. The conditions distinction, proportionality and necessity are of a certain relevance but cannot be used the same as for CW.

In Chapter 2, we saw that Taddeo attempts to solve this problem by designing a macro ethical theory that no longer emphasizes physical consequences but rather the consequences for information as a broadly defined concept. The goal of the second chapter was to analyze the JIW theory of Taddeo critically. We have seen that, according to Taddeo, there is an ontological difference between multiple kinds of harm in JWT. Her approach is to try to overcome this ontological difference. According to Taddeo, IE and JWT need to be merged in order to overcome the ontological problem. By combining these two frameworks, Taddeo designed three principles that can be guiding in the assessment of whether IW is fought justifiable or not.

We have also identified several problems with the theory of Taddeo. Firstly, following Stevens, there is a terminological issue with the term IW, which is too broad and outdated. Thus, states and militaries have already decided not to use the term anymore because it is too broad for its purpose. Secondly, Taddeo considers multiple types of harm in the same way. This is odd because, intuitively, the harm inflicted on a human being is different from harm inflicted on a computer or software. Thirdly, Taddeo's concept of the *infosphere* is ambiguous.

According to Taddeo, the well-being of the *infosphere* is something we should strive for. However, it is difficult to see what this flourishing of the *infosphere* entails. Finally, Taddeo uses the term victory in her article. However, this term is not relevant in IW. Because IW concerns the manipulation of information that is trusted by the target, but the target does not know that this information is used against him, the target acts against its own interest. For this reason, it is hard to tell when IW begins or ends. This makes it impossible to speak of victory in IW.

As a solution to the problems/dilemmas posed by IW, we then suggested that it would be more productive to stop thinking of IW as an integral concept. After all, there is usually no war in which land is occupied, or victory is possible for IW. In this sense, the term information warfare may be misleading or wrongly chosen. It is better to speak of different types and separate cyber-attacks. The goal of the final chapter has been to bring a solution closer to the question of how states should deal with or respond in IW and to cyber-attacks. The method of bringing this solution closer was by splitting up the concept of IW. This is important because IW consists of a lot of different kinds of warfare or attacks. Based on Libicki and Nichiporuk, we determined that IW consists of six different types of warfare or attacks. These are command and control warfare, intelligence-based warfare, electronic warfare, psychological warfare, information attacks on information processes and operational security. These attacks have subsequently been categorized along the lines of different types of harm. Based on categories of harm, because these are consequences of warfare or attacks, we can determine to what extent JWT is applicable or not.

In the second part of this chapter, the four categories of harm are discussed, which are physical harm, information harm, espionage harm and disinformation harm. With the use of these different categories of harm, it can be determined what the possible consequences of the different forms of IW are. From there, we can see to what extent JWT is applicable to these kinds of harms and attacks. JWT, however, was not applicable to all these kinds of harm, from which we can conclude that JWT is sufficient in assessing the justifiability of some types of attacks with associated harms, but not of all. When looking at different types of cyber-attacks individually, it was then found that attacks that directly or indirectly result in physical damage can simply be assessed through JWT.

In the case of attacks that have no physical consequences, this is not possible. But we have seen that most such attacks also have an equivalent in the conventional domain (espionage/propaganda/information). These forms of foreign interference are not, strictly speaking, acts of war and thus beyond the scope of JWT. Therefore, when assessing cyber-attacks without physical damage, one could rather look at how such type of foreign interference is dealt with in international law. Further research may explain what kind of frameworks could be helpful to assess other forms of harm than physical damage.

References

Abu Saada, M. & Turan, Y. (2021). Israeli-Palestinian Cyber Conflict. *Eskisehir Osmangazi University Journal of Economics and Administrative Sciences*, *16*(1), 186–204. https://doi.org/10.17153/oguiibf.869178

AP NEWS. (2019, 15 September). *Saudi Arabia: Drone attacks knocked out half its oil supply.* https://apnews.com/article/middle-east-yemen-ap-top-news-persian-gulf-tensions-international-news-d20f80188e3543bfb36d512df7777cd4

Beard, J. D. (2013). Operation Mincemeat: How a Dead Man and a Bizarre Plan Fooled the Nazis and Assured an Allied Victory. Intelligence and National Security, 28(6), 923–924. https://doi.org/10.1080/02684527.2012.755064

Bellamy, A. J. (2008). The responsibilities of victory: *Jus Post Bellum* and the Just War. *Review of International Studies*, *34*(4), 601–625. https://doi.org/10.1017/s026021050800819

Blanchard, A., & Taddeo, M. (2022). Jus in bello Necessity, the Requirement of Minimal Force, and Autonomous Weapon Systems. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4100042

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

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, *1*(1), 33–52. https://doi.org/10.1023/a:1010018611096

Frowe, H. (2015). *The Ethics of War and Peace* (2de editie). Routledge.

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.

IBM: Cost of a Data Breach Report. (2021). Computer Fraud & Security, 2021(8), 4. https://doi.org/10.1016/s1361-3723(21)00082-8

Jensen, E. T. (2012). Cyber Attacks: Proportionality and Precautions in Attack. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2154938

Joan, Reitz M. (2010) "Information Ethics." Online Dictionary For Library And Information Science. N. http://www.abc-clio.com/ODLIS/odlis_i.aspx

Kelley, M. B. (2013, 30 november). *The Stuxnet Attack On Iran's Nuclear Plant Was "Far More Dangerous" Than Previously Thought.* Business Insider. https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?international=true&r=US&IR=T

Kramer, A. E. (2022, 15 January). *Hackers Bring Down Government Sites in Ukraine*. The New York Times. https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

Kuehl, D. T. (2009) From Cyberspace to Cyberpower: Defining the Problem. *Cyberpower and national security, Potomac books and National Defense University,* 24-42.

Lazar, S. (2020). "War". *The Stanford Encyclopedia of Philosophy* (Winter 2018 Edition), Edward N. Zalta (ed.). Metaphysics Research Lab, Stanford Univerisity https://plato.stanford.edu/archives/spr2020/entries/war

Libicki, M. C. (1995). What Is Information Warfare? (1st ed.). National Defense University.

Lin, P., Allhoff, F., & Rowe, N. C. (2012). War 2.0. Communications of the ACM, 55(3), 24–26. https://doi.org/10.1145/2093548.2093558

Nichiporuk, B. (2002). U.S. MILITARY OPPORTUNITIES: INFORMATION-WARFARE CONCEPTS OF OPERATION. In Z. Khalilzad & J. Shapiro (Eds.), Strategic Appraisal: United States Air and Space Power in the 21st Century (1st ed., pp. 187–224).

Orend, B. (2000). Jus Post Bellum. *Journal of Social Philosophy*, *31*(1), 117–137. https://doi.org/10.1111/0047-2786.00034

Orend, B. (2013). The Morality of War - Second Edition. Amsterdam University Press.

Reuters. (2022, 24 februari). *Ukrainian president signs decree on general mobilisation of population -Interfax*. https://www.reuters.com/world/europe/ukrainian-president-signs-decree-general-mobilisation-population-interfax-2022-02-24/

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, *49*, 70-94.

Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.*, *47*, 79.

Stevens, T. (2012). Information Warfare: A Response to Taddeo. *Philosophy & Technology*, *26*(2), 221–225. https://doi.org/10.1007/s13347-012-0070-y

Taddeo, M. *(2011). Information Warfare: A Philosophical Perspective. Philosophy & Technology, 25(1),* 105–120. https://doi.org/10.1007/s13347-011-0040-9

Taddeo, M. (2014). Just Information Warfare. *Topoi*, *35*(1), 213–224. https://doi.org/10.1007/s11245-014-9245-8

The Spectator, (2022, 24 februari). *Full text: Putin's declaration of war on Ukraine*. The Spectator. https://www.spectator.co.uk/article/full-text-putin-s-declaration-of-war-on-ukraine

United Nations. (1945). *UN Charter*, available at https://www.un.org/en/about-us/un-charter

Weedon, J. (2015). "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine". In Kenneth Geers (ed.). *Cyber War in Perspective: Russian Aggresion*

Zetter, K. (2016, 3 March). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/