DOI:
10.1093/monist/onv029

Document Version
Peer reviewed version

The Monist 2016 99 (1): 55-69 doi: 10.1093/monist/onv029
Dr David Whetham, Department of Defence Studies, King's College London

"Are We Fighting Yet?" Can Traditional Just War Concepts Cope With Contemporary Conflict and the Changing Character of War?[1]

In the 'good old days', the traditional view is that one knew when one was at war – it was declared, people would fight, one side would win, the other lose, and then the war would be over. In Ancient Rome, the start of hostilities might take the form of high ranking *fetial* priests casting a spear into enemy territory to demand redress for a wrong committed against the Republic.[2] In the Twentieth Century, it might be like the formal declaration of war made by Britain against Germany following the latter's invasion of Poland:

> "This morning the British Ambassador in Berlin handed the German Government a final note stating that unless we heard from them by 11.00 a.m. that they were prepared at once to withdraw their troops from Poland, a state of war would exist between us."[3]

War was considered ended in Ancient Greece when the defeated side's lines broke and the fleeing troops lost possession of the battlefield. You knew if you were on the winning side because it was you who was being asked by the other side for 'permission to gather up their dead'.[4] The formal surrender of the Japanese armed forces on the deck of the USS Missouri on September 2nd, 1945, also represented a clear and unambiguous full stop to hostilities, marking a clear dividing line between war and peace.

It was in this context that the norms of war we are used to today were developed. The Just War Tradition, in the West at least, developed out of a synthesis of classical Greco–Roman and later Christian values, although it would be a mistake to consider it as a purely Western or even as a religious phenomenon.[5] The Tradition guides normative thinking about what is and what is not acceptable, even in times of war. Its core ideas – that there should be limits on when the use of force can be considered legitimate (the *jus ad bellum*), and that there should also be limits on what and whom that force can be directed against (the *jus in bello*) – have found expression in all societies due to the recognition that they need to restrain the wars they fight in some way.[6] While the exact details may vary a little, the core ideas are shared across religious and secular culture, underpinning international law. The ubiquitous nature of the thinking found in the Just War Tradition therefore represents something of 'a common language for discussing and debating the rights and wrongs of conflict'.[7] When those norms are violated, those violations are, generally speaking, recognised and condemned as such.

However, while the Just War Tradition may have historically been a useful guide to normative considerations regarding the use of force, things appear to be more complicated today. The spectrum of contemporary conflict appears to be growing and expanding in such a way as to challenge old notions of what it is to be at war, or even the idea that war is an exception to the normality of peace. While terrorism did not suddenly begin on 9/11 (although one might be led to believe this), events that day and the on-going threat and reality of mass casualty terrorism around the world have certainly shaped attitudes in the years subsequent to 2001. The character of conflict appears to be morphing in other ways too. Robert Gates, US Secretary of Defense, described the problem when he articulated, 'the categories of warfare are blurring and no longer fit into neat, tidy boxes. One can expect to see more tools and tactics of destruction -- from the sophisticated to the simple -- being employed simultaneously

in hybrid and more complex forms of warfare'.[8] Russell Glyn has suggested that the hybrid threat can be characterised as when 'an adversary…simultaneously and adaptively employs (1) political, military, economic, social, and information means, and (2) conventional, irregular, catastrophic, terrorism, and disruptive/criminal warfare methods'. This could involve a combination of state and non-state actors in the process.[9]

Should things like on-going terrorist activity on a large scale, or hybrid war, perhaps involving predominantly non lethal methods such as subversion or economic attrition, be tackled within a war paradigm that can be considered using the normative tools provided by the Just War Tradition, or should it instead be considered and approached with something looking more like a law-enforcement paradigm? Some argue that relying purely on the policing paradigm is flawed as it can only really be applicable for 'well-ordered societies that suffer from [only] occasional and small-scale violence engaged in by individuals or small groups'. They argue that the nature and scale of the current domestic and international threat means that the war paradigm is therefore a better fit with current realities.[10] Others argue that something in between or combining the two approaches is required and that such challenges can best be met by employing both war *and* law enforcement paradigms.[11] Although he was specifically referring to cyber attacks with political intent, Thomas Rid argues that this particular kind of conflict can best be considered as something in between as well - 'neither crime nor war, but rather in the same category as subversion, spying or sabotage, existing somewhere on the spectrum between apolitical crime at one end and genuine war at the other'.[12] So where does this leave us?

The reality is that despite President Obama's statement in February 2015 - "I do not believe America's interests are served by endless war or by remaining on a perpetual war footing" (ironically made while seeking approval for expanding the US war effort) – conflict, whether it deserves the name "war" or not, appears to be the norm rather than the exception for millions of people.[13] The US Assistant Secretary of Defense for Special Operations, Michael Sheehan, said before the Senate Armed Services Committee in May 2013 that the war against Al Qaeda would continue "at least 10 to 20 years".[14] 'What is dubbed the war on terror is, in grim reality, a prolonged, worldwide irregular campaign'.[15] It might not look like many of the conflicts in the Twentieth Century, but in terms of the scale of effort and resources in terms of blood and treasure dedicated to it, war it is.

Outside of the US, the UK does not officially consider herself at war. The UK never officially adopted the term "Global War on Terror" and yet, the security status of government and military facilities around the country remain heightened and British troops are deployed in 80 countries around the world engaged in small scale training and advisory roles all the way up to major deployments in support of local security forces, such as the 5200 troops who were still in Afghanistan at the start of 2014.[16] The shooting of 12 journalists in Paris in January 2015 led to a controversial attempt to broaden surveillance powers in the UK and the Prime Minister expressing concerns about whether or not the country was adequately prepared for a Mumbai style "roving firearms terrorist attack".[17]

Is this what peace looks like now, or should this more accurately be considered, as apparently the US administration does, to be a state of constant war? Rosa Brooks is not alone when she argues precisely this when she states that 'Perpetual war is unlikely to end in our lifetimes…it has become virtually impossible to draw a clear distinction between war and not-war.'[18] This matters because war is a situation in which states, and individuals acting on behalf of those states, are

permitted to carry out acts that are otherwise prohibited. This includes, of course, the deliberate and premeditated taking of human life, an issue highlighted by the arguments over targeted killings using drones.[19] It also includes allowing the state to interfere with some of our individual rights and liberties in order to protect us from a known danger, whether that be travellers putting up with longer queues at airport security screening, accepting increased surveillance and scrutiny of our private communications and activities, or curtailment of certain types of association deemed to be of concern to the state. The detention of captured enemy combatants for the duration of hostilities when those hostilities may never end, is another highly contentious issue.

If war is the norm, at least for the foreseeable future, then what actions and behaviours should be included in this understanding? Is all activity to be judged by the same standard? Who or what is included in the class of 'enemy'? What counts as a hostile act and what are you permitted to do in response to it, or has that question already been answered with the assumption that one's state is at war? The character of contemporary conflict is changing and this in turn raises questions about the suitability of normative frameworks that are supposed to govern it. Can something like the Just War Tradition, firmly grounded in traditional and arguably out-dated understandings of conflict, really cope with the realities of contemporary warfare?

A week's events in the UK in 20XX

To test some of these questions, the next section will outline a series of events that might take place in the not too remote future.

A question raised by a whistle blower organisation suggests that due to cutbacks in the oversight regime, the integrity of nuclear safety check data for several power stations must be called into question. The allegation is that expert nuclear weld engineers have been supplemented by trainee technicians who do not have the experience to be able to sign off the essential safety certificates. While the investigation continues into what data can be trusted, the media storm leads to the temporary shut down of four UK power plants, which combined with a wild cat strike in France by power workers (thus preventing the usual electricity sharing protocols), leads to rolling power cuts around the UK.

A leak from somewhere in Whitehall, initially reported on a blog site but quickly picked up by the print and broadcast media, alleges that the contact details of an infamous bondage party organiser, currently 'on holiday' and unavailable for comment, has been found on the Prime Minister's Blackberry. Despite angry rebuttals, Prime Minister's Question Time descends into farce as the Opposition hold up toy handcuffs, and questions about the PM's moral authority are severely damaging party discipline.

The supermarket giant Tesco's financial woes continue. However, a leaked internal auditor's report suggests that at least 20 other Blue Chip companies have also been playing games with the rules regarding discount payments and the financial year in which they are registered for profit purposes. The suggestion that the profits of such a large number of pillars to the UK economy may be severely overinflated leads to the largest one-day fall in the FTSE 100 for a decade. The pound begins to slide as wider questions about the British economy begin to be asked around the world. As the risk appetite in the UK business world dries up, mortgage products start to be withdrawn from the market by key foreign-owned financial institutions, leading to dire predictions of another UK housing market crash.

The Monist 2016 99 (1): 55-69 doi: 10.1093/monist/onv029
Dr David Whetham, Department of Defence Studies, King's College London

Rumours about a change in the TV licensing rules lead to riots at six British prisons as prisoners believe their TVs are about to be withdrawn from their cells. The military are put on standby to assist the understaffed prison service as the riots start to spread in the overcrowded facilities. At the same time, a legal challenge through the British courts is raised by a pressure group using the Human Rights Act to challenge any armed overseas deployment of British troops if there is no clearly identified link to UK vital national interests as defined in terms of preserving the life and liberty of UK citizens. Confusion over what this might mean causes great angst in the Ministry of Defence.

Environmental campaigners are granted an injunction to prevent the use of a certain type of new sonar used on British submarines due to an alleged link to the deaths of large numbers of endangered sea mammals. This means ignoring the ruling, operating at reduced effectiveness and increased vulnerability, or refitting, putting the UK's continuous at sea nuclear deterrent at risk of being gapped for the first time in its history. In less well known developments, the Chief of the Defence Staff is distracted by his son's arrest on drug possession charges after pictures of him apparently taking cocaine with friends at a university party appear on social media, prompting an on-going police investigation that is drawing in for questioning the children of many high profile political and military figures.

These events are combined with another twenty or thirty other simultaneous political, economic or legal developments, including a walkout of transport workers prompted by pension reform proposals leaked to the press, positive Foot and Mouth results forcing an embargo on all cattle movement in the North of England, a glitch in the Just in Time automated stock systems at three different national supermarket chains leading to empty shelves and panic buying among the public, asbestos traces found in the Cabinet Office briefing room forcing key government decision-making to relocate, a death attributed to Ebola in Scotland by a returning tourist from West Africa leading to fears of an epidemic as everyone she has been in contact with in her job at a petrol station for the past two weeks need to be tracked down. Vigilante mobs start targeting 'dirty Africans' in the streets, and a sewage pumping station error dumps two million gallons of untreated sewage into the River Thames. At the same in the background, of course, and getting no public recognition, the security and intelligence services continue their vigil, foiling various terrorist threats that may have manifested themselves in the deaths of small numbers of British citizens had they not been successfully disrupted.

These disparate, seemingly unrelated, events combine to paralyse aspects of UK decision-making and hamper any kind of coordinated response as the country goes into crisis mode.

Are we at war yet?

Is this war? Obviously, not a shot has been fired, and there certainly does not immediately appear to be any hostile political intent guiding the combination of the week's events. However, what if they had, in fact been initiated by a foreign power seeking to destabilise the UK - would this count as war? Given the effort, planning and resources that go into conventional military operations, the level of commitment to set up and launch a coordinated operation of this nature would be very small – a piece of information timed to be launched at a certain time, some fake reports leaked, data hacked and changed, a "whistle blower" contacting the press with compelling evidence, perhaps a credible but faked bomb threat to disrupt some high profile sporting event, a few vexatious legal challenges launched using perfectly legitimate

mechanisms in functioning democracies – nothing to rival the costs and potential risks of a conventional military operation, and yet the strategic effects could be considerable.[20] But how should one respond?

To add some context to the week above, what about if all of these apparently unrelated events begin to occur the week following a UK decision to commit military assets to reassure and protect Estonia under a NATO Article IV request for support. This request coming in the face of Russian military activity on the Estonian border and growing internal instability in Estonia sponsored and supported by as yet "unidentified external agents" - would that make a difference? With a lack of tangible proof about who was directing the actions, how is one supposed to respond? If it was later proved (or at least strongly suspected given the nature of the events) that some or all of these occurrences were actually instigated by the same foreign power would that be enough for this to be considered war, or do people actually have to die first? It seems intuitively wrong to think of this as war, certainly in the sense that we are used to considering the term. The foiled terrorist attacks and perhaps even the faked bomb threats might be considered to have crossed the violent attack threshold but this element seems to be almost token in relation to the overall effort rather than core even if it is connected with the same coordinating agent.

It is the problems posed by such questions that have led some people such as Thomas Rid to argue that attacks of this nature (to be specific, he was referring to cyber attacks but I believe the logic can be extended to the range of acts above) should really not be considered acts of war. Rid argues that the term "Cyberwar" is a misnomer for three reasons, because, unlike real war; it does not involve actual violence or the threat of violence, it is not instrumental and it is not attributable. This is a powerful critique. Taking each in turn, Clausewitz, the philosopher of war, tells us that 'War is an act of force to compel the enemy to do our will'.[21] Therefore, 'if an act is not potentially violent, it is not an act of war', at least as it has traditionally been understood.[22] Clausewitz also tells us that "War is a mere continuation of politics by other means."[23] Therefore, acts of war are merely means employed towards achieving a political objective by forcing the other party to accept your terms. Finally, you have to know who you are at war with – 'History does not know acts of war without eventual attribution.'[24] Rid argues that due to the lack of the essential features war requires, even political (as opposed to merely criminal) cyber attacks or manipulations should not be considered as war at all. They may be more than simply criminal acts, but they fall short of what can be considered war, as would presumably the array of most if not all of the acts imagined in the scenario above.

I have argued elsewhere why I believe this understanding is wrong, pointing out that these criteria can actually be met by some cyber-related threats, permitting them to be categorized as war in certain situations.[25] For example, to take each point in turn, I would argue that demanding that physical violence is required seems to be an overly restrictive interpretation of an "act of war", just as it would be to limit the definition of "assault" in a domestic jurisdiction. For example, in the UK, the legally-accepted definition of assault does not require physical harm, or even the threat of physical harm to be satisfied. The guidance also makes clear that psychological harm, including fear, distress or panic, can amount to Actual Bodily Harm.[26] One can be coerced into doing something unwanted (i.e. change one's policy if you like) through fear, an unequal power relationship, perceived authority or something else interfering with informed consent. This can still be regarded as an assault and therefore deserves to be regarded as a form of violence as a result. An assault need not be physical to cause injury and there are clearly and demonstrably many injuries that are not

physical. Clausewitz himself argues that depending upon the character of the struggle one is involved with, for example 'if our aim is only to obtain a single victory, in order to make the enemy insecure, to impress our greater strength upon him, and give him doubts about his future...we will employ no more strength than is absolutely necessary.[27] In this case, if one can achieve the policy outcome without revealing one's hand or committing to the high risk stakes of employing conventional armed force against a peer, that would appear to be both prudent and strategically sound.

Secondly, if a government were on the receiving end of a few weeks of the kind of activity set out above, it might well be tempted to seek a compromise with an agent thought to be responsible – such actions could then be seen as a cyber version of the medieval chevauchée, an operation using devastation of property and molestation of people as its means designed to force an opposing lord into negotiations. Therefore, while the chevauchée was not recognised as war by many military medieval historians as it did not involve battles, that was exactly what it was – an instrument or means to bring about a favourable change in policy.[28] Closely linked to the first point, it was precisely the *moral injury* that was so damaging in the medieval conception of the *chevauchée* because the lord who's lands and people were being harmed was supposed to be able to protect them. Therefore, their demonstrable inability to do so undermined their authority leading to the need to reach a compromise agreement before the situation got even worse and the lord's position became untenable. If a series of cyber attacks were intended to do the same through political pressure, surely, they too should be considered instrumental?

Finally, attribution appears to cause the most problems, both in terms of cyber attacks and in the type of hybrid attack outlined above. Even assuming the first two points are conceded, who are you to negotiate with if you don't know who is attacking you? As I will explore further below, the attribution problem and what to do about it is one of the most challenging areas of military ethics.[29] The nature of the cyber realm, or political subversion directed from afar, means that determining who is directing the activity is extremely challenging. However, surely it is not impossible that one can be under attack and still not know, or at least be able to prove, from who that attack was coming from? This is not a situation unique to the cyber realm, and in actuality, "attribution is often challenging even in circumstances of kinetic warfare, especially at sea."[30] Presumably, a genocidal surprise nuclear strike launched from concealed submarines would still be an act of war, even if no-one 'owned up' to it at the time?[31]

I believe it is possible to conceive of a cyber and therefore a hybrid-attack that does not necessarily involve physical harm, death or destruction, but is carried out with a clear intent to achieve a political purpose, even if ownership of the attack was not admitted by any party. I believe that this could, if the consequences were serious enough, be considered war. Therefore, does this mean that the Just War Tradition can be helpful as a normative framework for this type of activity? In fact I would go as far as to argue that even if Rid and others are correct and this is not and should not be considered war at all, the Just War Tradition can *still* be a useful tool for gauging what responses might be appropriate when faced with receiving and defending against harm inflicted by others.

The Just War Tradition and situations that may or may not be war

To assume that the Just War Tradition cannot apply because the situation is not war as we understand it is to confuse what the purpose of the Tradition is in the first place. While historically the moral reasoning invoked was applied casuistically to war

(hence resulting in and evolving into what we call today the 'Just War Tradition'), that reasoning contained in the Tradition could be (and often was) applied in a variety of other situations as well where one is seeking to do something that is, under normal circumstances, prohibited, i.e. deliberately cause harm to others. That harm, in war, is normally considered to be death or injury, but it is not necessarily limited to only these types of harm. The Just War Tradition, despite the name that it has taken on over the millennia, provides a structured approach to decision-making in such situations.[32] There is nothing novel about this. For example, in the *Summa Theologica*, Thomas Aquinas applied similar types of moral reasoning to a variety of practical moral conundrums, ranging from obedience to legal authority, to self-defence, *and* to war. In the first of these, the default position is that one should obey the state, the ruler, the government etc. That is what makes civilised life possible. However, just occasionally, a regime may be 'patently unjust or immoral' and that might make disobedience or resistance permissible, or in extreme situations, even necessary. But, any argument for non-compliance must be based on a 'grave and serious breach of moral propriety…what might be called a "just cause" for civil disobedience'.[33] This would therefore represent an exception to what is normally permitted – i.e. provides a case where a normally established rule or moral principle may be justifiably set aside or violated.[34] This is also precisely what the criteria within the Just War Tradition have evolved to address, in part, through a long-running dialogue between deontological (acts-based) and consequentialist (ends-based) reasoning, acknowledging that context must be taken into account when determining a correct course of action.[35]

Even if a strategy does not fit into normal conceptions of war, but instead involves fomenting disobedience, undermining legitimate political processes, spreading false information, lying, deception, and sometimes the actual doing of harm, the reasoning found in the Just War Tradition can help. While it is not necessarily about providing a set of answers, 'it can help to structure decision making as the factors it asks us to consider should be taken into account before and during any use of armed force' or indeed act of harm.[36] What happens if you try applying the Just War Tradition to situations that don't necessarily look like war?

The Just War Tradition demands that actions that can cause harm to others be undertaken only if there is a compelling, morally justifiable reason, that they are undertaken with the right intentions, authorised by those who have the legitimacy to sanction the suspension of the normal principles, that the harms that the action may produce in both the short and long term are proportional to what is at stake, has some prospect for success, and that there are not alternative options that may do less harm and still produce results, i.e. any harm inflicted is only done as a genuine last resort. In addition to these *ad bellum* requirements about whether an exception can be made, there are also certain *in bello* principles to guide the conduct of the exception itself. Specifically: discrimination to ensure that any harm brought about is really necessary, and that any harm to the innocent is limited and proportional to the legitimate aim being pursued.

Working through the list (although the different elements must be considered in relationship with each other as a whole rather then just "ticked off" separately), if one's actions are to be considered just, be they employing cyber, political, deceptive, subversive or conventional means (or combination thereof), they must have a *just cause*. The clearest example of this is self-defence in response to an attack on one's territory, but clearly the type of situation outlined above does not fit comfortably within this idea. There are debates about whether certain types of cyber attack at the

more catastrophic end of the spectrum could be considered to have crossed the legally recognised threshold of armed attack.[37] However, as long as one is taking into account the proportionality criteria below, whether or not it is an armed attack is irrelevant to the question "have I been harmed or injured in some way and do I have a right to respond to that harm?" That is not a question that demands interpretations about legal thresholds, but rather looks at the harm received or injury suffered.

Does that mean that one can only respond justly once harm has been inflicted? It has long been recognised that some threats need to be anticipated if they are to be successfully defended against. That is even truer in an age where mass casualty terrorist attacks are being averted. As long as you genuinely believe that an attack is imminent, you don't have to have been hit first before you can act. Indeed, if one had to accept a knock out blow before defending oneself, then that defence might well have been rendered irrelevant! However, whether acting as an individual or on behalf of a state or other political actor, treating every potential but un-actualised threat as if it is imminent because it might at some unspecified time in the future, become a threat, attacking in such circumstances 'cannot be considered self-defence, either legally or morally'.[38] Without getting this balance right, 'preventive self-defence' may amount to little more than felonious assault.[39] Again, as above, it does not matter if the injury, or threat of harm is not physical as this question is simply to determine if the harm justifies a response – it does not determine what type of response is then appropriate at this stage.

The classical formulation of the Just War Tradition requires that a declaration be made by a legitimate authority. In the contemporary environment, does it matter that the agent causing (or responding) to the harm may not be a state at all? Not at all – 'in its 'classical' formulation, the Just War Tradition was not tied to any specific international arrangement or political paradigm'.[40] Its classical origins long predates the Westphalian system of nation states we are familiar with today, and while the starting point for most Just War discussions starts today with a framework that owes much to Michael Walzer's 1977 classic *Just and Unjust Wars*, and its 'legalist paradigm', there is no reason to restrict the agents involved to legally recognised states.[41] The declaration element is often omitted but is also important for it is the means by which one signals why one is taking the actions being taken and what the other party or parties need to do to stop those actions, i.e. call a halt to hostilities. Normally, such a declaration will be public, perhaps even with a clear policy statement of what the state will do when faced with certain injuries, but there is no moral requirement for this declaration to be open to everyone, and the political environment may make backchannels more effective than grandstanding in many situations.

But how can this be applicable to the forever war where the lines can blur to such an extent, and there may be no notification, formal or otherwise, to those involved, regardless of whether the opposing agent is a recognised state or not. Closely related to the previous criteria, surely having a just cause must involve knowing who has attacked you – you can't really be at war when you don't know who has attacked you? Again, we tend to treat this as something new but looking back in human history, it has often been difficult to know when one was at war or not. For example, in 1339, Sir Walter Manny rode ahead of news of the outbreak of war between England and France in order to take the town of Mortaigne by surprise. They were clearly not expecting his attack and Sir Walter quickly overcame the defences.[42] One could argue that something not too dissimilar happened at Pearl Harbor, but as pointed out above, regardless of the legitimacy of the attack on yourself, the idea that

you can't be at war until you have worked out who is attacking you seems ridiculous in many different situations. What appears more likely is that you are under attack of some type, but do not know by whom – you do not know who you are at war with yet. In the cyber or largely non-kinetic hybrid war mentioned above, this lack of attribution makes anything other than passive defence (the cyber or social equivalents of shields, screens, walls or barriers) very difficult in moral terms. It might require months to determine the source of an attack and then one might still not be certain that this was the real culprit, which has further consequences (as discussed below). The controversy over the attribution of the cyber attacks on the media giant Sony in 2014 and whether or not they really were North Korean in origin is a very public demonstration of how difficult things are in this area, even when they appear obvious at first.[43] This is clearly a very different situation to conventional conflict where 'soldiers wear uniforms, and often the geography of an incident points to the identity of the organisation behind an intrusion'.[44] Rid and Buchanan argue that successful (if perhaps not certain) attribution *is* possible, and that this requires a range of skills on all levels, careful management, time, leadership, stress-testing, prudent communication, and recognising limitations and challenges. Ultimately, when faced with the resources at the disposal of an advanced state which has decided to pursue the issue due to what is at stake, 'attackers cannot assume that they can cause serious harm and damage under the veil of anonymity and get away with it', even if this investigative process takes some time.[45]

The spirit in which one acts - one's motivation - is generally considered important when judging the moral quality of an action. If one were to wait six months before responding to a threat, would that really be anything other than punishment, or even revenge? Could they be a sufficient motive for doing harm to others? Punishment in the face of injury was actually considered a moral duty in the Middle Ages. Law 'came from God and represented the natural order of things'.[46] When a wrong was committed, this meant that punishment had to be forthcoming for the injury to the moral order of things as well as for the injury to the specific individual or party. The Romans saw it more as a form of contract - 'if the citizens of one state injured the citizens of another state in some way and they were not punished by their own state, then the whole state [instead] could be punished by war'.[47] However, even when the line between punishment and revenge may have been somewhat blurred historically, today, pure revenge is very clearly not considered a legitimate motivation,[48] while punishment needs to be firmly grounded in terms of actions necessary to prevent an on-going threat. How can it be possible to respond weeks, months or even years after an attack, as might be required by the need to positively identify the culprit, and still claim that this is somehow an action taken in self-defence?

This question, therefore, is inextricably linked to the principles of proportionality, prospect of success and last resort at the *ad bellum* level, but also reaching across to the *in bello* level. Last resort is the Just War Tradition's necessity criteria – is there anything else that might work short of harming the other party – is this the only thing that has a prospect of working? Note that this does not require that the response is immediate to the initial harm, but rather, requires that there is nothing less damaging that can be done in order to prevent further harm or, if relevant, to return the situation to the *status quo ante bellum*. As long as the attacks are on going, or there is a credible fear that the attacks will continue at some point unless action is now taken against the newly identified actor, then this can still be in accordance with the last resort requirement.

In terms of proportionality, how significant is the harm that has been received or will be received if the on-going threat is not averted? What is therefore a proportionate response to that harm? Attacking one's attacker back might not be necessary at all. Successful defence could mean simply imply thwarting an attack through blocking actions in a way that makes success too uncertain to be worth the investment, or it might require pre-emption, as discussed above.[49] What this might mean in the cyber realm is going to be different to what it might mean in the political or legal realm, but note that the same broad ideas are still applicable, as is the importance of proportionality. If you do not want your information technology systems to be used against you maliciously, you ensure they are protected or, if they begin to malfunction, they can be shut down or disconnected. In the event of the civil, economic or legal structures that underpin western democratic states being manipulated or abused in a way that is intentionally damaging to those states, then having mechanisms in place to respond is just as important – from an ability to halt trading on your stock exchange in the face of false information being released that skews trading, or emergency legislation that can temporarily suspend a normal civil right or activity. Both situations demand that the response is proportional to the threat – you do not just suspend all civil liberties because an aspect of the judicial system is causing problems, no more than you would cut the internet connection to your own country to stop a fraudulent email from a fraudster in Nigeria seeking to get your bank details.

Looking towards the source of the injury rather than inwards at more internal defensive responses, if the injury received is minor, or the risk of future harm is not considered significant, then perhaps criminal law or diplomatic sanction against the offending actor may be sufficient to avert on-going or future injury, or return the situation to the *status quo ante bellum*. However, if the overall harm is already significant despite the defensive measures in place, or there is reason to suspect that the injury will grow or escalate unless responded to robustly, then it is possible that a proportional response may require some form of counter attack. This may involve inflicting harm that is greater than the current level of injury received, including moving into the more traditional military sphere if justified - the response to a cyber attack, for example, need not necessarily be a cyber counter-attack.[50] It may be determined, in good faith and based on credible investigations uncovering a serious on going threat, that the only thing that will prevent further political, economic, social, or information attacks causing significant harm to the state with or without an overt military (whether conventional or irregular) component being present, is itself, a military response. However, whatever the form of the defensive act, be it political, diplomatic, cyber or military, and whether that response is immediate, or comes weeks or months later once the offending party has been appropriately identified, the response still needs to be proportional to the injury received or the threatened injury that is genuinely believed to be coming.

At the *in bello* level, whatever actions one takes in response to the injury suffered, the Just War Tradition demands that only those who are responsible for the harm may be directly targeted by whatever means is considered appropriate – the principle of discrimination (or distinction as it is known in legal terms). It also requires that any unintentional harm caused to those who are not culpable is minimised as far as possible. An illustration of what this might mean is the question whether or not to destroy a server through which a malicious attack has been launched, causing substantial financial damage and disrupting economic activity. The questions that need to be asked begin with will the action actually harm the actor

responsible for the attack and prevent them continuing the attack or launching another one? Who else will be harmed? Note, just as with the injury received, harm does not have to be considered as a purely physical thing. Data, records, financial service etc. could all be disrupted or destroyed by an attack. How culpable are the owners of the server - did *they* launch the attack, if not, did they facilitate or just fail to prevent the attack, should they have known about it if they were acting responsibly, or were they oblivious due to the steps taken by the attacker to cover their tracks? Clearly, the less culpable they are, they less liable they are to harm. What about all the other people that have data stored on the server, or rely on it for their livelihoods? Is the likely harm that they will suffer, unintentionally or not, proportionate to the anticipated benefit of the attack?[51] If the attack on the server is deemed necessary, can the attack be carried out in a more discriminate way that only affects those who are culpable? These are just some of the questions that the *in bello* criteria should prompt in relation to any action that involves inflicting harm, lethal or not, intentionally or not, on others.

Conclusion

This paper cannot possibly hope to address every variation of the threats that states are faced with, nor every way in which the Just Tradition may be of relevance. The purpose was merely to firstly question what we commonly understand to be "war", and secondly, to try and demonstrate that just because the title of the Tradition appears to limit its usefulness in the contemporary security environment, the moral reasoning it represents is actually a very useful set of criteria that can be applied in a much broader set of contexts than might initially be imagined. The less convincing the answers are to the questions posed by the Tradition when taken overall, or if one particular area represents obvious or profound problems, the harder it is to claim legitimacy for one's actions. Were we were to disregard the Just War Tradition, and several millennia of structured thinking about the normative dimension of conflict in favour of something new and bespoke for the current age, we would predictably end by producing a very similar list of necessary conditions for justification anyway. The key questions the Tradition asks about things such as just cause, right intention, legitimate authority, last resort, and proportionality, are, at the very least, things that should be considered before breaking the 'normal' rules and consciously acting so as to harm others. In exactly the same way, we would also need to appeal to certain principles to guide the conduct of the exception, by seeking to limit the necessary harm to those who in some way have made themselves liable, and that any harm to innocent parties is nevertheless limited as far as possible and is proportional to what is trying to be achieved.

---

[1] This article has developed out of the ideas articulated in: D Whetham and George R. Lucas, Jr., 'The Relevance of the Just War Tradition to Cyber Warfare', in James Green (Ed) Cyber Warfare: A Multidisciplinary Analysis (Routledge, 2015).

[2] D Whetham, *Just Wars and Moral Victories: surprise, deception and the normative framework of European War in the later Middle Ages* (Leiden: Brill, 2009), 36.

[3] Neville Chamberlain, Prime Minister's Address to the British People, 11.15am, 3rd September, 1939.

[4] Jean-Pierre Vernant, Myth and Society in Ancient Greece, trans. J. Lloyd (London: Methuen, 1992), 27.

[5] JT Johnson, *The Just War Tradition and the Restraint of War* (Princeton: Princeton

University Press, 1981).
[6] R Sorabji and D Rodin (eds), The Ethics of War: Shared Problems in Different Traditions (Aldershot: Ashgate, 2007), 7.
[7] D Whetham, 'The Just War Tradition: a Pragmatic Compromise', in D Whetham (ed.) Ethics, Law and Military Operations (Basingstoke: Palgrave Macmillan, 2010), 65.
[8] Gates was quoting Colin Gray. See Robert M Gates, 'A Balanced Strategy: Reprogramming the Pentagon for a New Age', *Foreign Affairs*, Jan/Feb (2009). http://www.foreignaffairs.com/articles/63717/robert-m-gates/a-balanced-strategy
[8] http://www.army.mod.uk/operations-deployments/22753.aspx
[9] Russell W Glenn, 'Thoughts on "Hybrid" Conflict, *Small Wars Journal*, March 2009.
[10] Allen Buchanan & Robert O. Keohane, 'Toward a Drone Accountability Regime', *Ethics & International Affairs*, Vol 29, 1, Spring (2015), 16.
[11] Neta C Crawford, 'Accountability for Targeted Drone Strikes Against Terrorists?' *Ethics & International Affairs*, Vol 29, 1, Spring (2015), 39.
[12] T Rid, 'Cyber war will not take place', Journal of Strategic Studies, vol. 35, no. 1 (2012), 7.
[13] Remarks by the President on Request to Congress for Authorization of Force Against ISIL, 11th Feb, 2015. https://www.whitehouse.gov/the-press-office/2015/02/11/remarks-president-request-congress-authorization-force-against-isil
[14] Spencer Ackerman, 'Pentagon Spec Ops Chief Sees '10 to 20' More Years of War Against Al-Qaida', *Wired*, 16th May 2013 http://www.wired.com/2013/05/decades-of-war/
[15] Robert M Gates, 'A Balanced Strategy: Reprogramming the Pentagon for a New Age', *Foreign Affairs*, Jan/Feb (2009). http://www.foreignaffairs.com/articles/63717/robert-m-gates/a-balanced-strategy
[16] http://www.army.mod.uk/operations-deployments/22753.aspx
[17] Nicholas Watt, 'David Cameron: 'snoopers charter' will reappear after Tory election win', *The Guardian* 11th Jan 2015 http://www.theguardian.com/politics/2015/jan/11/david-cameron-snoopers-charter-tory-election-win
[18] Rosa Brooks, 'There's No Such Thing as Peacetime', *Foreign Policy*, 13 March (2015).
[19] For example, see David Whetham, 'Drones and Targeted Killing: Angels or Assassins?', in BJ Strawser (Ed), *Killing by Remote Control: The Ethics of an Unmanned Military* (Oxford: OUP June 2013).
[20] How could this be the case? Stored data can be manipulated and changed, then attention drawn to it triggering known protocols put in place to prevent societal harm – a risk averse culture means that action must be taken when the alarm is raised rather than waiting for the problem to grow and be beyond doubt. Social media can be mined for data linking individuals, reports can be fabricated and then subsequently denied, but it takes time to disprove apparently credible information targeted at the right outlet. NGOs, like all other institutions, need funding and some may be led in a certain direction by a concerned benefactor. Worker agitation is nothing new, and a prison population is particularly vulnerable to well placed rumours. International financial institutions have multiple interests in many countries, and of course, shareholders who can influence policy.
[21] Carl von Clausewitz, *Vom Kriege* (Berlin: Ullstein 1832, 1980), p.27.

[22] Rid, *Cyber War*, p.7.
[23] Clausewitz, *Vom Kriege*, p.44.
[24] Rid, *Cyber War*, p.8.
[25] The following argument is adapted from D Whetham, 'Cyber Chevauchées: Cyber War Can Happen', in BJ Strawser, Adam Henschke and Fritz Allhoff, *Binary Bullets: The Ethics of Cyberwar* (Oxford University Press, 2015).
[26] Crown Prosecution Service, *Offences against the Person, incorporating the Charging Standard* http://www.cps.gov.uk/legal/l_to_o/offences_against_the_person/ accessed 17 April 2015.
[27] Carl von Clausewitz, *On War*, ed. Michael Howard, Peter Paret and Bernard Brodie (Princeton, NJ: Princeton University Press, 1989), 92.
[28] The medieval chevauchée could, on occasions, be used to try and get one's opponent to commit to battle in order to prevent your activity, but this was rare in comparison to its use as a means to force a compromise agreement. See D Whetham, *Just Wars and Moral Victories: surprise, deception and the normative framework of European War in the later Middle Ages* (Leiden: Brill, 2009).
[29] For example, see Bradley J Strawser (ed.), *Journal of Military Ethics Special Issue on Cyberwar and Ethics*, Vol. 12. No.1. April 2013.
[30] Yoram Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference', *International Law Studies*, Vol 89, 2013, p.281.
[31] This and other arguments can be found in Whetham, 'Cyber Chevauchées'.
[32] For a fuller exposition of this argument, see Whetham and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*.
[33] *Ibid*.
[34] George R. Lucas Jr., 'Moral order and the constraints of agency: Toward a new metaphysics of morals', in Neville, R.C. (ed.) *New essays in metaphysics*, (Albany: State University of New York Press, 1987).
[35] D Whetham, 'Ethics, Law and Conflict', in Whetham, *Ethics, Law and Military Operations*, 15.
[36] Whetham, 'A Pragmatic Compromise', in Whetham, *Ethics, Law and Military Operations*, 84.
[37] S Waterman, 'U.S.-Israeli cyber attack on Iran was "act of force," NATO study found', 24 March 2013, *The Washington Times* [Online], http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all
[38] Whetham, 'A Pragmatic Compromise', in Whetham, *Ethics, Law and Military Operations*, 77.
[39] For a good discussion this area, see DK Chatterjee (ed.), *The Ethics of Preventive Warfare* (Cambridge: Cambridge University Press, 2013).
[40] Whetham and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*.
[41] M Walzer, *Just and unjust wars: A moral argument with historical illustrations*, 2nd edition, (New York: Basic Books, 1992). See also Michael Gross, *The Ethics of Insurgency: A Critical Guide to Just Guerrilla Warfare* (Cambridge University Press, 2015).
[42] Whetham, *Just Wars and Moral Victories*, 218.
[43] David E Sanger and Michael S Schmidt, 'More Sanctions on North Korea After Sony Case', *The New York Times* Jan 2, 2015.

http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html?smid=tw-share&_r=0

[44] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 23 Dec (2014).

[45] *Ibid.* Others are less convinced. For example, see A Critical Review of Tom Rid and Ben Buchanan's "Attributing Cyber Attacks", *Digital Dao*, 6 Jan 2015. http://jeffreycarr.blogspot.co.uk/2015/01/a-critical-review-of-tom-rid-and-ben.html

[46] See Whetham, *Just Wars and Moral Victories*, 75.

[47] *Ibid*. 80.

[48] Whetham, *A Pragmatic Compromise*, 77.

[49] Lukasik suggests that defence will play 'a larger role in cyber deterrence than in the nuclear case', where defences were seen as destabilizing the nuclear balance. See Stephen J Lukasik, 'A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains', Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (National Research Council, 2010), 102. http://www.nap.edu/catalog/12997.html

[50] For example, Clark and Landau argue that 'deterrence must be achieved through the governmental tools of state, and not by engineering design'. See David D. Clark and Susan Landau, 'Untangling Attribution', Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (National Research Council, 2010), 40. http://www.nap.edu/catalog/12997.html

[51] '[I]f the machine is an intermediary belonging to an innocent user, the degree of punishment (if it is allowed at all) must be carefully crafted to fit the crime.' See Clark and Landau, *Untangling Attribution*, 37.