Digital War (2023) 4:26–34
https://doi.org/10.1057/s42984-022-00043-8

ORIGINAL ARTICLE

Terrorism and the lawful preemptive use of force: the case of cyberattacks

Jean-François Caron[1,2]

Received: 16 October 2021 / Revised: 28 February 2022 / Accepted: 4 April 2022 / Published online: 11 May 2022

Abstract
Twenty years of war against terror has led to humanitarian tragedies where the West has chosen to intervene in addition to being unable to durably eradicate the terrorist threat. As this text argues, this situation calls for a renewed strategy that needs to amend the legitimate use of force by reconsidering the criteria of pre-emptive actions in order to pave the way for non-violent and violent alternatives to war. In this regard, different forms of cyber actions can play a significant role in this well-needed renewed strategy.

Keywords Terrorism · Cyberattacks · Pre-emption · Alternatives to war · Credibility of a threat · Stuxnet cyberattack

Introduction

The still on-going 'global war on terror' that has resulted from the 9/11 attacks has allowed us to witness one of the greatest humanitarian mistakes and political misinterpretations in mankind's history of warfare.

Firstly, the decisions to invade Afghanistan and Iraq, respectively, in 2001 and 2003 have shown that relying on full-scale wars to fight the terrorist threat can lead to the worst humanitarian outcomes. Indeed, these cases speak for themselves as they have both led to the deaths of hundreds of thousands of innocent civilians, which is highly paradoxical in light of the logic that supported these interventions. If the objective of these wars was to prevent the unjustified death of non-combatants, it is clear that they have simply transferred that risk (Shaw 2005) to the Iraqi and Afghan civilians,[1] as if 'our' lives had more value than 'their' lives, which is, of course, morally problematic. From this perspective, it is not difficult to understand why the fight against terrorism has been labelled by some as being terroristic as well. Moreover, full-scale wars against terrorist threats have very often resulted in a lack of political stability as well as an incapacity to eradicate the menaces that led to their beginning. In the case of Afghanistan, the withdrawal of US forces from the country in August 2021 has led to the return to power of those who once provided safe haven to members of Al-Qaeda in the years that preceded 9/11 in a way that has prevented the United States from saving face by implementing what Henry Kissinger has once labelled a 'decent interval' (Caron 2015).

Furthermore, in some cases, these interventions have even been directly linked with the emergence of new threats, as was the case of the Islamic State of Iraq and the Levant (ISIL) following the 2003 invasion of Iraq. At the end of the day, nothing has really changed, and it is hard to claim victory when the eradication of the initial menace has led to the creation of another one as—and sometimes more—dangerous than the former. For all these reasons, if these are the inherent disproportionate consequences of waging war against terrorism, there would be serious grounds to argue that this way of dealing with such groups is morally questionable.

Secondly, Western states have made the mistake of thinking that it is actually possible to win a war against terrorism. However, contrary to a state that can be defeated and against whom peace can be achieved following an armistice or a formal peace treaty, the large deployment of troops can do very little against an idea that will end up inspiring lone wolves or small cells all around the world and who will strike devastating and murderous blows at civilians who are calmly enjoying an evening walk on a boardwalk or a drink on a terrace, or simply reading a book on the subway on their way to

✉ Jean-François Caron
jean-francois.caron@nu.edu.kz

[1] Nazarbayev University, Nur-Sultan, Kazakhstan

[2] University of Opole, Opole, Poland

work. This Sisyphean strategy of waging war against terrorism is doomed to bring endless wars and destruction. Twenty years after the 9/11 attacks, this should now be obvious.

This paper considers, however, that the way the lawful use of force is considered does not provide effective solutions to prevent that reality from occurring. The main reason being that the resort to lawful violence has traditionally been thought to be the sole prerogatives of states, thereby creating a legal vacuum when it comes to non-state actors. This paper then suggests how the lawful use of force could be amended in a way that will allow states that are targeted by terrorist groups to defend themselves without leading to full-scale wars and, consequently, bring detrimental humanitarian and political consequences like those we have witnessed in the last twenty years. More specifically, I argue that a reconsideration of the principle of pre-emption based upon new criteria that are more adapted to the terrorist threat might allow states to have at the disposal the possibility to resort to violent or destructive alternatives to war with some forms of cyberattacks considered as proper means of actions.

This paper is divided into three parts. The first, focuses on the ways political violence is legally justified and how the current legal framework is hardly applicable against terrorist organisations because of the unique nature of violence they are favouring. The second, explains how this legal framework can be amended in a way that would allow states to resort to pre-emptive measures against these groups as well as evoking the ethical guidelines that ought to restrain this form of violence. Finally, I will consider how some forms of cyberattacks can be effective and morally justified alternatives to war against the terrorist threat.

The lawful use of force and its limits against terrorism

After two bloody global conflicts in the course of thirty years that have cost the lives of tens of millions of individuals, architects of the post-1945 international order gave themselves the goal to limit all resort to armed forces which was set out in Article 2(4) of the UN Charter. They nonetheless agreed to limit the lawful use of force to exceptional cases and always for the sake of self-defence (Neff 2005, p. 314). Indeed, Articles 41 and 42 of the UN Charter allows the international community to intervene and resort to measures akin to war in order to maintain or restore peace when it is either threatened or when a state has been victim of an aggression by another state. Irrespective of the UN's capacity or willingness to uphold this principle, the Charter has also maintained states' inherent right to defend themselves against an unlawful act of aggression. In this regard, and whether it was or not the intention of those who wrote the Charter in 1945, international law allows for this right of self-defence to be triggered not only after a state has been victim of a violation of its sovereignty, but also when it is facing a threat of aggression that is imminent and leaves no choice of means and no moment for deliberation.

Such a situation is known as a pre-emptive attack and finds its roots and principles in the *Caroline* incident of 1837, which involved the sinking of an American steamer operating on the Niagara River by the British forces. However, because firing the first shot can easily be perceived as an act of aggression, it is necessary for states claiming that such an action was triggered by a threat to their sovereignty to prove that it was actually the case. Philosopher Michael Walzer has reformulated this idea with three criteria, namely that the enemy displays 'a manifest intent to injure' and 'a degree of active preparation that [makes] that intent a positive danger' in such a way that 'waiting, or doing anything other than fighting, greatly [magnifies] the risk [to the state being targeted by this threat]' (2006, p. 81). For him, the Six-Day War of 1967 constitutes a good example of a pre-emptive attack that met these criteria. Indeed, three weeks before Israel struck the first blow, the UN had announced that its Emergency Force that had served as a buffer between Israel and Egypt in the Sinai since the end of the Suez Canal Crisis was to be withdrawn. Immediately, the Egyptian armed forces reoccupied this territory, while the Egyptian government closed the Gulf of Aqaba and the Strait of Tiran to Israeli boats. At the same time, the Egyptian armed forces were put on maximum alert and mobilised while military alliances were signed with Jordan, Syria, and Iraq. Finally, Gamal Nasser, the Egyptian President, declared on 29th May that in the eventuality of a war against Israel, his 'goal would be nothing less than [its] destruction' (Walzer 2006, p. 83). Faced with these threats, Israel attacked its enemies on 5th June as it became clear to its government that it was only a matter of days before the country would be under attack.

However, because of the reality of the world order following WWII, this understanding of legitimate violence can work only when we are dealing with conflicts between states and less with non-state entities. This creates a major problem since the pre-emptive logic is now of little use against terrorist groups. Indeed, contrary to state actors, it is very difficult to effectively prevent a terrorist threat from occurring through the logic of pre-emptive self-defence (Buchanan and Keohane 2004, p. 3), which makes the war against terror unique. Unless some concrete information about an upcoming terrorist attack becomes available, what is lacking here is the previously mentioned imminence criterion that cannot be assessed with these groups; because of their *modus operandi*, these elusive enemies are able to covertly attack and kill thousands of civilians without any precursory signs. In fact, contrary to state actors planning to violate another state's sovereignty, terrorist groups do not display the mass mobilisation of troops and military equipment alongside

their enemy's borders. On the contrary, because of the asymmetrical nature of their fight against great powers, their success relies on the element of surprise. Indeed, sticking with the notion of imminence against this type of threat is a recipe for disaster.

Owing to terrorist groups' surprise attacks and their potentially apocalyptic use of weapons of mass destruction (WMD), waiting for their threats to become immediate is suicidal (Beres 1991; Glennon 2002). This is why Dominika Svarc has argued that:

> The particularly grave threats which could materialize in attack without a reasonable degree of warning and time for defense may be regarded imminent even when the attack is not menacingly near. (…) Applying the narrow temporal standard of imminence in such contemporary reality might deprive a State from an opportunity to effectively repel the attack and protect its population from unimaginable harm. It would go counter to the object and purpose of the right of self-defense which provides States with a self-help mechanism to protect them from an attack when peaceful alternatives would prove inadequate and the multilateral response too tardy (2006, p. 184).

As a consequence, if states wish to abide by the current rules of international law, this basically leaves them with only one lawful option: wait to be under attack before claiming the right to self-defence, as any other proactive form of self-defence would de facto qualify as preventive in the absence of hard evidence that a terrorist group is about to strike. This is obviously a highly questionable option from a moral perspective, as states have to paradoxically first sacrifice the lives of their citizens in order to have a right to defend them. If states cannot effectively deflect this threat and protect their citizens through pre-emptive actions, there is a need to correct the situation through proactive actions that will not lead to full-scale wars like the 2003 invasion of Iraq. This implies two things: (1) reviewing the criteria regarding what ought to justify a pre-emptive strike which means replacing the criterion of imminence with another one, and (2) to envisage pre-emptive means of actions that will not lead to full-scale wars but rather to highly limited harm and destruction. The next section will focus on the first aspect.

Rethinking the admissibility of preemptive use of force against terrorism

Reassessing the pre-emptive attack logic is highly controversial and does not come without serious concerns since, as according to Deen Chatterjee, the '(…) US war on terror [against Iraq is] an example of what could go wrong with [a more permissive logic of political violence]' (2013, p. 2). The most important of these concerns is the adoption of an overly generous view of what constitutes an imminent threat, which would lead to a legitimisation of wars against entities that are not really a menace, ultimately leading to further destabilisation of the world order by setting off "a cascading series of 'preventive' attacks or interventions" (Bethke Elshtain 2013, p. 23). However, because of the terrible consequences of terrorist attacks and the inherent difficulties in foreseeing them, there is a need to act before these groups strike, which of course creates an incredible dilemma. In the words of legal theorist George Fletcher, there is a legitimate reason why we ought to avoid an unlawful strategy that prematurely legitimises the resort to force and, contrarily, to come up with an approach that makes retaliation after a terrorist attack has succeeded the sole option (1998, p. 133). This is why we cannot consider all forms of preventive actions under the same lens and why the criticisms usually associated with preventive wars against unfounded enemies cannot apply to those posed by the terrorist organisations described earlier. This renewed approach to violence ought to remain as limited as possible and should be based on an assessment that leaves little doubt about the nature of the threat, which is close to Walzer's understanding of the distinction between non-legitimate and acceptable use of preventive violence that ought to depend on a reasonable perception of the danger of the threat (2006, p. xiv). This begs the question of what ought to be that new threshold?

Since, by nature, terrorist groups resort to intimidation against individuals to pressure targeted states to change their policies, and such intimidation usually involves threats to kill or physically harm people, it would appear self-evident that we ought to have the right to strike before they fulfil their promise of destruction. However, this solution poses problems of its own. Indeed, in criminal law, threatening to kill or harm someone does not imply that the person who poses the menace ought to lose his immunity against violence. Such an outcome would depend on two important factors, namely the specific nature of the threat and its credibility. For instance, a drunk customer in a pub, barely able to stand on his feet and threatening to kill all the other customers if he is not served one more drink, would most probably fall short of meeting the threshold for prosecution as no reasonable individual would consider that his threat is actually genuine The reaction would, however, be different if three lucid, muscled guys armed with guns made the same threat. In this case, the other customers would probably consider the threat credible and genuinely fear for their lives. In this scenario, the public display of weapons pointed in their direction would allow the customers to resort to all possible actions, including deadly force, against the three men, a reaction that would be deemed commensurate with the nature of the threat and justified as a matter of self-defence. On the contrary, using the same level of violence against

the stumbling drunk would clearly not be proportionate to the menace he poses, as his worrying words would not be linked in any way with his actual capacity to fulfil his threat. Therefore, having the actual intentions and means of achieving one's ambitions is a fundamental variable to consider.

Of course, one does not need to wait until the attacker's threat becomes a reality before having the right to react and individuals who are facing this menace may protect themselves or count on the state's authorities to do so in their name. Indeed, credible threats against people's lives have always justified resorting to potential lethal counter-measures against their perpetrators, irrespective of whether or not they have the willingness to transform their threats into reality. In such a case, the appreciation of the threat and the methods that ought to be used to fight it are in the eyes of the beholder. For instance, let us imagine that a man walking his dog in a park is suddenly threatened by someone holding a handgun, who asks him to choose between his wallet or his life. However, this turns out to be an empty threat as the weapon is either not loaded or loaded with blank rounds. At the exact same time, a police officer on duty witnesses these events and is able to hear the perpetrator threatening the innocent walker. There is no doubt that he would be justified in using all possible means—including lethal ones—against the former individual. In this case, the threat is sufficiently credible and the police officer is not required to wait until the perpetrator pulls the trigger before acting. If he were to use his service pistol to neutralise the menace and it were to later be discovered that the perpetrator was not actually in a position to harm anyone, it would not make the police officer's decision less legitimate. In appearance, this is exactly the situation with terrorist organisations that make credible threats.

There is, however, a major difference between them and the aforementioned case of the man menacing the individual walking his dog, as in the latter case the threat to someone else's life is *credible, immediate, and imminent* from an empirical perspective. Such a situation is very similar to the cases of countries like Egypt, Syria, and Jordan, which were obviously planning an attack against Israel in 1967, and the aforementioned police officer's reaction would fall within the category of a justified pre-emptive attack. However, this is not really the case with terrorist organisations, whose verbal threats are not always perceived as imminent. This is, of course, a problem as words alone do not contribute to transforming a menace into a credible threat that requires immediate action. Consequently, and contrary to the previous case, resorting to pre-emptive counter-measures would not be justified. If we were to justify the resort to war solely based on verbal threats, the world would soon become even more chaotic and violent than it currently is. It is, nonetheless, also a dangerous game to automatically regard all sorts of threats as trivial and to systematically downgrade them simply to rhetorical hyperbole, especially when these threats are coming from terrorist groups. The crux of the problem with these entities is that there is rarely any transitional point between their verbal threats and the attack itself. As already stated, it must be noted that their *modus operandi* is unique in the sense that it is basically impossible for states to act pre-emptively when an attack from these groups becomes imminent as their strategy is all about striking at states covertly and taking them by surprise. In the case of the aforementioned example, the terrorist threat will not take the form of an individual approaching him with a handgun and an explicit threat to his life. It will rather take the form of a menace that will never be foreseen by the man until it is too late. More precisely, in this case, the threat will come from a bullet fired from hundreds of yards away by a well-hidden sniper or by a bomb that has been carefully concealed in a garbage bin, set to explode when the man approaches. In this situation, despite being real, the terrorist threat is not imminent to anyone because of its invisible nature.

From this perspective, a warlike rhetoric coming from a state whose decision to transform its words into actions will always be empirically obvious through clear evidence of its willingness to strike, just as is the case with an armed man walking towards you and threatening to kill you if you don't give him your wallet. In the case of states, this threat will take the form of the mobilisation of their armed forces and other preparations that indicate an upcoming attack, as it was the case with Russian against Ukraine in February 2021. If the resort to violence can be justified in such cases, it is not so with threats that cannot be seen.

Furthermore, the types of weapons terrorist organisations threaten to use against us and their risk-averse nature that differs from state entities are also factors that need to be taken into account. It is, of course, possible to adopt a broad and anticipatory interpretation of what constitutes a credible threat, such as the one by David Luban, who believes that a threat is credible when its propensity for future armed attacks is clearly based upon characteristics such as 'militarism, an ideology favouring violence, a track-record of violence to back it up, and a build-up in capacity to pose a genuine threat' (2004, pp. 230–231). When the international community faces such a threat, he believes we ought to be justified in resorting to preventive measures against it.[2] In this case, it also means that such measures should have been taken against the Soviet Union from 1945 to 1949, against North Korea before both countries were able to develop nuclear weapons and the means to use them against the rest of the world. In fact, alongside the aforementioned terrorist threat, the nuclear menace from a rogue state is also from a theoretical perspective a very good example of the shortcomings of the pre-emptive logic. Indeed, thanks to intercontinental missiles or first-strike weapons such as submarines, rogue states (that show no concern whatsoever for human

rights and display an aggressive rhetoric) now have the possibility to fire their missiles of death on their targets with little or no warning in a matter of less than half an hour. In fact, Manhattan Project scientist H.D. Smyth once described this weapon as being 'so ideally suited to sudden unannounced attack' (1945, p. 134), while Caryl Haskins called it 'an ideal weapon for aggressors' and Robert Oppenheimer 'a weapon of surprise' (Freedman and Michaels 2019, pp. 55–56). This is why 'preventive-war thinking was surprisingly widespread in the early nuclear age', more specifically 'the period from mid-1945 through late 1954' (Trachtenberg 2007, p. 43). After all, is there a threat more imminent than a nuclear apocalypse that can fall on our heads within the next 30 min?

Such a prospect has nonetheless led the international community to adopt a more liberal understanding of pre-emption and imminence. This threat pose by a state actor also needs to consider the chances that this rhetoric and weapon development may actually result in their actual use, especially when the possession of these weapons is widespread among nations. In this regard, there is a fundamental difference between a state actor—even a rogue one—and terrorist organisations, namely the fact that the former is a risk-averse entity. Indeed, because of their territorial nature, states—even rogue ones—remain perfectly aware that a nuclear strike on their part would very likely result in self-destruction through nuclear retaliation. This is why many Western leaders do not see Vladimir Putin's 2022 invasion of Ukraine as a precursory sign of Russia invading other countries in the near future (especially those that are members of NATO). On top of the fundamental shortcomings his army has shown in the first stage of this war, the fear of his own potential destruction if Russia were to enter in an open war with NATO (with three of its members having nuclear weapons) contributes to make Putin's menaces against the West not so credible even though they check all the boxes of Luban's aforementioned conception of pre-emption. In other words, when state entities are concerned, the mutual possession of such weapons of absolute terror is understood as a guarantee that they will not enter at war with one another even when some leaders who possess them may be thought to have delusion of grandeur or to be suffering from other mental problems.[3] We seem to assume in this regard that, as the character of Lieutenant Commander Hunter played by Denzel Washington said in the 1995 movie *Crimson Tide*, that the true enemy is war itself in a conflict between two nuclear powers.

However, this fear of mutual assured destruction is not necessarily a concern with terrorist organisations; because of their non-territorialised nature and fanaticism, they do not have the same sensitivity to the consequences of their actions. In this sense, if there are reasons not to exaggerate such threats from state actors, there are also reasons not to show the same optimism with terrorist groups. In other words, the terrorist threat is not only invisible, but it is also potentially more destructive and indiscriminate than the one coming from state entities.

There are, therefore, reasons to believe that the way the pre-emptive logic is conceptualised poses problems in the context of contemporary terrorist organisations and that it ought to be amended to enable states that are threatened by these groups to use more proactive measures to defend themselves and protect their citizens (Schmitt 2004; Franck 2002). Thus, we are obligated to abandon the notion of imminence understood as a threat being real in actual time and to go beyond the temporal proximity of a threat by thinking about a new threshold that will need to be crossed before an anticipatory act of self-defence can be justified since terrorist attacks will never meet the former standard. This void can be filled with the already mentioned notion of the 'credibility of a threat', which can be highlighted with the two previous examples of offenders threatening customers in a bar. This course of action ought to be used solely against groups whose threatening rhetoric matches their actual capacity to transform their promises into reality. This means that an organisation that promises to drop a nuclear weapon in a crowded urban area but that does not have the capacity to do so should be considered similarly to the drunk customer in a pub and, accordingly, should not be treated in the same way as a group with the genuine capacity to fulfil this threat.

The case for pre-emptive measures short of war: the example of cyberattacks

Following what has been said previously, the threat of contemporary terrorism requires us to rethink the threshold of legitimate violence under new criteria. As terrorist attacks will rarely appear as imminent as those of state actors, pre-emptive forceful measures therefore ought to be used against entities that are posing a credible threat. Such measures can be either non-violent or destructive and lethal. The former set of measures are usually those that are referred to as 'soft war measures' (Gross 2015; Gross and Meisels 2017) or as 'non-violent alternatives to war' (NVATW) and include measures such as the imposition of economic sanctions or arms embargoes, and the use of diplomacy.

We cannot deny that NVATW can prove efficient at preventing terrorist organisations from ever being able to fulfil their promises of destruction if they are deprived of their capacity to acquire WMD thanks to international surveillance by targeting states that are harbouring or sponsoring them. The idea behind such sanctions is making the targeted state realise that pursuing this course of action is a political dead end that will most likely be detrimental to the survival of its regime. If this is achieved, the risks

of these organisations' threats ever becoming credible are slim to none, which eliminates the necessity of setting down the path to what I have described elsewhere as 'violent alternatives to war' (VATW) (Caron 2021a, b). However, when NVATW have proved ineffective or when there are reasons to believe that they will not result in preventing credible a terrorist threat from becoming real, the resort to VATW ought to be considered, e.g. destructive and/or lethal measures on a limited scope and scale.

It must nonetheless be stressed that the physical eradication of the terrorist threat must not come at the expense of other duties, with the most important being the obligation to restrict the use of violence only against those who are legitimate targets. We need to emphasise the importance of the fact that justifying a more permissive use of political violence does not eliminate in any way the usual ethical constraints statesmen and members of the military ought to respect. Thus, these additional duties imply that the use of deadly or destructive force will need to be proportional to the nature of the threat and respectful of the discrimination between combatants and non-combatants. In this regard, states will have to consider a wide variety of options ranging from sending elite troops on the ground (whose actions will be limited to a surprise operation with limited usage of weapons) to the use of drones[4] with a much larger scope of destruction. One of the main criteria they will have to consider is the nature of the environment in which the individuals to be targeted are operating. More precisely, irrespective of the seriousness of the threat, the approaches may have to be very different if these individuals are located in the middle of the desert or in a densely populated area.

More precisely, the criteria that ought to be followed when it comes to the use of VATW are very similar to those that have been put forward by the Israeli High Court in a famous decision about the lawfulness of targeted killings (2006). These are in my view the most important principles to follow:

1. VATW can only be justified against enemies who are, based on reliable, authentic, and confirmed information from multiple sources independent from one another, posing a credible threat to civilians, more specifically that they have at their disposal the means to effectively transform their menace into reality or are actively trying to achieve this goal. Since individuals who will be victims of VATW are deprived of due process of law, a departure from this rule must not be taken lightly;
2. VATW are only permitted if NVATW are thought to be ineffective at eliminating the threat. This means that the resort to VATW must take into account the actual capacity of preventing the terrorist from striking first through NVATW;
3. VATW must solely be used for the sake of eliminating the identified threat and must end as soon as the menace has been eliminated;
4. Resorting to VATW must not result in disproportionate danger to civilians who might happen to be in the vicinity when the operation will take place or create unnecessary risks to the soldiers who will be deployed[5];

Cyberattacks can constitute valuable and effective NVATW against terrorist organisations. For instance, knowing that terrorist organisations cannot operate without financial resources, cyber heists can count as cyber measures short of war as they may contribute to hamper the capacities of terrorist organisations to strike against their enemies.[6] At the same time, cyberattacks can also play a constitutive part of VATW. We can think in this regard to cyber-assassinations. Hypothetically, cyber-assassinations would constitute a similar way of dealing with individuals who are involved in terrorist organisations that are posing a credible threat by, for example, remotely gaining control of their pacemakers[7] and delivering a shock in order to kill its users in a way that resembles the assassination of the US Vice-President in the television series *Homeland*, or by taking control of critical functions of their automobiles.[8] They can also play a role in the targeting of the infrastructures of a state collaborating with terrorist organisations that are suspected to produce or be instrumental in the production of WMD can take many forms, such as the cyberattacks directed against the Natanz nuclear facility in Iran by a malware known as 'Stuxnet' (Caron 2019c). Introduced inadvertently or on purpose by an employee who most likely plugged a contaminated USB drive into the central computers of the facility (which was not connected to the Internet), the virus—allegedly created by Israel and/or the US—managed to take control of nuclear centrifuges and caused them to malfunction and self-destruct, while sending contradictory messages to the operators who thought everything was in order. Although Iran never released specific information about the incident, it is estimated that around 1000 uranium-enriching centrifuges were destroyed, which led to a significant decrease in the country's enrichment efficiency (Broad et al. 2011) and delayed its capacity to potentially develop nuclear weapons by as much as two years (Stiennon 2015, p. 20).

I would argue that the Stuxnet virus constitutes a clear example of what I am defending as a pre-emptive attack under the lens of threat's credibility rather than its imminence. In this case, this cyberattack was not simply launched out of fear that Iran may eventually disrupt the regional balance of power, but rather that the WMD resulting from its nuclear programme could have easily fallen into the hands of stateless terrorist organisations. For instance, it is known that Iran has been providing various kinds of support to terrorist organisations—namely, the Hezbollah and the Hamas.

Moreover, alleged links with Al-Qaeda were found in connection with the 1998 attacks against the US embassies in Tanzania and Kenya (Thiessen 2011), the attack against the USS Cole (Hsu 2015), and even with the events of 9/11 (The 9/11 Commission Report, pp. 240–241). Additionally, the way in which the Iranian authorities deceived the international community about the nature of its nuclear programme also raised serious questions as to whether it was purely dedicated to civilian purposes. Alongside the discovery of undeclared nuclear facilities—namely, the Natanz complex, a heavy water production plant under construction in Arak, as well as centrifuges that were clandestinely imported in the 1980s—the rhetoric used by then Iranian President Mahmoud Ahmadinejad also contributed to fuel the credibility of the risk that Iran may eventually try to develop a nuclear weapon. Indeed, in 2006, he announced the decision to resume uranium enrichment at Natanz, which led the UN Security Council to adopt Resolution 1696, which was ignored by Iran. When all these elements are taken into account, it is possible to argue that the prospect of a country known for its close ties with terrorist organisations that use indiscriminate means of warfare having a nuclear programme with military dimensions posed potentially serious threats. There were, therefore, solid grounds to resort to this type of alternative to war in order to prevent this programme from ever being completed after other NVATW did not result in altering Iran's policy. In this sense, by opening up the possibility of resorting to VATW, states threatened by the Iranian nuclear menace were able to benefit from an additional arrow to their bow rather than simply seeing themselves as out of options and obligated to launch a full-scale war as it was the case in 2003 when the United States invaded Iraq.

In return, we also need to be aware of the inherent limitations of cyberattacks as NVATW or as VATW. The most important problem remains certainly that effective cyberattacks such as the Stuxnet cyberattack was only possible because the threat posed by the Iranian nuclear program was not imminent in the conventional meaning of the term, which allowed in return the entities that sponsored the development of this highly complex computer virus enough time to develop and deploy it before it was too late. In this perspective, an effective cyberattack as a deterrent force requires time and a lot of resources and preparation, meaning that it may only be an option to consider for states that are proactive in seeing the development of credible threats. This implies that states choosing to resort to this alternative to war must in parallel deploy a significant amount of energy on their intelligence agencies and enjoy a significant collaboration from their foreign counterparts. Similarly, to other forms of actions, we have to be aware that an ill-designed and precipitated cyberattack may simply lead to disproportionate consequences and end up violating the moral rules of warfare, as it can be the case with drones. Just like any other types of alternatives to war, a cyberattack should not be seen as a panacea in itself.

Conclusion

Looking back at the last 20 years of the war on terror, it is difficult not to have a very critical assessment of its effectiveness and morality. Following the rather chaotic withdrawal of the United States from Afghanistan in August 2021, those who once harboured Al-Qaeda are now back in power. The 2003 intervention in Iraq has, for its part, led to a destabilisation of the Middle East and to the birth of another terrorist organisation—the Islamic State of Iraq and the Levant (ISIL)—that has happily followed the path of Al-Qaeda by picking up the torch of global terrorism. Twenty years after 9/11, although Al-Qaeda is no longer the threat it used to be and ISIL no longer enjoying control over its former caliphate, the terrorist threat has not been eradicated and remains still a clear and present danger with members of the latter organisation still holding a stronghold in Syria's Idlib region now posing a genuine threat in the broad Khorasan region, while Al-Shabab is still very active in the Horn of Africa region. In fact, the number of terrorist attacks has been on the rise since 2017 (Statista). Furthermore, we cannot ignore that the unquestionable desire of Western nations to protect their citizens has been made possible at the expense of the lives of tens of thousands of innocent civilians living in the regions where our military actively fought these organisations. Paradoxically, the improper way in which we have fought terrorism tends to provide arguments to those supporting these groups, that we have ourselves acted in a terroristic manner. Thanks to this perspective, it is not hazardous to argue that resorting to war against terrorism was simply a largely inefficient and immoral strategy.

This is why it is necessary to think of alternatives to war against these groups in order for states that are targeted by them to pre-emptively defend themselves, which requires a reconceptualisation of this notion. Indeed, because of the stateless nature of these groups, the criterion of imminence—which is a core element of the logic of the pre-emptive attack—simply does not apply to terrorism. Therefore, there is a need to find an alternative notion that will facilitate the justification of when it is legitimate to resort to force against these groups. Obviously, loosening up the rules surrounding this logic runs the risk of becoming a slippery slope that will ultimately erase the necessary distinction between pre-emption and prevention. This paper has suggested that the idea of terrorist groups posing a 'credible threat' is a viable alternative that can lead to NVATW or to VATW. In this regard, some forms of cyberattacks ought to

be considered as effective and legitimate examples of such measures and not necessarily as violations of another state's sovereignty when they are used in the context and according to the criteria discussed here.

Notes

1. As written by journalist Philip Bump (2018), 'During the war [in Iraq] and during the Islamic State militant group's occupation of as much as a third of the country in recent years, the number of deaths runs into the hundreds of thousands, including civilians killed as a result of violence and, more broadly, those who died because of the collapse of infrastructure and services in Iraq resulting from the ongoing conflict'. For its part, the Watson Institute (2020) estimated in October 2019 that a little more than 150,000 people have been killed in the Afghanistan war since 2001 and that 43,000 of them were civilians.
2. For him, 'preventive war may be justified against a rogue state (in the sense given here, a threat state) aiming to construct WMD (in the sense given here, weapons that can cause mass casualties through a single use), if the state's intentions are hostile, because if the state succeeds in constructing WMD it may be too late to forestall a genocidal attack' (2007, p. 190).
3. As evidence of this claim, people will argue that Stalin, Kim Jong-Il and his son Kim Jong-Un are example of ruthless amoral leaders thought to be or have been irrational, but who nonetheless refrained from using such weapons against their enemies, since they knew it would have led to their own destruction.
4. Of course proper drone strikes must be restricted with proper rules of engagement and according to the moral rules of warfare. In this perspective, it is possible to severely judge the U.S. policy on drone strikes that made an ample use of what is referred to as 'signature strikes', namely attacks against unknown individuals whose behaviours are considered suspicious according to certain patterns-of-life analysis. For instance, individuals seen digging a hole and hiding something on the side of a road will likely be targeted since their behaviours can be interpreted as typical of terrorists planting an improvised explosive device. This policy has led to many blunders over the last 20 years that have led analysts to conclude that drones are immoral weapons (Chamayou 2015). However, this assessment is in my view inaccurate since the way a weapon is being used should not lead us to conclude that it is inherently immoral (Caron 2020).
5. For a discussion on the military's duty of care towards its members, see Caron (2018, 2019a, b).
6. Thus far, the USD 81 million cyber heist of the Bangladesh central bank's account at the Federal Reserve Bank of New York by the Lazarus group in 2016 is the most famous.
7. Some pacemakers have wireless interfaces that allow doctors to adjust their settings at a distance and to share data logs online. As stated in a BBC report, 'In 2012, security researcher Barnaby Jack demonstrated an attack using the radio-frequency interface on a heart device. [He] said he was able to launch his attack from a laptop up to 50 ft (15 m) away' (Vallance 2015).
8. Although this last example may run counter to the discrimination principle, since this malfunction may lead to pedestrians or other drivers being hit.

References

Beres, L. R. 1991. On assassination actual armed attack by nonstate actors. *The American Journal of International Law*, *106*, 770–777.

Bethke Elshtain, J. 2013. Prevention, Preemption, and Other Conundrums. In *The Ethics of Preventive War*, ed. Deen K. Chatterjee, 15–26. Cambridge: Cambridge University Press.

Buchanan, A., and R. Keohane. 2004. The Preventive Use of Force: A Cosmopolitan Institutional Proposal. *Ethics & International Affairs* 18 (1): 1–22.

Bump, P. 2018. *15 Years after the Iraq War Began, the Death Toll is Still Murky*. https://www.washingtonpost.com/news/politics/wp/2018/03/20/15-years-after-it-began-the-death-toll-from-the-iraq-war-is-still-murky/.

Broad, W.J., J. Markoff, and D.E. Sanger. 2011. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times*, January 15. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Caron, J.-F. 2015. *La guerre juste: Les enjeux éthiques de la guerre au 21ème siècle*. Québec: Les Presses de l'Université Laval.

Caron, J.-F. 2018. *A Theory of the Super Soldier: The Morality of Capacity-Increasing Technologies in the Military*. Manchester: Manchester University Press.

Caron, J.-F. 2019a. *Disobedience in the Military: Legal and Ethical Implications*. Singapore: Springer.

Caron, J.-F. 2019b. Exploring the Extent of Ethical Disobedience Through the Lens of the Srebrenica and Rwanda Genocides: Can Soldiers Disobey Lawful Orders? *Critical Military Studies* 5 (1): 1–20.

Caron, J.-F. 2019c. *Contemporary technologies and the morality of warfare: The war of the machines*. London: Routledge.

Caron, J.-F. 2020. Defining Semi-autonomous Automated and Autonomous Weapon Systems in Order to Understand Their Ethical Challenges. *Digital War* 1 (1): 173–177.

Caron, J.-F. 2021a. *Violent Alternatives to War: Justifying Actions Against Contemporary Terrorism*. Berlin: De Gruyter.

Caron, J.-F. 2021b. *L'Occident face au terrorisme: Regards critiques sur 20 ans de lutte contre le terrorisme*. Québec: Presses de l'Université Laval.

Chamayou, G. 2015. *A Theory of the Drone*. New York: The New Press.

Chatterjee, D.K. 2013. Introduction. In *The Ethics of Preventive War*, ed. D.K. Chatterjee, 1–11. Cambridge: Cambridge University Press.

Fletcher, G. 1998. *Basic Concepts of Criminal Law*. Oxford: Oxford University Press.
Franck, Thomas M. 2002. *Recourse to Force*. Cambridge: Cambridge University Press.
Freedman, L., and J. Michaels. 2019. *The Evolution of Nuclear Strategy*. London: Palgrave MacMillan.
Glennon, M. J. 2002. Preempting terorrism: The case for anticipatory self-defense. *The Weekly Standard*, *7*, 19.
Gross, M. 2015. *The Ethics of Insurgency: A Critical Guide to Just Guerrilla Warfare*. Cambridge: Cambridge University Press.
Gross, M., and T. Meisels, eds. 2017. *Soft War: The Ethics of Unarmed Conflict*. Cambridge: Cambridge University Press.
High Court of Israel. 2006. *Public Committee against Torture in Israel v. Government of Israel*, Case No. HCJ 769/02, December 13.
Hsu, S.S. 2015. Judge orders Sudan, Iran to pay $75 million to family of USS Cole victim, *Washington Post,* March 31. https://www.washingtonpost.com/local/crime/judge-orders-sudan-iran-to-pay-75-million-to-family-of-uss-cole-victim/2015/03/31/a2105dd8-d7b8-11e4-ba28-f2a685dc7f89_story.html.
Luban, D. 2004. Preventive War. *Philosophy and Public Affairs* 32 (3): 207–248.
Luban, D. 2007. Preventive War and Human Rights. In *Preemption: Military Action and Moral Justification*, ed. Henry Shue and David Rodin, 171–201. Oxford: Oxford University Press.
Neff, S.C. 2005. *War and the Law of Nations. A General History*. Cambridge: Cambridge University Press.
Schmitt, M.N. 2004. Direct Participation in Hostilities And 21st Century Armed Conflict. In *Horst Fisher, Ulrike Froissart, Wolff Heinegg von Heintschel and Christian Rapp*, ed. Crisis Management and Humanitarian Protection, 505–529. Berlin: BWV Berliner-Wissenschaft.
Shaw, M. 2005. *The New Western Way of War*. Cambridge: Polity Press.
Smyth, H.D. 1945. *A General Account of the Development of Methods of Using Atomic Energy for Military Purposes under the Auspices of the United States Government 1940–1945*. Washington, D.C.: USGPO, August.
Statista. *Number of terrorist attacks worldwide between 2006 and 2020.* https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/.
Stiennon, R. 2015. A Short History of Cyber Warfare. In *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A. Green, 7–32. Abingdon, Oxfordshire: Routledge.
The 9/11 Commission Report. https://avalon.law.yale.edu/sept11/911Report.pdf.
Thiessen, M.A. 2011. Iran Responsible for 1998 U.S. Embassy Bombings, *Washington Post*, December 8. https://www.washingtonpost.com/opinions/iran-responsible-for-1998-us-embassy-bombings/2011/12/08/gIQAuEAAfO_story.html.
Trachtenberg, M. 2007. Preventive War and US Foreign Policy. In *Preemption: Military Action and Moral Justification*, ed. Henry Shue and David Rodin, 40–68. Oxford: Oxford University Press.
Vallance, C. 2015. Could Hackers Break my Heart via my Pacemaker?, *BBC*. December 3. https://www.bbc.com/news/technology-34899713.
Walzer, M. 2006. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 4th ed. New York: Basic Books.
Watson Institute. 2020. *Costs of War*. https://watson.brown.edu/costsofwar/costs/human/civilians/afghan

Jean-François Caron is an Associate Professor in the Department of Political Science and International Relations at Nazarbayev University and in the Institute of Political Science and Administration at the University of Opole. He is also a Senior Fellow at the Institute for Peace and Diplomacy located in Toronto, Canada.