Journal of Applied Philosophy

Journal of Applied Philosophy
doi: 10.1111/japp.12169

Cyberattacks as Casus Belli: A Sovereignty-Based Account

PATRICK TAYLOR SMITH

ABSTRACT *Since cyberattacks are nonphysical, standard theories of casus belli — which typically rely on the violent and forceful nature of military means — appear inapplicable. Yet, some theorists have argued that cyberattacks nonetheless can constitute just causes for war — generating a unilateral right to defensive military action — when they cause significant physical damage through the disruption of the target's computer systems. I show that this view suffers from a serious drawback: it is too permissive concerning the types of actions that generate casus belli since many essentially peaceful and non-violent mechanisms can nonetheless cause physical damage. I resolve this difficulty by developing a sovereignty-based account of casus belli and applying it to cyberwarfare. I argue that legitimate states have a constrained right to unilaterally respond with military force to unfriendly actions that bypass or overwhelm the political deliberations of the target state in order to force a change in behaviour contrary to the determinations of the people of the target state. This new account of casus belli avoids the problems of the consequence-based view by plausibly restricting the types of unfriendly action that give rise to casus belli and yet offers an attractive explanation for why some cyberattacks nonetheless do generate a potential right to a unilateral defensive response.*

Introduction[1]

Cyberwarfare appears to represent a significant challenge to our moral and legal understandings of just war.[2] My article will focus on the relationship between cyberwarfare and *jus ad bellum*. Both within the just war tradition and international law, there is one type of action that can potentially justify an immediate and unilateral military response: aggression,[3] which has long been understood as the use of physical or violent means to achieve a political objective. Yet, cyberattacks do not appear to use physical or violent means.[4] Cyberattacks, after all, only involve the manipulation of computer code. However, given the potential ability of cyberattacks to create widespread havoc and destruction, it seems implausible to suggest that no state can ever use military force to protect itself from them.[5] A theoretical consensus — henceforth the Standard View — has arisen in order to explain how cyberattacks can justify the appropriate military responses. These theorists have argued that the nonphysical or nonviolent nature of cyberattacks is irrelevant as long as they produce significant physical *effects*. So, causing serious damage, regardless of how it is caused, is sufficient on this view to at least potentially justify a violent response in self-defence.

I show that this consensus is mistaken and that the Standard View is unacceptably inflationary when justifying unilateral defensive action. The problem with the view is that there are many ways to create a physical effect besides cyberattacks and that describing all those mechanisms — such as trade embargos or diplomatic pressure — as potential casus

belli (which I take to be an action that generates a *prima facie* right to unilateral defensive action[6]) is both normatively implausible and potentially destabilising. In response, I present an alternative account of cyberattacks and casus belli that is based on the sovereignty of the target state that is in turn based on the rights to self-determination possessed by its citizenry. More specifically, I argue that some actions — those which we should understand as 'aggressive' that potentially justify unilateral military actions in defence — attempt to completely bypass or overwhelm the political deliberations of the target state and forcibly generate a particular political result. Other actions, which include trade embargos and political pressure, impose costs on the target state in order to motivate changes in behaviour. The former actions impose the will of the attacker upon the victim and simply avoid or ignore the political determinations of the target state while the latter actions work through those political determinations. The latter are unfriendly and often unjust but only the former constitute casus belli. My view has the significant advantage that it can explain why the most substantial and dangerous cyberattacks are casus belli while remaining relatively deflationary about the types of unfriendly state action that generate rights to unilateral military responses. I then present some implications of my view for cyberwarfare and respond to two major objections.

The Standard View

The nonphysical or nonviolent yet dangerous nature of cyberattacks has led to a fairly robust consensus that we need to reconceive the fundamental basis for evaluating when a state action represents a casus belli. Rather than focus on the violent *means* for achieving a particular political end, the new consensus argues that a 'casus belli' is one that produces particular kinds of effects.[7] Namely, the view is that a state is justified in using military force to defend itself unilaterally from attacks that produce significant death and destruction. Michael Schmitt writes:

> Armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury.[8]

Many have thus suggested something like a *consequences*-oriented view of 'armed attack' or 'aggression'.[9] The idea is that one can avoid questions about the physical or non-physical nature of computer programs by concentrating instead on the physical consequences of their deployment:

> Suppose Stuxnet [a computer worm aimed at Iran's nuclear program] is not a physical thing . . . the bare nonphysicality of the attack is not morally relevant. Imagine a hypothetical case of physical aggression that parallels Stuxnet as closely as possible: a commando raid on Iran's uranium enrichment facilities at Natanz that successful destroys several hundred uranium enrichment centrifuges . . . Such a raid clearly falls under *jus ad bellum* . . . there seem to be differences [between the raid and Stuxnet] . . . What seems most relevant in these two cases is not whether the means were physical but whether an action causes damage to a state's tangible assets.[10]

States may only respond to cyberattacks with military force when they, singly or in concert, intentionally and directly produce significant death and physical destruction.

For example, it does not matter whether patients die in a hospital because of a cruise missile or as a result of a virus shutting down life support machines; nor does it matter whether an airliner is shot down or brought down by an intentional disruption of its GPS system. The intentional effects of the action are what is relevant on the Standard View.

The Standard View does have some *prima facie* plausibility. Military responses are likely to be blunt, escalatory, and destructive. There should be a high bar for their deployment and the Standard View captures that by requiring that the military response be justified according to the serious consequences against which it purportedly defends. But more importantly, the Standard View offers a plausible story as to why certain relatively trivial cyberattacks do not constitute 'armed attacks' for the purposes of self-defence. This is a desirable feature: many cyberattacks have comparatively tiny effects while remaining indistinguishable from far more damaging attacks in terms of their violation of the target nation's cyberspace or the manipulation of the targeted state's computer systems. The same type of 'hack' can be used to shut down a website, steal corporate secrets, and cause traffic accidents, but it seems implausible to think that all such attacks should be subject to a military response. Rather than attempt to draw an arbitrary distinction based on the nature or type of the attacks, the Standard View argues that cyberattacks that produce insignificant physical effects are for that reason not casus belli. There are two types of cyberattack, in particular, that are quite common yet do not pass the Standard View's threshold: surveillance and corporate theft. First, many cyberattacks are intended for purposes that are more easily characterised as espionage. Namely, cyberattacks are often used to steal data or surveil the operation of communication nodes and other computer programs. Second, the private sector, especially in the United States and Western Europe, finds itself frequently and increasingly under cyberattack, either to steal economic secrets or to undermine their computer networks. While these attacks are expensive and frustrating, many doubt that they are casus belli. The Standard View explains this easily: cyberattacks that aim at economic and political espionage do not usually intend and produce the relevant effects and so do not generate a right to respond militarily for the targeted state. Attacks that manipulated computer code in essentially the same way but produced more serious effects nonetheless could generate the right.

Problems with the Standard View

Despite its strengths, the Standard View suffers from some major defects. The first set of problems revolve around the Standard View's account of the relevant consequences. By arguing that *only* death and physical destruction are relevant, the view implies that *territorial faits accomplis* and *overwhelming invasions* do not constitute casus belli. In the former case, a state will cross an international border and occupy the territory of another state before the other state can respond or resist. As a consequence, the invaded state then has the onus of initiating a military action to force the invading state out of its territory. Yet, in a territorial *fait accompli*, the invading state need not inflict any damage on the country it invades. So, the Standard View would suggest that the invaded country has no right to unilaterally respond in self-defence. This is implausible; there are other ways that an attack or invasion can undermine the legitimate interests of a polity beyond causing physical damage. Similarly, if a country were subject to overwhelming force and

thereby decided not to resist, advocates of the Standard View seem forced to conclude that the invaded country is not subject to armed attack. After all, if the invading country has managed to intimidate the subject nation to a sufficient extent that it need not inflict any death or physical destruction, then the necessary consequences would not obtain.

The Standard View may attempt to rescue itself by including violations of territorial sovereignty as another element of the 'consequences' that give rise to a right to unilateral defence. Perhaps this can be made to work, but I have my doubts. It is hard to see how even relatively trivial acts of espionage, economic cyberwarfare, or surveillance fail to violate the sovereignty of the targeted state in at least some minimal ways. Thus, the Standard View may need to give up its clearest advantage — its attractive manner of dealing with trivial violations of sovereignty that seem to fall short of casus belli — in order to accommodate the above counterexamples.

The second, and more important, difficulty with the Standard View is that it is implausibly inflationary when it comes to the types of political actions that give rise to a unilateral right to self-defence. The broad point is that if we argue that rights to self-defence are generated by a particular set of consequences, then the principled difference between economic pressure and cruise missiles — or between political manipulation and special forces — disappears. Consider three different hostile state actions.

> TORPEDO: The flagship of the target state's navy is severely damaged by a torpedo from a submarine, preventing it from being deployed in a territorial dispute.
>
> LOGIC BOMB: A computer operator under the employ and direction of a rival state hacks into the computer systems of the target state's flagship and subtly changes its navigation software. As a consequence, the ship is severely damaged as its runs into a shoal.
>
> EMBARGO: Upon being subject to an economic embargo from a rival state, the target state foreseeably reduces its budget for military preparedness. As a consequence, the engine of its flagship becomes damaged as a result of undermaintenance. The vessel cannot be put to sea during the ensuing dispute.

On a consequences-oriented view, it is hard to see what distinguishes these cases from each other, yet the first is clearly a casus belli, the third is typically thought to be a clear case of unfriendly action short of war, and the second seems like a clear case of an aggressive cyberattack. So, the consequences oriented view seems committed to the idea that EMBARGO is a casus belli, contrary to ordinary practice and international law. A reference to the *intended* consequences does not help. While embargos are not necessarily aimed — in an intentional fashion — at reducing military effectiveness, they clearly can be. And if one had sufficient knowledge of the internal political processes of the targeted country, one could foresee and intend that the economic consequences of the embargo would undermine its military effectiveness. Of course, it may be true that actions like TORPEDO are more likely to produce the relevant consequences than actions like EMBARGO, but that does not mean that particular embargos cannot be more certain in their destructive consequences than particular kinetic actions. In other words, there are many ways of producing effects but not all those mechanisms appear to be on equal footing when it comes to justifying a military response. Trade embargos[11] do not give rise to rights to engage in unilateral actions in self-defence even if the consequences of that embargo are equivalent in severity to that of a military assault. Yet, the

consequences-oriented Standard View would — in principle — suggest that many peaceful yet unfriendly actions are casus belli. After all, sanction, embargos, political pressure, and the like are designed to generate negative consequences within the targeted country. Or perhaps even more dramatically, consider the following case:

> RARE EARTH MINERALS: X and Y are engaged in a territorial dispute. X, either coincidentally or intentionally, has developed a monopoly on rare earth minerals that play an important constituent role in electronics. The Y government, fearing that this monopoly might be used to X's geopolitical advantage, funds a research project to create *ersatz* replacements for those minerals. The research program succeeds, causing large-scale economic dislocations in X when Y's demand for rare earth minerals plummets. As a further consequence, some citizens of X die, suffer injuries, and generally see their interests ill-served.

This is certainly an example of an unfriendly strategic action: Y is internally developing a capacity in order to undermine the relative geopolitical position of X. This unfriendly action causes death and destruction as economic dislocations so often do. So, assuming that the other conditions were satisfied, the Standard View seems to imply that the X government would be justified in using military force to stop the research. This would be a radically profligate departure from our current understanding as to when states are justified in unilaterally acting in self-defence. The Standard View, consequently, faces a dilemma: if it restricts its analysis to peaceful means in order to exclude RARE EARTH MINERALS and EMBARGO, then it will fail to apply to even quite serious cyberattacks, but expanding a consequences-oriented view to include cyberattacks will implausibly require the inclusion of RARE EARTH MINERALS and EMBARGO as potential just causes for war.

Proponents of the Standard View occasionally indicate that they are aware of the radical consequences of their view. The response they offer is that an attack must be an action that causes death and destruction in a particular sort of way. Namely, the action must *directly* produce death and destruction.[12] The argument must be, then, that EMBARGO and RARE EARTH MINERALS represent *indirect* causes of the relevant sorts of damage while TORPEDO and LOGIC BOMB represent direct ones.

There are two problems with this elaboration of the Standard View. First, the *moral*, as opposed to the psychological or legal, significance of directness is not clear. Obviously, actions that rely on relatively long causal chains often have less certain consequences than those predicated on short ones, but it is unclear why that should matter in principle. Similar things can be said about the length of time between cause and effect.[13] At any rate, it would certainly be unacceptable, even perverse, if a rival nation could avoid being held accountable for an attack simply by constructing a Rube Goldberg machine that undermined the proximity between cause and effect. Second, it is not obvious that any plausible account of directness divides the cases in the way the Standard View wishes. A logic bomb can lie dormant in a computer system for a long time before it activates. Similarly, a cyberattack that alters the navigation system of a ship or an airplane may require many steps and a fair amount of time before it is effective, but the motivation for adopting the Standard View is the intuition that a systematic series of cyberattacks aimed at the production of a concrete and physical consequence should count as an armed attack. Nonetheless, I will argue that the Standard View correctly identifies something

relevant about the fact that some actions use human judgment and agency to accomplish the effect and others do not. But I suggest that this feature should not be characterised in terms of causal directness.

The Sovereignty View

My rival account departs from the Standard View in two ways. First, rather than focusing on characterising a set of sufficiently serious consequences, my view is based on rights to self-determination held by individuals and, derivatively, collectives.[14] Sovereignty is constituted by a bundle of rights that states and their citizens possess that makes it possible to maintain a political community capable of self-determination. These include rights to territorial integrity, rights to determine policy within one's borders, rights to determine one's foreign policy, and rights to enter into relations with other states. Of course, each element of this bundle is qualified, and there is debate about whether some elements ought to be eliminated entirely from the bundle, but there seem to be two rights that are essential to collective, political self-determination. First, there is the right to political autonomy: individuals and their collectives have the right to deliberate upon and implement policies as they see fit. Second, political self-determination seems to require a right to territorial integrity. Without control over territory, it is difficult to implement the policies one has determined to be best. At any rate, I am going to assume that the fundamental self-determination rights for political collectives are political autonomy and territorial integrity: individuals organised into legitimate political collectives have a strong right to determine policy within their borders. An initial and crude pass at describing the Sovereignty View would be the following: casus belli are generated when one state violates the political autonomy or the territorial integrity of the target polity.

Two things are worth noting here. First, the collective right to self-determination is predicated on individual self-determination rights; so a violation of self-determination, in the end, is an imposition on individuals. Second, the rights we are interested in are those to *political* self-determination. It might be possible to undermine one's cultural or economic position in ways that do not undermine one's ability to engage — or engage adequately — in the political processes that determine policy. So, a cyberattack — such as distributed denial of service attack, which we will discuss in greater detail later — may undermine a private collective's ability to self-determine without necessarily violating any particular person's rights to engage in *political* self-determination, either singly or collectively. It is not the case that any infringement on any person's ability to self-determine in any sphere generates a casus belli. So, for example, a cyberattack on a Kiwanis club or a private university need not generate a casus belli if the attack cannot be understood as undermining the political self-determination of particular people either singly or in a group.

Yet, this does not narrow the scope of political self-determination nearly as much as one might think. The reason is that, while personal projects or the operations of private associations may not be relevantly political, the various political and legal entitlements that are often the basis of the pursuit of one's projects or the development of private associations are political in the relevant sense. After all, we work together to structure and mediate the pursuit of individual projects and the operations of private associations with a legal and political system that determine the bounds of possibility by creating

various requirements, powers, responsibilities, and privileges that come to at least partly constitute these projects and associations. As a consequence, it might very well be that a particular cyberattack does undermine those entitlements in the process of attacking an individual or private association and if *that* happens, then an attack on a particular association or individual may undermine the self-determination rights of the political community by attempting to rearrange, undermine, or violate the legal and political entitlements that we have collectively decided will be the policy within our borders. Consider the following case:

> UNION: Oceania wishes to gain an economic advantage over Eastasia. Rather than offer an inducement to Eastasia to change port policy, agents of Oceania covertly enter the stevedore union offices and change electoral results so that the candidate favourable to their interests is elected. Assume that the net economic effect on Eastasia negligible.

Do the actions of Oceania undermine the political self-determination of the citizens of Eastasia and not merely that of union members? It seems that the answer is clearly, 'Yes'. Unions are a legal construct and the people of Eastasia have collectively determined that unions have a particular legal structure, elect officers in particular ways (or have legally determined discretion concerning their leadership structure) and these determinations have economic and political consequences that Oceania is attempting to undo. As a consequence, Eastasia can — assuming it meets the relevant conditions, whatever our substantive theory of legitimacy happens to be, of domestic self-determination — use political violence to enforce those determinations and protect those entitlements within its territory. Of course, it is unlikely that the actions of Oceania would justify an invasion by Eastasia but that is true of many casus belli.[15]So, while an attack on a private association — such as the Kiwanis Club or stevedore union — may not generate a casus belli, if those attacks undermine the relevant political entitlements, then those attacks may very well justify the unilateral use of military force in self-defence.

The Sovereignty View suggests that any action that violates the self-determination rights of the political community gives rise to a casus belli. Yet, I have already alluded to a potential problem with this formulation: many trivial and intuitively peaceful cyberattacks appear to violate the sovereignty of the target state. We are understandably reluctant to say that *any* action that constrains, restricts, or imposes costs on the agency of a state represents a potential casus belli. Fortunately, not all constraints on the political autonomy of a political community are equal. The key difference, I submit, is whether the unfriendly strategic action aims to achieve its political objective *through* or *in spite of* the deliberations of the target state. Some unfriendly actions impose costs on the target state with the hope that the state will change its policy; other actions attempt to *force* a change in policy despite resistance. UNION represents a good illustration of the distinction. Oceania is not presenting a set of sanctions or incentives and hoping that Eastasia decides to adopt a favourable port policy; they are covertly bypassing whatever deliberative procedures Eastasia has in place in order to ensure — against the will of the people of Eastasia — that a particular set of policies are ultimately enacted. In what follows, I argue that only the latter — impositions of will — generate qualified rights to a unilateral military response. I will then apply the distinction to the case of cyberwarfare.

It is important to emphasise this point.[16] My account has two important elements. First, my view of sovereignty and political self-determination is such that it is partly

constituted by the specific legal and political entitlements of members of the political community. This restricts what counts as a potential casus belli: the cyberattack must be aimed at a relevantly political interest that is part of the self-determination of the target community. Of course, one might disagree which interests are relevantly political — perhaps a corporate theft via break-in by agents of North Korea is not an act of war — but still agree that casus belli are generated by the need to protect relevantly political interests. However, not every action that *affects* or *burdens* these interests is thereby a casus belli. After all, embargos and economic competition do that. The second component of my view is that the *structure* of the cyberattack matters for its status as casus belli: only impositions of *will* are casus belli. Actions that merely impose costs on a community's political autonomy may be unjust — and may demand remedial, preventative, or rectificatory action — but they do not just unilateral military force in response. So, a cyberattack is a casus belli when it is an imposition of will upon a community in order to generate a specific, politically relevant result.

The idea that warfare is distinct in that it aims for the imposition of one's will upon the enemy has a long pedigree. The Standard View rejects Clausewitz's famous aphorism that war is defined by its means.[17] I would argue that a 'means' based understanding on war is only part of the Clausewitzian story. He clearly thinks that the war always aims at a political end and that political judgments ought to direct the employment of military force. Yet, Clausewitz also argues that war itself has an internal logic that, if not carefully controlled, can break free of its political bonds. He writes:

> *War is thus an act of force to compel our enemy to do our will* . . . Force — that is, physical force, for moral force has no existence save as expressed in the state and the law — is thus the *means* of war; to impose our will on the enemy is its *object*. To secure that object we must render our enemy powerless; and that, in theory, is the true aim of warfare.[18]

This logic, however, drives Clausewitz's analysis of effective war-fighting. The aim of warfare *qua* warfare is to 'disarm' the enemy. This allows you to impose your will on the enemy and decisively facilitates the achievement of your political goals. The aim of war-fighting is to put yourself in a position where the enemy is incapable of resisting your attempt to achieve a particular objective. This is different, though obviously akin, to what is usually called a 'coercive' strategy whereby I attempt to induce a change in behaviour by imposing a cost for noncompliance (or providing an incentive for compliance). To see the difference, consider the classic highwayman who says, 'Your money or your life'. Despite the surface grammar of the utterance, the highwayman is not really offering the choice he appears to be.[19] After all, if you refuse to hand over the money, the highwayman will simply kill you and take it anyway. When it comes to your money, the highwayman has forcefully imposed his will upon you: your consent is irrelevant. Of course, you might induce the highwayman not to kill you by being compliant but that hardly changes the fact that he is getting your money regardless of what you do. In comparison, imagine a person that imposes an unfair cost upon you:

> GASOLINE: There is a hurricane approaching and you need gas for your generator. You approach the last gas station in town and discover that prices have increased ten times. The only way to get the gas is to pay the exorbitant, price-gouging amount.

In GASOLINE, the owner of the gas station is imposing a *cost* but she is not imposing her *will* upon you. She is offering a choice: you must pay this amount if you are to achieve what you want. But, should you decide that the cost of the gasoline is so high that you'd rather suffer through the storm without power, the gas station attendant will not take your money out of your wallet. The attendant is making you pay a cost, perhaps an unfairly high one, but you are choosing whether to pay it. There is a difference in the relationship between what the highwayman or the gas station attendant wish to achieve and your will: the former achieves what he wants regardless of your will, but the latter works through your will.[20]

It is important to see that I am *not* saying that what the attendant does is permissible and what the highwayman does is not. It seems clear that sometimes people who act as the gas station attendant does wrong their victims, that GASOLINE could describe an act of coercion, and that a possible remedy of that wrong could be collective political action. But what I do think is plausible is that the imposition of will represents a qualitatively different kind of assault upon another person when compared to the imposition of costs. The latter still treats you as an agent. In fact, it is essential to the strategy that the target can understand the costs for actions, judge whether it is worthwhile, and then act on that judgment. The former actions treat the target fundamentally as an object whose agency or judgment is irrelevant. Will imposition represents a particularly egregious violation of an agent's rights to self-determination and this drives the difference in defensive response. That is, I can respond to impositions of will with force without going through normal mechanisms of political adjudication, but the same cannot be generally said of impositions of cost.

In response, one might be tempted to think that impositions of will only appear more egregious because they tend to operate against more important interests than impositions of costs and that is why we are more likely to think forceful defensive action might be justified.[21] I am sceptical. Imagine:

> TRIVIAL HIGHWAYMAN: You are walking along the road, carrying a trinket you just won at a carnival. A person approaches you and demands that you turn the trinket over to him. You refuse and the person grabs at the trinket. You respond by pulling the item away and punching your assailant in the nose. The thief flees.

The trinket might be of considerably less value than any of the relevant interests that might be ill-served by the actions of the attendant in GASOLINE. Consider: if the lack of gasoline merely causes your food to spoil, you have lost more money by a wide margin than the value of the trinket. Yet, *unilateral* defensive action is more justified in TRIVIAL HIGHWAYMAN than GASOLINE. The reason, it seems to me, is that impositions of will represent a fundamental attack on the agency of the targeted person. A person you unfairly impose costs on might be a person you do not treat as you ought or as an equal, but imposing your will on someone is a way of saying they are not even really a person at all.

Can the imposition of a cost transition or transform into an imposition of will? Or to put it in terms of GASOLINE, can your need for gasoline be such that charging such high prices *amounts* to an imposition of will? I believe that it can, but whether it does so is not simply a matter of how significant the costs are. Rather, the key element is whether the costs are structured so that they go beyond an inducement to compliance and

undermine the very possibility of making a choice to comply at all. Consider Scott Anderson's account of coercion, which depends on the following notion of enforceability: 'where the sense of enforceability here is exemplified by the use of force, violence and the threats thereof to constrain, disable, harm or undermine an agent's ability to act'.[22] The imposition of costs can become an imposition of will when the costs are sufficiently well-targeted and severe as to undermine the ability of the target state or agent to determine, distribute, and direct the burdens imposed by the hostile action. This is not merely or simply a matter of making people poorer or worse-off, but rather concerns the undermining of the social, political, and economic institutions that make it possible for citizens of the targeted state to discuss and decide how to respond to the imposed costs. The equivalent in the interpersonal case would be if a pharmacist insisted on price-gouging for anti-psychotics in a crisis: being unable to take those drugs is not simply an imposition of a cost but rather undermines — over time — the ability of the person subject to the imposition to judge the costs and act upon those judgments. If the imposition of costs presents that sort of threat to the agency of the targeted agent, then it becomes the kind of attack that justifies a more forceful response.

So, we now have the outlines of the Sovereignty View. An unfriendly strategic action generates a unilateral right to use military force in self-defence under two distinct circumstances. First, the unfriendly state may impose a set of costs that are sufficiently burdensome or sufficiently well-targeted that they undermine the very ability of the targeted state to engage in *political* self-determination. Second, the unfriendly state may impose its will upon the targeted political community. This second casus belli has two features: it must be disposed to overwhelm, bypass, or override resistance by the target state in order to achieve a particular objective and that objective must be of a relevantly political character. The latter requirement is important: it indicates that the imposition of will is relevant when it is meant to undermine, change, or violate political and legal entitlements that are the outcomes of the political deliberations that constitute collective political self-determination even when those entitlements are — in terms of overall material consequences — fairly minor. We can now turn to cyberwarfare.

If I am right about the distinction between the imposition of a will and the imposition of a cost, then we can distinguish some cyberattacks from economic coercion. Proponents of the Standard View are correct to want to draw a distinction between RARE EARTH MINERALS/EMBARGO and TORPEDO/LOGIC BOMB. They are not correct in thinking that this distinction can be drawn with reference to causal directness or immediacy of the causal connection between the action by the targeting state and the effect in the targeted state. Rather, the key difference is in the nature of the contributory factors that mediate between the formation of the intention in the attacking or intervening state and the production of the relevant geopolitical consequence. Whether the causal chain involves the informed agency of members of the target state or not determines whether it's the will of the attacker or costs that are imposed. In RARE EARTH MINERALS and EMBARGO, the hostile state imposes a set of costs on the subject state. The subject state then decides, through its own policies, how those costs will be distributed amongst the population. It is this mediation of the political and economic decisions of the targeted state between the imposition of the cost and the effect that makes RARE EARTH and EMBARGO different from LOGIC BOMB and TORPEDO.

LOGIC BOMB might be considered the tricky case, since it is a human decision that results in the ship being run aground. There are two reasons to think that LOGIC

BOMB is closer to TORPEDO. First, in LOGIC BOMB, it is not the case that the judgment about what ought to be done in light of the imposed costs plays a role in the captain's decision to take that particular route. Rather, it is the *false belief* that has been engendered by the logic bomb that the route is safe that leads to the captain's decision. The agent's judgment in this case is bypassed and their view about what should be done is made irrelevant by the fraudulent program. We could imagine a case where a captain decided to take a more dangerous yet less fuel-expensive route in order to save resources that would be much closer to EMBARGO than TORPEDO, but that is not what is happening in LOGIC BOMB. In the latter case, the will and judgment of the captain are being made irrelevant: the hacker will do whatever it takes to get the ship to run aground. Second, I would argue that the imposition of will implies the irrelevance or overcoming of resistance. Again, in the original highwayman, refusing to comply is irrelevant to what actually happens. In LOGIC BOMB, the hacker overcomes resistance and acts to produce the desired effect regardless of what the targeted state wishes to accomplish. To put it another way, TORPEDO and LOGIC BOMB focus on accomplishing a geopolitical objective in the face of persistent non-compliance, while RARE EARTH MINERALS and EMBARGO are attempts to induce compliance. Of course, an attack can fail to overcome effective resistance, but acting to achieve one's ends in the face of the resistance does seem like a good indicator that one is attempting to impose one's will.

One consequence of this distinction is that hostile actions that give way immediately in the face of any token resistance are not impositions of will. The typical historical example of this kind of behaviour is represented by 'probing'. During the Cold War, the United States often violated Soviet airspace in order to test Soviet responses. Today, China routinely sends vessels into disputed territorial waters and withdraws when faced with resistance by the target state's navy. In *Nicaragua*,[23] the ICJ ruled that such minor border incursions do not constitute a casus belli. My view can accommodate this: if I withdraw the moment I am faced with any resistance whatsoever, then it is implausible that I am attempting to impose my will. Rather, I am imposing a cost on the targeted nation: by requiring them to respond frequently, the targeted nation will need to expend money and resources to order to maintain its resistance. This sort of probing, then, does not represent a casus belli and fails to generate a unilateral right to defensive military action. The reverse seems also to be true. If an incursion that retreats immediately even in the face of token resistance is *not* an imposition of will, then the failure to offer even token resistance undermines to some extent the claim that one's will is being imposed upon. After all, how would we be able to distinguish between an imposition of will and a judgment that the imposed costs are not worth paying if some minimal threshold of resistance is not met? But there are two reasons or caveats that explain why this is not an onerous or implausible requirement. First, the failure to resist only creates a defeasible presumption against imposition. A failure to resist that was reasonably motivated by a judgment that resistance was pointless or excessively dangerous would not undermine the claim that one's will was being imposed upon. Second, what constitutes resistance is contextual. For example, in the context of a legal system that possessed effective enforcement power, claiming a legal right to a thing could very well constitute 'resistance' to it being taken. Similarly, placing a good inside your home, where there is an effective legal right against trespassing, would count as the minimal level of resistance. But it is unlikely that simply claiming a territory, given the lack of an effective enforcement mechanism in international law, would constitute the minimal level of resistance.

Not surprisingly given the self-help nature of the system, effective control, and thus the possibility of resistance, has long been a necessary condition to rightfully claiming a territory.[24]

To sum up, there is a distinction between imposing one's will and imposing costs. The former generate claims to engage in unilateral self-defence while the latter do not. We can use this distinction to show why actions like TORPEDO and LOGIC BOMB are armed attacks while RARE EARTH and EMBARGO are not. In the former case, the attacking state is attempting to impose its will upon the targeted state, bypassing their sovereignty and the agency of its citizenry. In the latter, the hostile state is imposing a cost while ultimately operating through the agency and judgment of the targeted state. LOGIC BOMB is an imposition of will because it operates by fraudulently inculcating a damaging belief in the face of resistance. In the next section, I describe some practical implications of the imposition of will view.

Practical Implications of Cyber Warfare

I would like to focus on three implications of my view. First, it looks like surveillance and data skimming will not *normally* be casus belli. Generally speaking, these actions do not involve overcoming resistance; rather, they exploit gaps in the system and withdraw when faced with resistance. Furthermore, even penetrative espionage exploits do not involve the attempt to impose a particular policy result. That is, they normally involve the theft of data rather than its destruction or alteration.[25] Second, and more importantly, distributed denial of service attacks would not count as impositions of will and, thereby, would not generate a right to unilateral military action. DDoS attacks do not involve any kind of penetration into the network. Rather, cyberattackers performing a DDoS take over many computers ('botnets') and use these computers to request information from a network at a much greater rate than usual and at a greater rate than the network can process. As a consequence, use of the network is compromised because its resources are expended responding to spurious requests for information. This is little different from border 'probing' that is used to impose costs in virtue of their response, and like border probes, DDoS does not involve the penetration of a network in the face of resistance. As a consequence, DDoSs are unfriendly, but they are not attacks unless DDoSs are so effective at undermining the capabilities of the targeted networks that the ability of the targeted state to make policy decisions and engage in any resistance at all is compromised. The relatively low status of DDoSs is not surprising, given that they are the most common cyberattack but among the most easily dealt with.[26] It should be noted, however, that DDoS attacks that fundamentally undermined the ability of the target's state political and social institutions to deliberate and respond to these cost impositions could become casus belli.

Most controversially, my view implies that any cyberattack that results in cyberharm through a penetration of the network in the face of resistance is an armed attack as long as some individual has the relevant legal and political entitlement to the effective functioning of the computer system. Cyberharm can be defined as:

> [Cyberharm] is intentional harm by an agent, *via* an infomatics network such as the Internet, in which the functioning of a system (a person, a machine, software, or an economy) is in some way impaired or degraded.[27]

The broad point is this. Any action performed by or attributable to state agents that penetrates a network that has made the minimal efforts to resist the intrusion and causes the network to malfunction is an armed attack upon the state where the system resides as long as it has been determined by the political community that some person or group of person's have rights to non-disruption of their system.

Let's consider some examples, both real and hypothetical. This view implies that the deployment of Stuxnet against Iran by Israel and the United States could potentially have justified a military response. Stuxnet was a computer virus that was designed to penetrate Iranian computer networks — especially Siemens systems that controlled industrial processes — and alter certain programs so that the centrifuges necessary for the production of fissile nuclear materials would be damaged. As long as Iran engaged in minimal efforts to prevent this kind of intrusion, then the hostile states bypassed Iranian deliberations and judgments to impose a particular outcome upon them, resulting in physical damage. Similarly, LOGIC BOMB[28] represents an armed attack on this account. The logic bomb penetrates the network and causes the system to malfunction in a way that is designed to produce a political objective. Again, as long as the system was designed to resist this intrusion, then this amounts to an imposition of will upon the targeted state. Furthermore, it seems like this is true regardless of whether the network is private or public. One reason for this is that, at least in the United States, the distinction between private and public cyber infrastructure and networks is ambiguous, porous, and often nonexistent.[29] The more important reason is that the imposition of will on persons or private agencies appears to be a violation of sovereignty just as much as an attack on public infrastructure or government operations. An Iranian commando assault on Stanford University is just as much an act of war as an assault on a military base. So, similarly, if a state's cyber command were to break into private networks of the United States banks to alter or destroy financial records, then that action would be an armed attack generating a *prima facie* right to respond militarily. The cyberattack represents an attempt to impose a particular network configuration upon the targeted state, replacing and ignoring the agency of those subject to the attack.

Objections

There are two significant objections I would like to address. First, we might worry that the distinction between imposition of will and imposition of costs does not map well on the distinction between unfriendly state actions and casus belli. Specifically, since the development of airpower and strategic bombing, military power has increasingly been used to impose costs on other countries in order to induce compliance. Robert Pape,[30] for example, argues that strategic bombing in particular can serve a counter*force* or a counter*value* function. In the former, the strategic bombing undermines the target state's capacity to resist in order to serve the end of disarming and occupying the target state (e.g. the attempt by American strategic bombing forces in Europe to destroy the German armaments industry would be a counterforce strategy). Countervalue strategies, by contrast, bomb targets that have high value to the people of the target state with the hope they will decide that the war will be too costly and comply with the political demands of the attacking country (e.g. Operation Rolling Thunder in the late 1960s was an explicit

attempt to cause so much damage to North Vietnam via aerial bombardment that the government in Hanoi would accept peace terms favourable to the United States and the Republic of Vietnam).

Here is the point of the distinction. For much of human history, the only way to militarily achieve one's goals was to impose one's will directly on the target political collective. However, the development of airpower and precision weaponry allows one to compel another state's compliance simply by imposing costs upon them without obeying the Clausewitzian dictate to disarm them. I do not deny the distinction though we should be sceptical that countervalue strategies reliably succeed in inducing compliance. Rather, I think the claim that a countervalue strategy does not represent an imposition of will takes the 'state as person' metaphor much too literally. It is true that if we think of the target state as being the agent that is being imposed upon, we might think that a countervalue strategy is simply the imposition of a cost. But the agents who have moral standing, and are subject to the imposition of the will by the attacking agents, are the citizens of the targeted country. Countervalue bombing is a straightforward physical attack on them even if their own state could conceptualise their deaths as part of the costs of engaging in particular policy. Countervalue strategies may, of course be just or unjust; it depends on whether they satisfy the normal conditions of discrimination, proportionality, and necessity. But either way, they do not thereby fail to be physical attacks (and therefore impositions of will) on people simply because they represent an attempt to impose a cost on a *state*. This is why, for example, blockades, ship seizures, and the mining of harbours ought to be considered impositions of will even though the usual purpose of these actions is to undermine the economy of the target state. In other words, we should not confuse the *mechanism of target state compliance* with the coercive dynamics of the tools used to generate that the mechanism. This objection illustrates the importance of focusing our attention on the rights and entitlements held by *individuals* in the course of political self-determination. The physical attack represents an imposition upon particular individuals in violation of their relevantly political and legal entitlements as determined by a legitimate political community.

The second objection is more serious. My view seems profligate with the unilateral right to self-defence. In fact, it appears to be worse on this front than the Standard View because it grants a unilateral right to self-defence in cases where the consequences are relatively trivial! While the Standard View might be over-permissive, at least it only granted the right to self-defence in cases where the consequences were serious. The Sony Pictures Entertainment hacks[31] represent a significant real-world test case. Obviously, no one ought to suggest that the United States go to war to deter North Korea from hacking into Sony Pictures email accounts and then publicising them. Yet on my view, so the objection goes, North Korea's actions represent a casus belli if we assume that the hacks were deliberate policy by the DPRK. Those hacks represent impositions of will upon Sony Pictures; they bypassed resistance in order to produce a result that was contrary to the deliberative determinations of Sony Pictures.

However, my view focuses on the self-determination of the relevant political community and not corporations, so it does not necessarily follow that these hacks generate a casus belli. It will depend on the details of the case. If the DPRK were merely *surveilling* Sony Pictures by collecting information, then this would not represent a casus belli because the DPRK would not be attempting to impose a political result on an agent. What's more, if the DPRK were imposing costs on Sony such that Sony would not

release *The Interview*, then we would still not have a casus belli. There would be a political objective but only the imposition of cost. Yet, let us suppose that this is not what the hackers did. Let us suppose that these hackers violated specific legal and political entitlements that we have determined — collectively as a legitimate political community — that Sony, its shareholders, or its officers ought to have. These entitlements are the result of the political actions of the people of the United States as done by their elected and appointed officials at various levels. So, the distribution of property entitlements and rights to privacy is a political action; actions that impose a will in a way that restructures or violates those entitlements are an imposition upon the political community as well as the particular rights-holder. What's more, North Korea engaged in this violation in order to produce a specific result favourable to its interests. So, the operation against Sony Picture is essentially equivalent to that of UNION. In both cases, a state engages in an unfriendly strategic interaction that violates the particular legal and political rights of a private association and the association members in order to produce a, relatively minor, consequence favourable to their interests. Of course, compared to the violation of the entitlement to one's life that strategic bombing represents, the violation of the rights in the Sony hacking case are minimal. But that does not change the underlying nature of the North Korean action as a violation of the right to self-determination as held by the American people, just as the relatively minor violation of rights in UNION does not change the underlying status of the action. So, it does look like the Sony Pictures hack satisfies the two independent conditions of my view: it is an imposition of will by a foreign power — it bypasses resistance and compels an intended result — and that imposition represents a violation of the political community's rights to self-determination. As a result, it does look like the North Korean action generates a casus belli while the Standard View does not.

I concede that this objection characterises the relative permissiveness of the two views accurately. Yet, I submit that the objection that my view is inflationary is not decisive. There are three ways a view can be inflationary. First, a view might be type-inflationary. That is, compared to other views, a type-inflationary view has the implication that additional *types* of action potentially generate casus belli. The Standard View is *type* inflationary: embargos and other kinds of economic competition — which have typically been understood as peaceful — are casus belli. Second, a view can be quantitatively inflationary about *just causes* in particular: contingent features of the world make it such that there are many more casus belli according to one view rather than another. Finally, a view might be inflationary about *justified instances of military action*. It is important to see that a view can be inflationary about casus belli without thereby being inflationary about actually justified instances of self-defence. Military action must be proportional and necessary as well as being a response to a just cause. So, a view could be inflationary about just causes but non-inflationary about justified uses of military power if those just causes were very likely to fail the requirements of proportionality or necessity. So, my response is that my view is inflationary in the relatively benign second sense (my view generates many just causes in our world) while the Standard view is inflationary in the much more problematic first and third senses.

The key point is that those actions that seem to be the most problematic counterexamples for my view — the trivial cyberattacks — are precisely the actions that will not be able to satisfy the additional conditions that need to be met in order for a military response to be justified. There are two reasons for this. First, their very triviality works

against them. If the cyberattacks produce insignificant consequences, then the military response will produce comparatively tiny benefits even if it successfully punishes the current attack and deters future ones. And if the benefits are small, as they surely must be, then the costs of almost any military attack upon the hostile state will be disproportionately high when compared to them. As a result, trivial cyberattacks will only justify military attacks — if they can justify them at all — in those exceedingly rare cases where those military attacks stop the cyberattacks yet cause very little damage otherwise. This does not strike me as an implausible result; I see no reason why we should think that the United States should refrain from a *proportionate* and necessary military response to stop a cyberattack on a private agent. Yet, even if one were unconvinced by the proportionality considerations, the necessity and last resort conditions would not easily be met in the case of trivial cyberattacks. After all, expending resources on cybersecurity in order to prevent those sorts of intrusions will be more effective and less costly than any military attack. Why attack the headquarters of Chinese Cyber Command if you can create more effective firewalls? In other words, my view is 'overly' generous in granting 'casus belli' status to those actions that will fail to satisfy the other criteria for a justified military response. And this is no accident; the features of the cyberattack that motivate the claim that my view is being too profligate are the very features that make the actions less likely to satisfy those other conditions.

The same cannot be said for the Standard View. The profligacy of the Standard View is far more dangerous, and the danger is essential to the view. The Standard View, understood properly, demands that economic and political coercion and pressure be included as casus belli if they lead to significant, kinetic consequences. Yet, the very severity of the consequences will more likely justify military responses since they are more likely to satisfy the proportionality requirement. And since economic coercion can only be internally adapted to with difficulty and is often damaging even to the imposer, it is likely that military responses could satisfy the necessity and last resort conditions as well. Somewhat ironically, then, the focus on severe consequences makes it more likely that serious conflicts will occur when compared my view and not less. So, my view might be inflationary in the sense that trivial impositions of will generate casus belli (though, my view is strongly deflationary when it comes to DDoSs or impositions of cost, which will only very rarely and only under extreme circumstances generate a casus belli), my view will not be inflationary when it comes to *actual military operations* being justified. The Standard View, by contrast, will be inflationary when it comes to justifying actual military operations. And since it is military operations — and not casus belli judgments — that affect the interests of particular people, the inflation of the Standard View is much more problematic than mine.

There is another way in which my view is less inflationary. The Sovereignty View is applying a particular category — impositions of will — that I take to be a motivating logic of how aggression relates to sovereignty and self-determination. It may very well be true that when this logic is faced with a radically new situation, it is has inflationary implications. But these are implications concerning an unsettled class of cases. The Standard View, by contrast, is inflationary concerning settled classes of strategic action, which is why I emphasised that the Standard View is much more inflationary concerning *types* of strategic action. That is, there is a long-established consensus that cases like EMBARGO and RARE EARTH MINERALS do not constitute casus belli and it is this consensus that the Standard View is committed to rejecting. In other

words, my theory presents a set of fairly radical implications for a new and radically different context while the Standard View presents a conservative set of implications for the new context of cyberwarfare at the cost of radically rejecting our judgments about already considered and settled cases. I think this is a significant epistemic advantage for my view.

It is important to see that the Sovereignty View is not quite as inflationary as we might think and does not reduce all judgments about the justifiability of military operations to considerations of proportionality.[32] The most important initial judgment concerns whether a particular cyberattack is an imposition of will or an imposition of costs. And this is not trivial thing, either epistemically or in terms of actual practice, because the most common form of cyberattack is (DDoS) is not an imposition of will. What's more, we will need to make determinations of how the attack relates to the possibility of resistance and the attack's relationship to target state's deliberations. Next, we will need to determine whether the imposition of will operates against specifically political self-determinations. If the attack meets both of those criteria, then we can ask the question of whether there is a necessary and proportional means that may deter or stop the attack. And like in the case of UNION, I see no reason — in principle — to refrain from the use of those proportional means in order to protect our rights — collectively and individually — to political self-determination.

Patrick Taylor Smith, Department of Political Science and Global Studies Programme, National University Singapore, AS1, #04-10, 11 Arts Link, Singapore, 117570. polspt@nus.edu.sg

NOTES

1 This article was inspired by Elaine Korzak's presentation of 'Computer Network Attacks and International Law' at the Center for International Security and Cooperation Working Papers Group on 10 October 2013. Her presentation was part of the Social Science and International Security Seminar Series in the Center for International Security and Cooperation. I would like to thank the members of the Stanford University's Center for Ethics for their helpful comments, especially those of Mark Budolfson and Brian Berkey. I would also like to thank both Oxford University and the NATO Cooperative Cyber Defence Center of Excellence for an opportunity to present this paper. Finally, I would also like to thank two sets of two anonymous referees for their helpful comments.

2 Randall Dipert 'The ethics of cyberwarfare', *The Journal of Military Ethics* 9,4 (2010); 384–410 and Patrick Lin, Fritz Allhof & Neil Rowe 'Is it possible to wage a just cyber war?' *The Atlantic* 5 June 2012, available at: <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/. Both argue that the just tradition, as represented in its highest expression by Michael Walzer, *Just and Unjust Wars* (New York: Basic Books, 2006), will need to be fundamentally revised to accommodate cyberwarfare. Generally, these revisions suggest that the *nonphysicality* and the *speed* of these attacks justify revision. In this article, I will only be focusing on how the former feature ought to be captured by the notion of aggression. I will not be discussing whether the speed and difficulties of attribution justify a wider and more proactive understanding of preemptive war or whether cyberattacks, because they cause less damage, might just preemption in penumbral cases.

3 See Brian Orend, *The Morality of War* (Peterborough: Broadview Press, 2006, pp. 32, emphasis in original): 'But international law, and just war theory, insist that, rough as it may be, [a trade embargo] is not severe enough to merit warfare as a response. It is only when the tough treatment in question is *coupled with physical violence* that we begin to contemplate armed conflict.'

4 There is certainly a sense in which cyberattacks supervene on physical states and are thereby physical in some sense. After all, altering code will require deploying energy to alter physical states of another computer. But the energy release and physical change is *de minimis* (after all, there is both energy release and physical change that is concomitant with flashing a searchlight across a border, but no one would say that that action

violates the target nation's sovereignty). Rather, the energy release and physical change are only relevant insofar as they restructure the code in *relevant* ways. In the end, little in this article or in the dispute between my view and the Standard View depends on the non-physical nature of cyberattacks; we all agree that the relevant just war categories should be applied to cyber and military attacks alike. Rather, the mediated, indirect, and *de minimus* physicality of cyberattacks combined with their potentially serious effects force us to confront questions about the nature of aggression in just war theory. I thank an anonymous referee for forcing me to be clearer on this point.

5 The Department of Defence (http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf), for example, has suggested that military force is justified in response to 'significant' cyberattacks. For a more thorough discussion of the dangers of cyberattacks, see Michael Schmitt, *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (NATO Cooperative Cyber Defence Center for Excellence; Cambridge: Cambridge University Press, 2013).

6 It is important to note that I am only discussing when an unfriendly action by a state can *potentially* justify unilateral military action (i.e. when it is a casus belli). It is a separate and further question whether the target state can appropriately act all things considered in light of the requirements of necessity and proportionality.

7 I am changing the terminology of the consensus somewhat. Most theorists use 'armed attack' rather than 'casus belli' because the former is the terminology of Article 51 of the United Nations Charter (59 Stat. 1031; TS 993; 3 Bevans 1153). I use the latter term because I wish, at least initially, to keep the 'deeper morality' and the legality of cyberwarfare separate. See p. 732 in Jeff McMahan, 'The ethics of killing in war' *Ethics* 114 (2004): 693–733 for a more detailed description of the distinction.

8 See Michael Schmitt, 'Computer network attack and the use of force in international law: Thoughts on a normative framework', *Columbia Journal of Transnational Law* 37 (1999): 885–937, at p. 913; and this account is substantially reproduced in the *Tallinn Manuel on the International Law Applicable to Cyber Warfare* (2013).

9 See James Cook, ' "Cyberation" and just war doctrine: A response to Dipert', *The Journal of Military Ethics* 9,4 (2010): 411–423; Marco Roscini, 'World wide warfare — "jus ad bellum" and the use of cyber force', *Max Planck Yearbook of United Nations Law* 14 (2010): 85–130; Daniel Silver, 'Computer network attack as a use of force under Article 2(4) of the United Nations Charter', *International Law Studies* 76 (2002): 73–97; Ian Brownlie, *International Law and the Use of Force by States* (Oxford: Oxford University Press, 1963); Leonard Kahn, 'Just war theory and cyber-attacks' in F. Alhoff, N. Evans & A. Henschke (eds) *Not Just Wars* (London: Routledge 2013); Schmitt op cit.; Lin, Allhof & Rowe op. cit.; and Christopher Eberle, 'Just war and cyberwar', *The Journal of Military Ethics* 12,1 (2013): 54–67. Dipert op. cit. makes sceptical noises though he seems to adopt the Standard View in the end. Other sceptics include Jason Barkham, 'Information warfare and international law on the use of force', *New York University International Law and Politics* 34, (2001): 57–113; and Matthew Hoisington, 'Cyberwarfare and the use of force giving rise to the right of self-defence', *Boston College International and Comparative Law Review*, 32,2 (2009): 439–454.

10 See Ryan Jenkins, 'Is Stuxnet physical? Does it matter?' *The Journal of Military Ethics*, 12,1 (2013): 68–79.

11 It should be noted that embargos are quite different from *blockades*. If the United State refuses to sell a country scrap iron or oil, then that is an embargo. If the United States sends its navy to use force to prevent any other nation from entering the targeted state, the force it uses on the merchant marine of the targeted state and others is surely aggression. Blockades are acts of war; embargos are not.

12 Schmitt (op. cit., p. 913) refers to the 'direct results caused', and Silver (op. cit., pp. 92–93) states that what matters is whether the death and destruction was a 'direct and foreseeable consequence' of the action. The Talinn Manual includes both *directness* (i.e. the greater or lesser extent of attenuation in the causal chain) and *immediacy* (e.g. the sooner the effect manifests) as its criteria for assessing the relationship between from cyber-cause and physical effect.

13 A paradigm example of this point would be Stuxnet, which achieved its goal relatively slowly and through an comparatively elaborate series of steps. Yet, if we grant that these steps made the successful production of the intended results *more certain*, it is implausible to suggest that immediacy and directness are independently relevant for determining whether Stuxnet is an armed attack.

14 I do not purport to offer a full defence or account of political self-determination, but it is widely accepted that, at least, legitimate political collectivities have constrained rights to direct their own affairs that ought to be respected. For more robust discussions, see Andrew Altman & Christopher Wellman, *A Liberal Theory of International Justice* (Oxford: Oxford University Press, 2009), chapter 2; John Rawls, *A Law of Peoples* (Cambridge, MA: Harvard University Press, 1999); and Michael Walzer 'The rights of political communities' in C. Beitz (ed.) *International Ethics* (Princeton, NJ: Princeton University Press, 1985).

15 It is because of cases like UNION that I reject the following, *prima facie* plausible, revision to the view: self-determination rights protect socially basic interests — such as the right to life — and only cyberattacks that undermine *those* interests represent violations of sovereignty. I understand the appeal of the view, but I would suggest that socially basic (or fundamental) interests ought to play a different role in a theory of self-determination. Rather, they set the conditions as to when a political *community* has self-determination rights against external interference. Yet, once the community is relevantly self-determining, violations of those collective rights cannot be excused or justified simply because they directly affect interests that are less urgent than socially basic human rights.

16 I was helpfully asked to clarify the distinction between these elements of my view by an anonymous reviewer.

17 See Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1976), p. 87: 'We see, therefore, that war is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means. What remains peculiar to war is simply the peculiar nature of its means.'

18 Clausewitz op. cit., p. 75.

19 The implausibility that the highwayman is really offering a choice is the basis for a well-known joke of Bob Hope's, who was famously cheap. The highwayman says, 'Your money or your life', and after a long pause, the highwayman says, 'Well?' Bob Hope responds, 'I'm still thinking about it!'

20 An excellent example of a view that captures somewhat of the distinction I am aiming at is that of David Sussman ('What's wrong with torture?' *Philosophy and Public Affairs* 33,1 (2005): 1–33), who argues that the special wrongness of torture lies not just in the infliction of pain but in how the torturer *uses* your body to bypass your will and force you work against your own judgment and ends. This view, obviously, has strong affinities with Kantian views of morality in general and the Formula of Humanity in particular. See, especially, Christine Korsgaard, *Creating the Kingdom of Ends* (Cambridge: Cambridge University Press, 1996) pp. 106–132; and Onora O'Neil, *Constructions of Reason* (Cambridge: Cambridge University Press, 1989) pp. 105–125. For a sceptical note, see Japa Pallikkathayil, 'The possibility of choice: Three accounts of the problem with coercion' *Philosophers' Imprint*, 11,16 (2010) Nothing in my argument rides on the particulars of Kant's view, but the imposition of will view is clearly Kantian-inspired.

21 A different yet attractive way to conceptualise the distinction is to conceive of an 'Imposition of Will' and thereby 'casus belli' as *moralised* by indexing it to particular set of rights people have. On this view, imposing one's will on another is violating a particularly urgent set of rights, say to one's property or one's bodily integrity. An advantage of the moralised conception is that it can easily say why threats look like impositions of will rather than costs. Consider a case where the highwayman says, 'Your money or I'll break your windshield' and *genuinely means it*; the highwayman will break the windshield and walk away without your money, somewhat bizarrely. The moralised conception can call this an imposition of will because you have a *right* to your windshield and your money, so the imposition results from the fact that your rights will necessarily be violated by the highwayman no matter what you do. In the international context, we might be able to work out the distinction between forceful interventions on the one hand and non-forceful interventions on the other by referencing some right to territorial integrity or political autonomy that is *not* violated by EMBARGO or RARE EARTH MINERALS. I am not sure such an account will be forthcoming. But even if it were, the view has the following implausible result: the United States and Great Britain did not attack the empire of Nazi Germany when they landed in Normandy. After all, Germany had no right to French territory. This does considerable violence to the language. The better thing to say, I submit, is that the United States *justifiably* attacked Nazi Germany. But then we need a non-moralised account of what constitutes an attack. Of course, this mirrors a serious divide in accounts of coercion that I won't attend to here.

22 Scott Anderson 'The enforcement approach to coercion', *Journal of Ethics and Social Philosophy* 5 (2010): 1–31; see p. 6.

23 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) (1986 I.C.J. 14).

24 Effective control over a territory is a necessary condition for state recognition in the Montevideo Convention (165 LNTS 19; 49 Stat 3097), for example.

25 There is an interesting question concerning whether the theft of *data* could be characterised as analogous to the attempted theft of the trinket in TRIVIAL HIGHWAYMAN. Is data property?

26 See Dilpert op. cit., p. 388, for description and counter-measures.

27 Dilpert op. cit., p. 397.

28 I am treating Stuxnet and LOGIC BOMB as distinct cases. I thank an anonymous referee for asking me to clarify my view here.

29 This does make discrimination quite difficult, as it is very hard to attack only legitimate targets with cybertools if the important computer networks are all dual use. In fact, dual-use networks might be characterised, in a way, as an attempt to use civilians as a human shield.
30 Robert Pape. *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996).
31 See Michael Cieply & Brooks Barnes, 'Sony cyberattacks, first a nuisance, swiftly grew into a firestorm', *The New York Times* 30 December (2014).
32 I thank an anonymous reviewer for urging me to be much clearer about the inflationary nature of both the Standard and Sovereignty views.