Cyber War Forthcoming: "It Is Not a Matter of If, It Is a Matter of When."

https://www.e-ir.info/2020/07/08/cyber-war-forthcoming-it-is-not-a-matter-of-if-it-is-a-matter-of-when/

HARRIET CHARLOTTE TURNER, JUL 8 2020

A new security climate which encompasses threats beyond the realm of conventional warfare has brought about new challenges and new questions for strategy analysts. One question at the heart of the contemporary and complex security landscape remains; will cyber war take place or is it merely a sophisticated extension of sabotage, subversion and espionage? All three of which, as Thomas Rid (2012) emphasises, are certainly not new. The essay will stand in agreement with Rid by arguing that indeed, cyber war has not taken place in the past. However, it will proceed to argue that cyber war will take place in the future because cyber-attacks are likely to eventually meet the criterion necessary to constitute warfare. Thus, to claim otherwise as Rid has, is outdated, an 'overly restrictive' interpretation of what war is (Whetham, 2016. P.61) and underestimates the technological advancement in cyberspace. The essay will carry the idea that 'it has not happened yet, but it will' forward by cross-examining five crucial points which are as follows.

Firstly, it will argue against Rid where he claims that there is no force or direct violence involved in cyber-attacks that would render them acts of war. Secondly, it will tackle the most complex issues of all which are attribution, declaration and anonymity. Thirdly, it will challenge Rid's distinction between sabotage and warfare by re-defining these boundaries and examining the Stuxnet attack as a plausibility probe by means of the equivalent-effects and Schmitt tests. Fourthly, it will argue that cyber-attacks do not need to be potentially lethal or involve physical injury or death to be considered acts of war. Lastly, it will argue that some cyber-weapons will have the capacity to damage all three areas which constitute the paradoxical trinity which can generate a strategic paralytic effect and 'compelour opponent to fulfil our will' (Clausewitz and Heuser, 2008, p.13). In summary, the essay will argue that cyber war will take place by dissecting and challenging Rid's journal article and employing the work of scholars such as Amit Sharma, John Stone and David Whetham who constructed credible counter-arguments.

As James Cartwright stated, an act of war is "in the eye of the beholder'' (Nakashima, 2012). Thus, it is of initial importance to attach a definition to what will be meant by warfare in the following essay. Like Rid, the essay will agree that an act of war has to meet the following criteria which were outlined by Clausewitz; firstly, the act has to be inherently violent, secondly, it has to be instrumental and finally it has to be political (Rid, 2012, p.7). It will also agree with Rid and argue that we should not categorise all acts of cyber hostility as an act of war, such as cyber-espionage and subversion, because this blurs the boundaries between war and non-war and risks war becoming a hodgepodge notion. However, it will diverge from Clausewitz and Rid's idea that the employment of maximum force to produce violence is necessary and argue against this. It will also argue that human lethality is not necessary for acts of force to fall under the rubric of war because violence also entails damage to physical property and psychiatric injury (Whetham, 2016, p.61). Thus, the broad definition and interpretation of what is considered war will be an amalgamation of both Sun Tzu and Clausewitz' ideas, as opposed to maintaining a narrow focus on one theorist's ideas. As Amit Sharma (2010, p.64) noted,

Cyber warfare derives the essence of both of these great military theorists, as it is warfare that is capable of compelling the enemy to do your will by inducing strategic paralysis to achieve desired ends, and this seizing of the enemy is done almost without any application of physical force.

After all, the reason that Rid's argument is an outdated and uses an 'overly restrictive' (Whetham, 2016, p.1) interpretation of what war is, is because the entirety of his journal article rests on the foundation of Clausewitz. This essay does not wish to belittle the significance of Clausewitz' work, but it would be wrong to claim that Clausewitz' ideas do not need to be modified to fit the current security climate. After all, a lot has changed since 1832 – specifically the emergence of cyber-weapons which has simultaneously decreased the idea that maximum force is desirable and gave Sun Tzu's ideas of minimal force and deception (Sun Tzu and Griffith, 1963, p.77) a new lease of life.

To begin, it is important to show how cyber war will take place in the future by demonstrating that acts of limited force can translate into inconceivable violence, rather than synonymising the two terms. As John Stone rightly noted, 'the fundamentals of war were never considered properly because strategy as a discipline was very pragmatic but had nothing to offer by way of clarification for important terms such as 'force' and 'violence' (Stone, 2012, p.104). However, clarification is necessary in order to argue that cyber-war will take place. Limited force (providing it produces a violence), combined with instrumentality and being political can indeed fall under the rubric of war. This is where Sun Tzu's ideas are particularly relevant because he wrote that 'to seize the enemy without fighting is the most skilful' (Griffith, 1963, p.77) which is applicable to cyber-attacks since it *could* be possible to subjugate the enemy without the deployment of conventional armed forces and minimal force. Nonetheless, it has been demonstrated through Stuxnet and fictional cyber-attack scenarios that cyber-attacks have and *could* meet the criteria necessary to constitute an act of war and compel the enemy to fulfil its will through minimal force, whilst simultaneously encapsulating the art of war where the wise warrior avoids the battle (Griffith, 1963), – at least, conventionally. Therefore, Rid is incorrect to state that because the force necessary to conduct a cyber-attack is limited that cyber-attacks cannot conjure enough violence to be considered acts of war.

This point can be further reinforced because whilst Clausewitz makes it clear that force is the pivotal point of war, he never quantifies how much force is necessary for it to qualify as an act of war. Clausewitz merely states that maximum force is desirable to gain the upper hand in a conflict (Clausewitz and Heusser, 1976, p.14). However, in cyberspace that is not applicable because gaining the upper hand can actually be achieved through minimal force and bloodshed. This is primarily because acts of force which are as small as tapping a keyboard can translate into mass violence; injuring (physically or mentally) or killing people and/or physical objects along the way (Stone, 2013, p.107). In addition, the idea that minimal force can gain the upper hand is heightened by the deceptive nature of cyber-attacks and the fact that they are generally not declared but rather the attacker 'attacks him where he is unprepared and appears when he is unexpected' (Griffith, 1963, p.89), which can amplify damage and thus chances of victory. In brief, Rid is mistaken to synonymise and conflate the terms 'violence' and 'force' in order to make his case because small force *could* cause inconceivable violence.

This naturally leads the essay to show that despite difficulties in attribution, cyber war *could* still take place. The fact that cyber-attackers often appear when the opponent is unprepared and when he is unexpected leads to the most complex issues of all which are attribution, anonymity and the absence of declaration. It is argued by Rid that cyber war cannot take place in the future because 'history does not know acts of war without eventual attribution' (Rid, 2011, p.8). Rid's reasoning behind this is that without being able to attribute an attack to another state, the attacked state does not know how or in which geographical location to conduct a counter-attack. However, although history does not know acts of war without eventual attribution, the future might because it seems that this *will be* a new, challenging facet of what will be defined as war (Stone, 2013, p.105). Indeed, it is possible that due to the changing character of war, there will be an inability to ever definitively attribute an act of war to another actor in cyberspace. However, this does not mean that the act does not constitute an act of war. Where an act of war meets the criteria outlined earlier in the essay, namely; the act is inherently violent, political and instrumental, then 'matters of openness and attribution are not germane to any attempt at distinguishing between war and sabotage' (Stone, 2013, p.106).

To build on this, questions that have proven difficult for strategy scholars are; firstly, how can it be a war if it takes weeks, months or even years to eventually attribute it to another actor? Secondly, could a response be considered a counter-attack or simply punishment beyond a certain threshold? Firstly, Clausewitz never attaches a time limit to the word 'eventual' when he is discussing attribution which is incredibly vague and open to interpretation. Thus, regardless of whether it takes days, months or even years to for the attack to be attributed to the auspices of a

government – the act *could* still be rendered an act of war because 'eventually' holds no actual time limit and is open to the interpretation of the reader. In response to the second question posed to strategy scholars, 'Under the Law of Armed Conflict and Article 51, it is not made clear what degree of certainty in identification is required to justify a response' (Farwell and Rohozinski, 2011, p.35). Therefore, the law of armed conflict and article 51 should ideally be modified in order to make matters clearer for states for if and – more appropriately – *when* they are devastated by a cyber-attack.

Diverging from the previous point, in order to show that cyber war will take place, it is important to cross-examine Rid's failure to properly distinguish between what is sabotage versus an act of war in literary terms. Rid argues that any 'deliberate attempt to weaken or destroy an economic or military system' where 'things are the prime targets, not humans' (Rid, 2012, p.16) is sabotage and thus cannot be considered warfare. However, the distinction in Rid's analysis rests solely upon the fact that the damage cannot merely affect physical property but should injure or kill people on at least one side of a conflict. This is where Rid is mistaken because a violence, as defined in the Oxford English Dictionary, need not necessarily kill or injure people (Stone, 2013, p.104). Rather, an inherently violent act can solely cause damage to physical property. A violent act could even cause no damage at all because the mens rea has to only be for the commission of the act, and thus the actual result is insignificant. This misunderstanding of the essence of the word 'violence' is clearly why Rid believes that the Stuxnet attack on the Iranian enrichment plant can squarely fit within what is defined as sabotage as opposed to recognising that the Stuxnet case was a deeply contestable one which does not squarely fit within the bracket of sabotage. Rid's failure to recognise Stuxnet as an act that transcends sabotage can be credibly opposed by the fact that first and foremost; the act was political in that as David Clemente (2010) said 'it is of such complexity it could only be a state behind it' (Beaumont, 2010) and more specifically, a 'cyber superpower' was behind it (Rid, 2012, p.19). Secondly, it was instrumental in that Stuxnet had a means and ends because it effectively forced Iran to accept the offender's will of a delayed Iranian nuclear programme (Zetter, 2014). And ultimately, it was violent because it was the first instance of a physically destructive cyber weapon which damaged centrifuges (Zetter, 2014).

To further reinforce the idea that Stuxnet was not a merely grand version of sabotage, it is crucial to examine it via two key indicators which are as follows. Firstly, the Stuxnet attack qualifies as an act of war under the equivalent-effects test because it is comparable to a kinetic attack and has 'the effect of a cruise missile or a commando raid' (Wedermyer, 2012, p.20). The equivalent-effects test is important for categorisation purposes because it is one of the primary ways to distinguish between an act of mere hostility and an act of war. As Lewis (2011) noted, 'no damage or no casualties, means no attack' which is why, as Rid stated, cyber-espionage cannot be considered an act of war. This is because there is hostile activity in cyberspace such as cyber-espionage, 'but it stays below the threshold of an attack' (Lewis, 2011). However, Stuxnet is different because it did cause physical damage akin to a kinetic attack. Another way to demonstrate that Stuxnet could potentially be considered an act of war in the future is the fact that it largely satisfies the Schmitt test criteria because it caused 'physical damage to the Iranian nuclear infrastructure, was highly invasive, its damage was quantifiable, and it was almost certainly created under the auspices of a national government' (Wedermyer, 2012, p.21). All things considered, one question remains; if the United States (US) and Israel conducted a commando raid against the Iranian nuclear facility, would it be considered an act of war or merely sabotage because it did not kill anybody? It is likely that it would be considered an act of war or more specifically, be akin to a covert operation conducted by the Special Forces. Although this contestable cyber-attack has not caused a cyber-war, it certainly demonstrates how cyber war *could* take place in the future. Thus, whilst Rid (2012, p.20) states that Stuxnet has taken computer sabotage to an entirely new level, he is detracting from the fact that this is not simply a new level of sabotage.

Furthermore, it is important to note that cyber-attacks *can* be considered acts of war if they transcend the realm of physical harm to people and property and only affect the psychological wellbeing of people; causing psychiatric injury. Therefore, by 'demanding that physical violence is required seems to be an overly restrictive interpretation of an "act of war," just as it would be to limit the definition of "assault" in a domestic jurisdiction' (Whetham, 2016, p.61). To elaborate on this point, ''in the UK the legally accepted definition of assault does not require physical harm to be satisfied'' (Whetham, 2016, p.61). Psychiatric injury can, in certain cases, be classed as Actual Bodily Harm (ABH) and therefore, damage and harm does not necessarily have to be physically visible for it to be considered an act of force or violence. To summarise, violence should not be restricted to the bounds of physical damage but rather

should be extended to psychiatric injury which is not visible. With that in mind, if a cyber-attack achieves the desired policy outcome through a means of psychiatric injury which subsequently compels the adversary to fulfil its will – surely Clausewitz would have considered this an act of war? Clausewitz (1989, p.92) states that to obtain a single victory, 'we will employ no more strength than is absolutely necessary' so this must suffice, on the condition that it compels the enemy to fulfil its will.

Moreover, it is important to challenge Rid's idea that cyber war will not take place by challenging one contradictory statement. Rid is careful to outline the difference in immediacy and directness between a kinetic attack such as a drone attack compared with a possible future cyber-attack and states that where potential cyber-attacks are concerned, 'the causal chain that links somebody pushing a button to somebody else being hurt is mediated, delayed, and permeated by chance and friction' (Rid, 2011, p.9). Although, Rid states that despite this, they *could* still be considered an act of war if, say, a derailment, caused by logic bombs crashed a train or caused air traffic systems and their backups to collapse (Rid, 2012, p.9) and thus resulted in a number of injuries and deaths. However, if he can recognise that this *could* happen then he cannot credibly dismiss the idea that cyber war will take place. It is likely that Stuxnet is not where cyber-weaponry advancement ends. As I write this essay, people are probably researching the next physically destructive weapon which could produce an equivalent effect or a apply combat power simultaneously at the strategic, operational, and tactical levels of war to paralyse an adversary's ability to function. States' cyberspace is becoming increasingly vulnerable due to the ever-increasing technological advancements that are occurring. Therefore, to claim that cyber war will not take place could result in a failure to respond appropriately due to a 'lack of a harmonised framework to effectively respond to the challenges posed by this incident' (Trimintzios, et al. 2015, p.16).

Finally, it is important to demonstrate how cyber-war could happen in the future through the notion of trinitarian warfare. The trinity is composed of three tendencies which are as follows; the government, the people – including the economy – and the defenders of the state; all of which are considered crucial to keep the cogs of the state turning (Sharma, 2010, p.64). Individually, each component of the trinity is resilient enough to recover from challenges posed by adversaries because it can rely on another one of the components in the trinity to resuscitate it. However, 'when all of the three components are destroyed together or in conventional terms are subjected to parallel warfare, 'cascade effect' is generated to induce a strategic paralytic effect on the nation' (Sharma, 2010, p.64) which catapults the state into a state of turmoil and tumult. It is now the case that all three tendencies heavily rely on technology, particularly in modern states, which can be supported by Jeremy Corbyn recent proposal that Wi-Fi should be free at the point of use because it is an essential, basic utility as opposed to a luxury (Walker, et al. 2019). This dependence on cyberspace certainly exposes the vulnerabilities of all three tendencies to parallel warfare. This is currently evident in the COVID-19 pandemic as a successful cyber-attack on the health service infrastructure and communications technology *could* induce a strategic paralytic effect on the UK. To further emphasise this point, the Titan Rain attacks on Estonia and Georgia were not successful acts of war because they were tactical in nature and were targeting individual components of the trinity, as opposed to applying power simultaneously at the strategic, operational, and tactical levels of war and thus impacting all three components of the trinity (Sharma, 2010, p.68). Therefore, for cyber-attacks to be considered acts of war, they should cause equivalent damage to a kinetic attack and for them to be particularly successful at subjugating the adversary, they should be conducted using the paradigm of parallel warfare (Sharma, 2010, p.67). All things considered, whilst previous cyber-attacks have not been successful acts of war, this does not imply that they will not be in the future and thus cyber-war *could* take place in the future.

In conclusion, it is clear that although cyber war has not yet happened, it is likely to happen in the future. This is primarily because some cyber-attacks can fulfil the criteria necessary to constitute an act of war which is as follows; inherently violent, political and instrumental. It is also the case that small acts of force – such as the tap of a keyboard (Stone, 2013, p.107) – can cause inconceivable violence. As for the incredibly difficult issue of attribution and declaration, although history knows no act of war without eventual attribution, the future of war *could* pose an unprecedented challenge to the world where there never is definitive attribution. Moreover, violence caused by an attacker does not have to be lethal but can be extended to the damage of physical property and psychiatric injury. One specific plausibility probe that was discussed in the essay and reinforces the argument that cyber war will take place is the Stuxnet attack on the Iranian nuclear facility which gave the world foresight into what could take place but on a larger, more sophisticated scale in the future. Finally, cyber-attacks have the potential to induce a 'cascade

effect' where all components of the trinity are damaged and thus seize the enemy through strategic paralysis. It is no longer a question of if cyber war will take place but rather a question of when it will take place.

Bibliography

Beaumont, P. (2010). Stuxnet worm heralds new era of global cyberwar. The Guardian. Accessed on: 3rdMay 2020. Available at: https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar.

Clausewitz, C, Heusser, B, Howard, M. and Paret, P. (2008). *On War*. Oxford: Oxford University Press, 2008.

Farwell, J. & Rohozinski, R. (2011) Stuxnet and the Future of Cyber War, Survival, 53:1, 23-40, DOI: 10.1080/00396338.2011.555586

Lewis, A. J. (2011). Cyber Attacks, Real or Imagined, and Cyber War. Accessed on: 5th May 2020. Available at: https://www.csis.org/analysis/cyber-attacks-real-or-imagined-and-cyber-war.

Nakashima, E. (2012). 'When is a cyberattack an act of war?' The Washington Post. Accessed on: 2nd May 2020. Available at: https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html.
6. Rid, T. (2012). Cyber War Will Not Take Place, Journal of Strategic Studies, 35:1, 5-32, DOI: 10.1080/01402390.2011.608939.

Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. Strategic Analysis, 34:1, 62-73. Accessed on: 27th April 2020. Available at: https://www.tandfonline.com/doi/pdf/10.1080/09700160903354450?needAccess=true.

Sun Tzu, The Art of War, trans. Samuel B. Griffith. (1963). Oxford University Press, Oxford, 1963, p. 77.

Stone, J. (2013) Cyber War *Will* Take Place!, Journal of Strategic Studies, 36:1, 101-108. Accessed on: 27thApril 2020. Available at: DOI: 10.1080/01402390.2012.730485.

Trimintzios, P., Ogee, A., Gavrila, R. and Zacharis, A. (2015). European Union Agency for Network and Information Security. On Cyber Crisis Cooperation And Management. Accessed on: 1st May 2020. Available at: DOI: 10.2824/948513.

Whetham, D. G. (2016). "Are We Fighting Yet?" Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War? Accessed on: 28th April 2020. Available at: DOI: 10.1093/monist/onv029.

Walker, P. et al. (2019). Labour's free broadband plan fires up the election battle. The Guardian. Accessed on: 4th May 2020. Available at: https://www.theguardian.com/technology/2019/nov/15/free-broadband-essential-uk-compete-john-mcdonnell-labour-policy-openreach.

Wedermyer, L. J. (2012). The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict. Accessed on: 1st May 2020. Available at: https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1206&context=king.

Zetter, K. (2013). Legal experts: Stuxnet Attack on Iran was Illegal 'Act of Force'. Wired. Accessed on: 3rdMay 2020. Available at: https://www.wired.com/2013/03/stuxnet-act-of-force/.

Written at: University of Leicester
Written for: Dr Robert Dover
Date written: May 2020