Section: Debate

Between doomsday and dismissal

Cyber war, the parameters of war, and collective defense

Isabelle Duyvesteyn[1]

Cyber operations, the 'fifth dimension' of warfare, is a contentious issue in scientific debates. This article analyzes two opposing theoretical frameworks about cyber war: 'doomsday or dismissal'. Some scholars argue that cyber Armageddon will be upon us, while others claim cyber war does not even exist. At the Wales Summit, NATO member states have decided that cyber attacks can warrant collective action under the NATO treaty stipulations. Therefore, it is more than necessary to think through the offensive and defensive uses of cyber power within the war paradigm.

Cyber war in Wales

Little noticed among the deliberations during the NATO Wales summit, which primarily focused on the Ukraine, was the path-breaking decision to include cyber attacks among the triggers for the collective defense clause. In their joint communiqué the 28 member states stated that the NATO treaty's foundational doctrine of collective defense now also applies to cyber attacks. A cyber attack on one of the member states of the alliance could now be perceived as an attack against all. The communiqué states:

> "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."

This development calls for an urgent thinking through of the concept of cyber war. The scientific debate about cyber war at present is highly polarized. Doomsday or dismissal: these are the most common positions taken. On the one hand, we have scholars such as Richard Clarke who have vociferously argued that if we are not careful, cyber Armageddon will be upon us. Such doomsday scenarios envision concerted cyber attacks causing the collapse of the electrical grid and critical power-supply failures, bringing hospitals, trains, airplanes and the financial system to a grinding halt. According to Clarke, "A sophisticated cyber attack by one or several nation-states could do that today in fifteen minutes, without a single terrorist or soldier ever appearing in this country."

Others, including Thomas Rid, have written articles and books with titles such as *Cyber War Will Not Be Coming*. Their view is that the possibility of cyber war has been exaggerated by a modern-day digital-industrial complex. By paraphrasing the nineteenth-century military philosopher Carl von Clausewitz, they argue that war is fundamentally an act of force intended to compel an enemy to do one's will. Thus, for something to be called 'war', there must be at the very least a demand made by one combatant or another accompanied by the

threat of real physical harm. Cyber weapons, such as Denial of Service attacks, installing malware or the hacking of computers, sometimes in the shape of organizing botnets, are by themselves incapable of directly causing any kind of loss of life. Furthermore, in the cyber domain demands are often vague and combatants anonymous; therefore, authors such as Rid argue that, strictly speaking, 'cyber war' does not and cannot exist.

This article aims to be a corrective to this polarized and lopsided view of the link between cyber and war. It will argue that cyber war, contra Rid, does exist and has occurred in the past and present. However, cyber warfare will most likely take a form different from the existential destructive model that Clarke has so ominously sketched. To what extent is there an identifiable enemy against whom force or coercion can be used to attain a desired political end?

Three parameters of war under attack

In contemporary discussions the idea of cyber war challenges the existing strategic paradigm in three important ways. First, there has been debate about the violent nature of cyber conflict. Rid argues that most cyber security breaches come in the shape of sabotage, espionage and subversion. Based on this distinction, he argues that "No cyber offense has ever caused the loss of human life. No cyber offense has ever injured a person. No cyber attack has ever damaged a building." The argument, however, ignores the important distinction between force and lethality, according to which, as John Stone has argued, "acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character."

Second, there is debate over whether cyber war fits into the relational parameter of war. War requires at least two identifiable actors with opposing wills and goals. There seems to be some measure of agreement that the problem of attribution in the cyber domain challenges this fundamental prerequisite. This article will argue that contemporary patterns show that most significant cyber security breaches are still largely state-based and that the identification of the perpetrators of cyber security breaches is not as challenging as portrayed in the current debate.

Third, there is debate about the instrumental paradigm of war, as a means to an end and guided by politics. This argument fits in with a larger debate since the early 1990s about the changing character of war. Cyber war, it is now argued, goes beyond the political parameters of war, where it can no longer serve a rational political end and is geared towards personal or commercial benefit or destruction, viz. the arguments of Rid and Clarke *cum suis*. This article will argue that this presumption is overstated.

War and violence

The scholarly debate has to a great extent focused on the non-violent character of cyber attacks. Clausewitz emphasized the conditionality of the violent character of war: "War is a clash between major interests, which is resolved in bloodshed — that is the only way in which it differs from other conflicts." However, at the same time he argued that decisive force might not always be necessary: "operations with direct political repercussions … can greatly improve our prospects and … they can form a much shorter route to the goal." This

idea is very close to the thinking of Sun Tzu who stated that "there are no constant conditions [for war]", thus detaching war from violence and force as essential parts. Clausewitz's term 'Gewalt' leaves room for ambiguity because the German language does not make a distinction between force and violence.

The scholarly debate, however, has unfortunately shifted away from this terminological question to place emphasis on the question of (potential) lethality. The absence of violence has been the most prominent and telling objection of critics like Thomas Rid against classifying cyber attacks as war. However, if we look beyond the physical manifestation of the Clausewitzian use of the term 'force' to its utilitarian characteristics, we find that the definition of force can and needs to be broadened considerably in order to understand the essence of war. According to Clausewitz, force serves the purpose of maneuvering one's opponent into a situation where giving in to one's wishes would be less damaging than even the most optimistic assessment he is likely to make of his chances should he keep fighting. For Clausewitz, that goal was most clearly realized by decisive force. However, this 'giving in' could be, and has also been, in many cases achieved by other means. Force is not necessary or sufficient *on its own* to create strategic effect in the clash of wills. It is undoubtedly the most direct route, as Clausewitz identified, but there is always the role of will, rather than force as capability, that holds the key to delivering what one desires from an opponent.

General Sir Rupert Smith, in his book *The Utility of Force,* convincingly argued that Western states have long specialized in using force to create a condition in which other levers of power deliver the political result rather than via a direct application of decisive force. The 'other means' Clausewitz refers to in his description of the essence of war only work in close conjunction. Those who emphasize the production of lethality at the expense of force and other means of power do an injustice to the essence of war and run the risk of developing faulty strategies.

The relational parameter

War in whatever shape or form has certain perennial features. There need to be at least two actors with conflicting interests who are capable and willing to inflict physical harm upon one another in pursuit of their interest. There is a methodological problem here: which actor is sending or signaling is often unclear. This is the so-called attribution problem.

Attribution is deemed fundamental in the discussion about cyber war. It has been interpreted as a conflict-inducing mechanism: "this ability to stealthily use cyber power, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it a very attractive instrument for governments and other actors."[2] Deterrence and a justified counterattack become difficult when the sender remains anonymous. As David Betz and Tim Stevens have argued, in any coercive confrontation a sender and a receiver are necessary:

> "Strategy ... requires agency by design because it starts with some notion of purpose. Of course there is an iterative element to the balancing of ends and means: the aim of policy may be beyond the means available and therefore, unless more means are discovered, the end must be reduced; but the process starts with someone setting the agenda."[3]

If it remains unclear what the sender desires from the receiver, the act of coercion misses its goal. Therefore cyber war does not fit the conventional understanding of war strategy because, they argue, the relational parameter has been fundamentally undermined.

This debate about attribution has been largely conducted from a technological angle. Some have argued that we should lower our standard when it comes to attribution and instead focus on who benefits from particular actions: "for the cases of Estonia and Georgia 'whether or not you accept that some, all, or none of these events occurred with the sanction of the Kremlin, each event has been instrumental in furthering RF [Russian Federation] policy, and the Kremlin has never acted to stop them. Hence the RF benefits'."[4] Research has also shown that in regards to the timing of the attacks there is little doubt that the cyber attackers knew the exact time of the Russian military advance in the case of South Ossetia.[5] It is very likely that in cases of open conflict the attribution problem is mitigated by the weight of interests at stake. In fact, John Stone argues that clear attribution is not necessary for something to be called a war.

According to recent statistics, the overwhelming majority of cyber attacks can today be traced to states, most notably China, Russia and Iran.[6] Cyber war remains a relational activity. The methodological challenge of identifying the sender can, in practice, be mitigated by using the historian's toolkit and the art of carefully reconstructing cases to bring forward the most plausible explanations for causality. There are three main ways of assessing the attribution for a cyber attack; the context of the attack, the analysis of the target and its possible opponents (the dyad) and the message or intention behind the attack (place and time). The attribution problem is no impediment to the application and applicability of the concept of strategy.

The instrumental parameter

The instrumental parameters, i.e. war as a means to an end, which have guided thinking about war since the nineteenth century have been challenged by current ideas about cyber attacks. Clausewitz argues that a means-ends relationship is present in war. A casual reading of the cyber war literature might suggest that cyber war could be seen as an end in itself and possibly a new incarnation of Clausewitz's absolute war beyond the realm of politics. According to Dennis Murphy, "some observers equated that cyber attack [against Estonia in 2007] to an act of war in the Clausewitzean [sic] sense, with the intent to create mass social panic."[7] In a slightly more muted form, the idea of cyber war provides a "false allure ... in the notion that it provides a sneaky way to return a decisiveness to major war which ... it has lacked for many years."[8]

In linking the means to the end, a message is necessary: what is it that the opponent needs to do, or refrain from doing, in order to avoid further harm? There is another methodological challenge here: how to analytically separate the means and the motivations behind cyber attacks? Tanks cross borders, rockets are launched and land somewhere, bombs are directed at a target; these means and their targets usually reveal the sender, the goal and often the motivation. In a cyber setting, the actor uses a limited set of means or tactics that can simply cause havoc and destruction but can also deliver a political message. Since cyber attacks come in a limited number of shapes and guises, it is difficult to infer intention and motivation behind an attack from the type of attack. The type of attack does

not say anything about the attacker; common criminals as well as state agents can use the same means to achieve their highly distinctive ends: personal gain or gratification versus political advantage. Others have noted that "Nearly every significant cyber event reported since 2005 involves tradecraft, techniques and code tied to the cyber-crime community."[9] Furthermore, "cyber crime is the laboratory where the malicious payloads and exploits used in cyber warfare are developed, tested and refined."[10]

Cyber war needs to be distinguished from other cyber security breaches. The former should be seen as an act of force that aims at achieving a political end. It involves violence, a political message and at least two actors with opposing wills, whereby the threat of physical harm is instrumental in conveying that message. Cyber war fits very well in a constraining and utilitarian approach.

Conclusion

Despite arguments made by Richard Clarke and Thomas Rid, cyber war can be identified as an analytical category and fits into a political framework. Seeing cyber attacks as destructive existential threats or as problems of espionage and subversion distracts us from the real challenges.

As the NATO member states have now decided that cyber attacks can warrant collective action under the NATO treaty stipulations, it is more than necessary to think through the offensive and defensive uses of cyber power within the war paradigm. The Netherlands is one of the few states that have openly acknowledged that it is in the process of developing offensive cyber weapons. How and when can cyber weapons be effectively used? How should we view the development of strategy and doctrine which include cyber attacks? These are urgent questions that need to be debated in both academic and policy circles.

Isabelle Duyvesteyn holds a Special Chair in Strategic Studies at the Institute of Political Science, Leiden University. She wrote this article in collaboration with Sofia Lettenbichler, Marijn Nagtzaam, Martijn van Nijnanten, Thijs van Rijn, and Jascha Wieldraaijer.

Would you like to react? Mail the editor: redactie@atlcom.nl.

1. The author would like to thank Jeremy Butcher and John Stone for their input in previous versions of this article.
2. John B. Sheldon, 'State of the Art: Attackers and Targets in Cyberspace', *Journal of Military and Strategic Studies* 14/2 (2012).
3. David Betz and Tim Stevens, *Cyberspace and the State; Toward a Strategy for Cyber-Power Adelphi Paper 424* (London: Routledge 2011), 118.
4. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA.: O'Reilly Media 2010) 161.
5. Jean-Loup Samaan, 'Cyber Command; The Rift in US Military Cyber-Strategy', *The RUSI Journal*, 155/6 (2010) 16-21.
6. Richard Clarke, 'China's Cyberassault on America', *Wall Street Journal,* 15 June 2011.
7. Dennis Murphy, 'Attack or Defend? Leveraging information and balancing risk in cyberspace', *Military Review* (May-June 2010) 91.
8. Betz and Stevens, *Cyberspace*, 95.

9. James Farwell and Rafal Rohozinski, 'The New Reality of Cyber War', *Survival*, August-September 2012.
10. Jeffrey Carr, *Inside Cyber Warfare*, 5.