# How Serious is the Threat of Cyber Warfare?

https://www.e-ir.info/2012/05/22/how-serious-is-the-threat-of-cyber-warfare/

DAMIAN STRUGLINSKI, MAY 22 2012

For a long time war in cyberspace remained the domain of science fiction writers. The average person usually experienced cyber hostility only in the form of the occasional computer virus or similar malicious software. However, with the creation of the US Cyber Command as part of the US Strategic Command in June 2009, it seems that cyber warfare has become an official and serious concern for international security. With that development many questions about the nature of war begin to arise. How will this new medium affect war? Is a "cyber-war", a phrase so oft-quoted lately, to be expected or perhaps cyberspace will become another plane of combat, much like sea or air? The discussion is currently a very popular topic and will probably remain so, if not from inherent ambiguity alone then because of the speed with which technology evolves. The purpose of this essay is to evaluate how serious are the threats of cyber warfare and how it influences the reality of war. This essay will argue that even though an instance of cyber war as a standalone entity is not going to happen, that area of warfare is relevant. First of all, the essay will analyse the core issue of defining the entity of said conflict and whether is it really a possibility. In second part, it will focus on the actual "weapons" of the cyber age, their characteristics and what threats do they pose. It will examine corrupt soft- and hardware, the DDoS attacks and Stuxnet separately as representing different threats. Finally, this essay will attempt to establish how such cyber threats fit in and influence war.

The most crucial aspect in the on-going discussion is establishing what a "cyber war" should constitute. Looking back in time one can see how perceptions changed in the last two decades. When John Arquilla and David Ronfeldt published their article on this matter, the concepts of cyber war[1] and net war[2] were just formulating and highly speculative. However, several key elements can immediately be brought to attention. The idea of conflict revolving around the axis of information has scaled well with time and technology. Furthermore, the prediction that there would be a transition from state actors to networks, i.e. non-state groups, has proved accurate. However, equally apparent are the flaws in that argument; given the situation at the time of writing, the modern combat seems far from "decisive campaigning without a succession of bloody battles".[3] In these circumstances then, the question whether cyber war does exist still stands. The Pentagon announced in 2011 that cyber-attacks will be considered as acts of war and in turn act as *casus belli*.[4] In spite of that, the discussion about interpreting aggressive cyber activity as the use of force in light of the UN Charter is inconclusive and a legal consensus is not to be expected soon.[5] The idea of a cyber war as a standalone instance of war seems improbable though. As noted by Thomas Rid, cyber warfare lacks the essential characteristics to meet the conditions of becoming an act of war; if the"use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria".[6] And though that idea may not be the most vocal amongst the scaremongering, it is certainly not neglected. Specialists from the Center for Strategic and International Studies seem to back up this view as well.[7]

Even though cyber war may not be an issue that does not mean that, by proxy, "cyber weapons" are not a threat and hence require examination. The most basic and dated forms of such measures would have to be simply corrupted soft- and hardware. A prime example, though perhaps the only allegedly successful one, would be sabotaging the Soviet Urengoy–Surgut–Chelyabinsk natural gas pipeline in 1982. According to Thomas C. Reed, the CIA procured a modified pipeline control system in anticipation of KGB trying to steal it. The result was supposedly a massive explosion after the eventual malfunction and pump reset.[8] While that issue seems like a significant threat there are numerous factors that limit the actual importance. First, that can hardly be considered cyber warfare as it requires direct physical intervention. Furthermore, with the development of safeguard measures which constantly check for malfunctions and authenticate security certificates it becomes virtually impossible to sneak in corrupted wares, even without counting in the human factor. Proof seems self-explanatory: no other instance of a similar attack has been documented and even this one has been doubted.

The most widely known and perhaps the most overemphasized cyber attack at the time of writing is by far the DDoS which stands for Distributed Denial of Service. Its main strength lies with its accessibility; a plethora of software of varying degrees of complexity, both free and commercial can be easily obtained.[9] That is precisely the reason why protesters and other groups often resort to DDoS as means of communicating their discontent. However, the actual threat that these measures pose is quite limited. Firstly, the DDoS is a blunt tool. In essence it floods an internet address with data in hopes that the server will “clog” and shut down. As such it serves very little purpose in most case scenarios; internal networks are immune to such attacks by design and hence institutions core to the national interest and security are essentially safe. Furthermore, with the rise of DDoS a rise of countermeasures quickly followed. While no clear solution has been found, one can choose from simple switches to block surges in internet traffic, through renting secure tunnels, to complex blackholing (passing the incoming data through a selective filter) provided by some companies. That is why, even though DDoS attack sophistication has increased the actual duration of assaults and downtimes have been on the decrease. According to a report provided by Prolexic, on average the duration was down by 10 hours over the last year and mitigation rates went up by 45%.[10] Even during the most notable instance, Estonia in 2007, downtimes of websites as a result of DDoS assaults lasted only only for up to 2 hours showing limited military potential.

If the DDoS attacks are the most popular, then Stuxnet may well be seen as the most complex. This piece of malicious software has been presented as a herald of the new way of war ever since Iran publicly acknowledged that their nuclear facilities had been compromised.[11] As the virus spread over tens of thousands of computers over a relatively short period of time it has been at times thought of as a sort of weapon of mass destruction, but upon closer inspection it seems that it couldn’t be farther from the truth. By design, Stuxnet possesses surgical precision in terms of delivering the payload to the target. Its activation relied on identifying two core PLCs[12] in the nuclear facilities: S7-417 and S7-315[13]. Furthermore, contrary to public opinion, the aim was not to destroy any industrial equipment but rather to sabotage it for extended periods of time. While Stuxnet caused a significant amount of panic in international security circles, I would argue that worms of that kind cannot be expected to be seen as “cyber missiles”[14], let alone constitute a cyber war. The main argument for that is the way the virus operated; success relied on being undetected. Within months of being discovered the virus has not only been neutralized, but also the code has been thoroughly examined by the Iranian side. As a result, the zero days[15] used by the virus have been patched, preventing not only a secondary Stuxnet attack but also any other assaults using these methods of entry. Furthermore, as the target was not directly accessible, the worm had to rely solely on a *modus operandi* of aggressive infection in hopes of eventually reaching its destination. Therefore, in terms of use in direct war such software, while theoretically significant, has little practical value; a weapon relying on chance, requires extended periods of time to take effect, cannot be used overtly and capable of only striking once can hardly be considered a particularly threatening one at this stage.

So, as the new weapons do not fit the bill as means of direct war-waging, a different niche has to be sought. A surprisingly large number of discussions about cyberwarfare seem to theorize on how destructive it could possibly be[16], while neglecting arguably more important sides of the matter. First and foremost in dealing with cyberspace in general is the problem of attribution. DDoS attacks can be launched from virtually anywhere and with botnets, proxy servers and VPNs[17] the original source is near impossible to reliably track down as the whole operation becomes highly decentralized. Stuxnet itself was not officially attributed to any state or group at the time of writing; any speculation is rumor and educated guesses. In conjunction with its reliance on being undetected to achieve the desired effect it stands to reason that open war for cyber warfare can be only detrimental. To fully capitalize on their potential, cyber attacks need to remain anonymous and in some cases covert. Firstly, that allows the actual payloads to be delivered. Secondly, that would largely mitigate the risks of both retaliation and the Clausewitzian escalation; while the US may see cyber attacks as the aforementioned *casus belli,* without a clear enemy neither a retaliatory cyber offensive nor an armed response can occur. As such, the cyber weapons of this day and age do not synergize well at all with open war.

In conclusion, the debate about cyber war suffers heavily from media hype. The modern version of the concept itself can hardly be called reasonable in the current state of the world. The cyber weapons do are not weapons in the classical sense; they have different objectives, are used in different and so cannot be expected to work in the same manner. Through analysis it seems that providing corrupted soft- and hardware to an enemy is nigh impossible with modern security measures, even more so in a state of war. DDoS attacks are blunt tools of very limited military potential, which serve protesters better than the army. Even Stuxnet, the pinnacle of cyber warfare, is not a direct and fast effect-on-target weapon and in conjunction with being essentially capable of only hitting once lacks the qualities of a weapon sought by the militaries in open conflict. Cyber weapons should rather be used where their strength lies – in covert operations, sabotage, long-term effect on target – or otherwise their effectiveness will inevitably dwindle rapidly.

[1] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol 12, No. 2, Spring 1993, p.30

[2] Ibid., p.28

[3] Ibid., p.45

[4] *Pentagon to Consider Cyberattacks Acts of War,* NY Times, May 31 2011, accessed via http://nyti.ms/wSTm7A

[5] Matthew C. Waxman, 'Cyber-Attacks and the Use of Force', *The Yale Journal of International Law*

36, 2011, p.459

[6] Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2011, DOI:10.1080/01402390.2011.608939, p. 6

[7] James Andrew Lewis, *The Cyber War Has Not Begun*, Center for Strategic and International Studies, March 2010

[8] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War*, New York, 2004, p. 268

[9] See http://ddos.arbornetworks.com/2012/02/ddos-tools/ for a detailed analysis

[10] http://ww.prolexic.com/l/9892/2012-02-01/2f2r2 accessed for free after registration

[11] *Ahmadinejad: Iran's nuclear program hit by sabotage,* Washington Post, 29 November 2010
accessed via http://wapo.st/fwYR24

[12] Programmable Logic Controllers

[13] A detailed analysis in Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.4*., Symantec Corporation, February 2011 accessed via http://bit.ly/tdKDk3

[14] A phrase often used to describe Stuxnet by Ralph Langer; see http://bit.ly/dNSDJA

[15] Flaws and loopholes in the software that bypass security measures, not known by designers

[16] For instance the Cyber Shockwave exercise in the US, which painted a grim picture of a nation in chaos with the entire eastern coastline power grid down, http://bit.ly/dAKV9N

[17] Virtual Private Networks

—

*Written by: Damian Struglinski*

*Written at: King's College University*
*Written for: Dr Thomas Rid and TA Eduardo Peris Deprez*
*Date written: Feb 2012*