How Seriously Should the Threat of Cyber Warfare be Taken?

https://www.e-ir.info/2014/01/17/how-seriously-should-the-threat-of-cyber-warfare-be-taken/

PHILIP SMITH, JAN 17 2014

Cyber warfare is very much a contentious issue. To briefly illustrate this, in 1993, John Arquilla and David Ronfeldt wrote an article entitled “Cyber War is Coming!” (1997) whilst, more recently, Thomas Rid wrote an article entitled “Cyber War Will Not Take Place” (2012). During this time, a cyber attack actually managed to take control of physical infrastructure and disrupt Iranian nuclear ambitions whilst the cyber domain allowed for the unstoppable publication of hundreds of thousands of secret diplomatic cables and war logs, referring here to the WikiLeaks fiasco. The fact of the matter is that cyber-attacks happen, cyber espionage is rife, and has been since the early 21st century, along with all sorts of other politically and financially motivated illegal or malevolent cyber activity.

The main focus of this essay is whether the world is in the midst of a cyber war. The essay argues that both those who think cyber warfare is a threat to international security and those, like Thomas Rid, who feel that cyber war has not and will not take place are to a large extent both right and wrong. To think that the world is in a full-blown cyber war serves to confuse the definition of warfare and ignores more pressing security dilemmas, whilst to completely dismiss the phenomenon risks ignoring the issue of cyber security itself.

This essay will first attempt the difficult task of defining the term “cyber warfare” and will show that cyber security is currently a bigger issue for international security than the limited spectrum of cyber warfare. As the essay will demonstrate, using the term “warfare” narrows down issues within the cyber domain, which risks overlooking the threat posed to international security from non-state entities in cyberspace. Also, the term “warfare” may not even be accurate to describe conflict between states within cyberspace. Following this, the essay puts the issue into context by outlining how pervasive politically motivated cyber activity has been over the last 20 years, which will also demonstrate that the issue is, perhaps, not as new as one would initially think. Following this, the essay outlines some of the most prominent examples of cyber-attacks, in order to illustrate the seriousness of the threat and determine whether it is accurate to describe such incidents as cyber warfare. Finally, the essay illustrates the seriousness of the threat posed by some of the most sophisticated cyber-attacks, specifically referring to the Stuxnet attack on Iranian nuclear facilities, and demonstrates, more explicitly, that policy makers and researchers should take the treat from the cyber domain seriously, because the tools used to carry out cyber-attacks are available to all internet users.

As a term on its own, cyber is fairly straight-forward to define. Joseph S. Nye (2011) offers a useful definition: “cyber is a prefix standing for computer and electromagnetic spectrum related activities” (Nye, 2011, p. 19). It includes the physical and digital networks of networks that make up the internet and the world wide web, but also other communication technologies and infrastructure such as “mobile communications, fiber optic cables, and space based communications” such as GPS (Global Positioning System) (Nye, 2011, p. 19). Complexities arise, however, when the term warfare is used in conjunction with cyber. Immediately what comes to mind when attempting to define cyber warfare is that it must involve acts of war against a state using ICTs. But within the literature surrounding this area, policy makers and researchers clearly use the term to describe acts that are not war-like.

For instance, Jeffrey Carr (2011) describes Magomed Yevloev, who died in 2008, as a casualty of cyber warfare (Carr, 2010, p. 1). Yevloev set up an anti-Kremlin website and was arrested and “accidently” killed whilst he was

being transported by police (Carr, 2010, p. 1). Carr does acknowledge the ambiguities in defining cyber warfare, and the above example illustrates the main issue with the term—can we really consider the act of creating a website or taking websites temporarily offline as acts of war? This is not to say that they are not politically motivated cyber acts. Perhaps Carl von Clausewitz's traditional concept of war will help illuminate the issue.

According to Thomas Rid (2012), cyber war will not take place; instead, any political cyber-attacks that have, or will take place in the future, will be nothing more than "sophisticated versions of activities that are as old as warfare itself: subversion, sabotage and espionage" (Rid, 2012, p. 6). Based on Clausewitz's classic interpretation of what war is, Rid concludes that no act of cyber warfare meets all three of Clausewitz's criterion—these being violent, instrumental, and political (Rid, 2012, pp. 7-10). Certainly, thus far, there is no recorded cyber-attack that has been violent, instrumental, and political at the same time, which according to Rid, is the point of Clausewitz's definition of warfare (Rid, 2012, pp. 7-10). With relative certainty, there has been no instance of a cyber-attack ever ending in violence, although, as the essay shows, cyber attacks have been utilised alongside military excursions.

Before moving further, for the context of this essay, "cyber warfare" relegates to inter-state military affairs. Although the essay acknowledges that authors such as Jeffrey Carr, John Arquilla, and David Ronfeldt use terms like "cyber warfare," "netwar," and "information war" almost interchangeably but, throughout much of the literature, there seems to be little attention in defining terms in this area, and when there is attention to definition, sufficient conclusions are rarely drawn (Arquilla and Ronfeldt 1997, 27). However, as mentioned in the introduction, this does not mean that the broader issue of cyber-attacks and cyber security cannot be discussed because it may confuse the debate. On the contrary, the essay focuses simply on cyber-security in all its forms. With regard to what is to be secured in cyber-security, it is cyberspace and all that exists within the cyber domain, from control systems to sensitive information. Although Arquilla and Ronfeldt do attempt to distinguish between cyber war and netwar, stating that cyber war is a predominantly military concern whilst netwar involves social, economic and political cyber conflicts, they go on to state that "netwar represents a new entry on the spectrum of conflict that spans economic, political, and social as well as military forms of *war*" (Arquilla & Ronfeldt, 1997, p. 28). Again, there is a lack of distinguishing features between terms here.

As much one may consider cyber security and its related areas like cyber warfare and cyber espionage as new developments within security discourse, in fact, Information and Communication Technology (ICT) has been exploited for political purposes for at least the last two decades. There is a sufficient amount of evidence, for example, that China has been involved in the cyber espionage business for much of the last decade, particularly aimed at the United States (US), in order to circumvent the US's land, sea, and air superiority (Inkster, 2010, pp. 55-66). Even in the late 1990s, China was accused of infiltrating American nuclear facilities.

What is more, the Chinese government is not shy about revealing how important it feels the cyber domain is within its military establishment and has on many occasions publicised its development of a strong cyber army (Crosston, 2011, pp. 105-106). In fact, China is "unabashed in their virtual patriotism; honkers (hackers) espouse a philosophy that the best defence is a capable offense" (Crosston, 2011, pp. 105-106). China's cyber doctrine seems to be that not only should China protect its cyber *territory*, but also that it must respond to cyber-attacks in a dominant fashion, not necessarily in a proportionate fashion (Crosston, 2011, p. 106). Matthew D. Crosston (2011) concludes that this may mean that states like China and Russia consider themselves to be in a cyber-war with potential adversaries and rivals, but that this may be a one-way mind-set because weaker states, compared to say the US and the UK, clearly may be taking advantage of the more level playing field in cyberspace, where as a level playing field certainly does not exist within conventional military environments (Crosston, 2011, p. 106).

It is worth mentioning that the internet, itself, was initially created as a military application during the early stages of the Cold War (Castells, 2000, pp. 68-69). The first unofficial cyber-attack to have physical consequences happened in 1982 where it is alleged that the US Central Intelligence Agency (CIA) indirectly supplied the Soviet Union with control systems for a pipeline which contained malicious code (Rid, 2012, p. 10). Since the explosion of the internet in the 1990s, there has been an exponential growth in online criminal and politically motivated activity; wherever the internet has impacted areas of social, economic, and political life, the opportunity for criminal and political actors has increased. When Russia invaded Chechnya in 1997 to retain a "Moscow-friendly regime," both sides engaged in

what Jeffrey Carr (2010) describes as information operations, this mainly involved temporarily taking websites offline (Carr, 2010, p. 3). Herein lies one of the most prominent methods of political cyber-attacks—disabling websites usually by way of Distributed Denial of Service (DDoS) attacks.

The Russian Georgian War 2008 is the first example of large-scale cyber attacks being initiated along with a land, sea, and air invasion, which one would be forgiven for suggesting that a cyber-war was happening alongside conventional warfare. Again, the main focus of attack in this situation was to take official websites offline via DDoS attacks (Carr, 2010, p. 3). Perhaps, the most pervasive form of political activity in cyberspace is espionage. Carr agrees that cyber espionage is much more evident than cyber warfare, and he distinguishes between the two activities (Carr, 2010, p. 4). The media and the US do not apparently recognise the difference; for example,*the Financial Times* recently reported that China is stepping up its cyber spying doctrine and ran the article's title as, *"US says China is stepping up Cyber War"* (McGregor, 2013 Online). Here is an example of the issue over definitions; can one really consider taking websites offline as acts of war?

Although few would suggest that cyber warfare is an unrealistic scenario, the examples in this essay amount, at best, to politically motivated or criminal acts, not full scale acts of war. The Stuxnet event, however, has provided researchers in this area with a glimpse of what a full-scale cyber war may look like, with consequences that amount to traditional warfare. Many commentators have labelled the Stuxnet attack on Iranian nuclear centrifuges as the stuff of science fiction turning into reality—and for a good reason too. Stuxnet exemplified the first instance of a cyber-attack actually having a physical impact on critical infrastructure; it was significant because it is likely that Stuxnet put back Iran's alleged nuclear weapons ambitions by several years (Demchak & Dombrowski, 2011, pp. 32-61). On a more positive, or useful note, Stuxnet achieved what the international community had been trying to do for years. The question must come to mind: what if such an attack was aimed at critical national infrastructure in the West, infrastructure which millions of civilians rely upon for their wellbeing? The same question can be posed for military equipment, especially electronically controlled military equipment such as communications and drones.

The most interesting and, perhaps, worrying aspect of the Stuxnet event is the fact that the virus was not sophisticated, considering the amount of damage it caused. Many authors such as Sean Collins, Stephen McCombe, and Charles J. Dunlap, along with other commentators, not to mention the news media, have been quick to highlight the sophistication of the Stuxnet worm, claiming that only a state or official authority could have pulled off such an attack (Dunlap, 2011, p. 81; Collins & Stephen, 2012, p. 80; Cimbala, 2011, p. 120). The point the media and some commentators have not highlighted, however, is the fact that much of the component parts of Stuxnet are readily available at the criminal level of the cyber domain.

For example, the DNS (Domain Name System) based command and control network characteristic of Stuxnet, as well as other core technical features, "made it less stealthy than much of the more advanced malware that criminals use" (Farwell & Rohozinski, 2011, p. 25). According to James P. Farwell & Rafal Rohozinski (2011), the code contained in Stuxnet was nothing new, and again, much more sophisticated programs exist within criminal and hacking communities' online (Farwell & Rohozinski, 2011, p. 25). As much as Stuxnet is likely to have been state-sponsored, either by the Israelis, the Americans, or even the Russians or the Chinese, there are two key developments that need to be highlighted in isolation from any political discussion. First, science fiction is now a reality, and the physical environment is vulnerable to attack from within cyberspace. Second, Stuxnet exemplified how power in cyberspace is not weighted in the states favour and is, in fact, sporadically dispersed right down to the individual level. The essay will now briefly look at these two issues, infrastructure and power diffusion, as they highlight broader concerns for cyber security.

Clearly, if a state or non-state actor delivered a cyber attack towards critical infrastructure, which resulted in physical harm, death, or destruction on a large scale, then it would be reasonable to declare such an attack as an act of war. The Stuxnet attack on Iranian nuclear centrifuges has set a precedent for the future of cyber security. The doomsday scenario may be possible; Stuxnet, to a large extent, confirms this. With regards to national nuclear energy facilities, cyber security attacks have been taking place since 2002. Carr, for instance, provides five examples from 2002-2008 (Carr, 2010, pp. 10-11). The key issue with critical infrastructure today is the physical control systems that are increasingly being connected to the public Internet for remote control purposes among other useful means (Carr,

2010, pp. 8-11). And, even if control systems run on separate networks external to the public Internet, they are still just as vulnerable to cyber attacks.

As it turns out, the Iranian nuclear facility at Natanz, which was the main target of the Stuxnet worm, was "air-gapped; in other words, the centrifuges were not connected to the public internet" (Farwell & Rohozinski, 2011, p. 24). The developed world has come to rely upon ICTs, critical infrastructure such as water, gas, electric, and energy facilities, telecommunications, public transportation, public health facilities, national economies, and the global economy "have become reliant on software, computers and networks" (Edward, 2011, p. 1). When discussing cyber warfare or cyber security, the systems that control national infrastructure are absolutely key to understanding how serious the threat is. Building up traffic on a website and temporarily shutting it down through a DDoS attack is one thing, but manipulating train signalling or nuclear energy reactors is paramount to an act of terrorism, which could, in a worst case scenario, result in injury or loss of life.

Warfare is a policy area which has traditionally been monopolised by states; the cost of military resources imposes a high barrier to entry and thus makes it possible for states to dominate this realm (Nye, 2011, pp. 19-20). However, power in the 21st century is being diffused much more sporadically, and nowhere is this truer than within the cyber domain, specifically the Internet. If the power of the Nation-State has been challenged by non-state entities since the 1960s with the rise of the Multi-National Corporations and financial markets, cyberspace is likely to take this to a whole new level. The costs for non-state entities to participate in cyberspace, compared to land, sea, and air, are virtually zero (Nye, 2011, pp. 19-20). The nuance of this situation lies in the power that ordinary individuals have. For examples, see the events surrounding the WikiLeaks controversy, the use of social media in the Arab Spring, and the activities of hacktivists (Howard & Hussain, 2011; Bellia, 2012, pp. 1472-1476; Lunghi & Wheeler, 2012, pp. 32-39).

The Internet has grown and invaded all aspects of social, economic, and political life at an exponential rate, and it has simply been too quick to keep up with as far as security is concerned. This is due to not only the speed by which the internet has been rolled out into the public, but also because governments have had little influence over its development, as it has been primarily market driven (Castells, 2000, p. 69). The developed world may now have created an undesirable situation whereby everyone is so dependent on ICT whilst simultaneously cyberspace is very exposed and vulnerable to malevolent behaviour.

Although warfare is still largely dominated by land, sea, and air, and strategists, academics, and policymakers clearly understand these environments—i.e. what tools are used in these military environments and who the players are, usually states and non-state actors such as terrorists, paramilitary groups, and guerrilla fighters—cyberspace is completely different. The cyber domain is, in fact, primarily made up of civilians, or *netizens*. Because of how diverse cyberspace is, discussing cyber-war is limited with national interest dominating the agenda, and as military affairs are still dominated by physical military power, cyber warfare only serves to ignore the greater security concern, which is protecting the physical and digital infrastructure itself.

At the moment, cyber warfare is also narrow with regard to what actors are under discussion at any one time, usually between two states like that of the US and China. But the cyber domain is a truly global and transnational phenomenon; it is a borderless world where jurisdictions do not play an important role as much as they do in the physical world. The point is that security concerns for cyberspace go beyond military affairs. For instance, in the last three to four years, the world has seen much more activity from individuals disrupting the cyber domain than from states, or at least the activity of individuals over states has been more broadly publicised. The well-known example is WikiLeaks taking the global media spotlight for virtually most of 2010.

Furthermore, cyber crime is also much more pervasive and damaging than cyber reconnaissance missions by China, for example. It may well be too early to determine if the world is amidst a full cyber warfare situation, but from reading the literature in this area, it would seem that the world has not reached that point yet. As a result, some points for deliberation in policy circles and research environments ought to focus on possible outcomes of cyber-attacks more broadly, not just concerning cyber warfare between states and how society deals with, not necessarily doomsday scenarios, but certainly undesirable outcomes—which this essay leaves unchecked—that could have serious consequences for the daily running of globalised institutions such as the global economy and national and

international communications.

Whether the threat of cyber warfare should be taken seriously is difficult to answer. Still, cyber security ought to be taken seriously, as cyber attacks have been demonstrated to be a widespread problem. However, one must also bear in mind that no state has officially declared a cyber war—yet. Also, when war is declared, officials do not use the terms *land war* or *sea war*, but rather declare war in all its variants. During times of conflict along land, sea, and air warfare, cyberspace may simply become another environment to conduct military activity, without formal cyber warfare being declared.

Bibliography

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is Coming! *RAND Corporation*, 23-39. Available from: http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [Accessed April 2013]

Bellia, P. L. (2012). WikiLeaks and the Institutional Framework for National Security Defences. *The Yale Law Journal*, 1450-1526. Available from: http://www.yalelawjournal.org/images/pdfs/1067.pdf [Accessed on: 23 March 2013]

Carr, J. (2010). *Inside Cyber Warfare .* Beijing : O'Reilly.

Castells, M. (2000). *The Rise of the Network Society.* Oxford: Blackwell Publishers.

Cimbala, S. J. (2011). Nuclear Crisis Management and "Cyberwar" Phishing for Trouble? *Strategic Studies Quarterly, 5:1*, 117-131. Available from: http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf [Accessed: April 2013]

Collins, S., & Stephen, M. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism, 7:1*, 80-91. Available from: http://www.tandfonline.com/doi/abs/10.1080/18335330.2012.653198#.UYl0lLWRdqU [Accessed on 23 April 2013]

Crosston, M. D. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. *Stratigic Studies Quarterly, 5:1*, 100-116 Available from: http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf [Accessed: April 2013].

Demchak, C. C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian Age. *Stratigic Studies Quarterly, 5:1*, 32-61. Available from: http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf [Accessed: April 2013]

Dunlap, C. J. (2011). Perspectives for Cyber Strategists on Law for Cyberwar. *Stratigic Studies Quarterly, 5:1*, 81-99. Available from: http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf [Accessed: April 2013]

Edward, A. G. (2011). *Cyber attacks: protecting national infrastructure.* Oxford: Butterworth-Heinemann.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy, 53:1*, 23-40. http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586#.UYl0ErWRdqU [Accessed on 06 April 2013]

Howard, P. N., & Hussain, M. M. (2011). Opening Closed Regimes: What was the role of Social Media During the Arab Spring? *Project on Information Technology and Political Islam*, 1-30. Available from: http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf [Accessed on: 23 March 2013]

Inkster, N. (2010). China in Cyberspace. *Survival: Global Politics and Strategy*, 55-56. Available from: http://www.tandfonline.com/doi/abs/10.1080/00396338.2010.506820#.UYlzyLWRdqU [Accessed on 24 April 2013]

Lunghi, A., & Wheeler, S. (2012). All the memes of production, Deterritorial Support Group. In A. Lunghi, & S. Wheeler, *Occupy Everything: Reflections on why it's kicking off everywhere* (pp. 32-39). New York : Minor Compositions.

McGregor, R. (2013 Online, May 6). US says China is stepping up cyber war. *Financial Times*. Available from: http://www.ft.com/cms/s/0/41f930e6-b69a-11e2-93ba-00144feabdc0.html#axzz2SYbNqyfV [Accessed on 06 May 2013]

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly 5:1*, 18-38. Available from: http://www.au.af.mil/au/ssq/2011/winter/nye.pdf [Accessed: April 2013]

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35:1*, 5-32. Available from: http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939?journalCode=fjss20#.UYlzELWRdqU [Accessed on 23 April 2013]

—

Written by: Philip Smith
Written at: Staffordshire University
Written for: Dr. S. Bali
Date written: May 2013