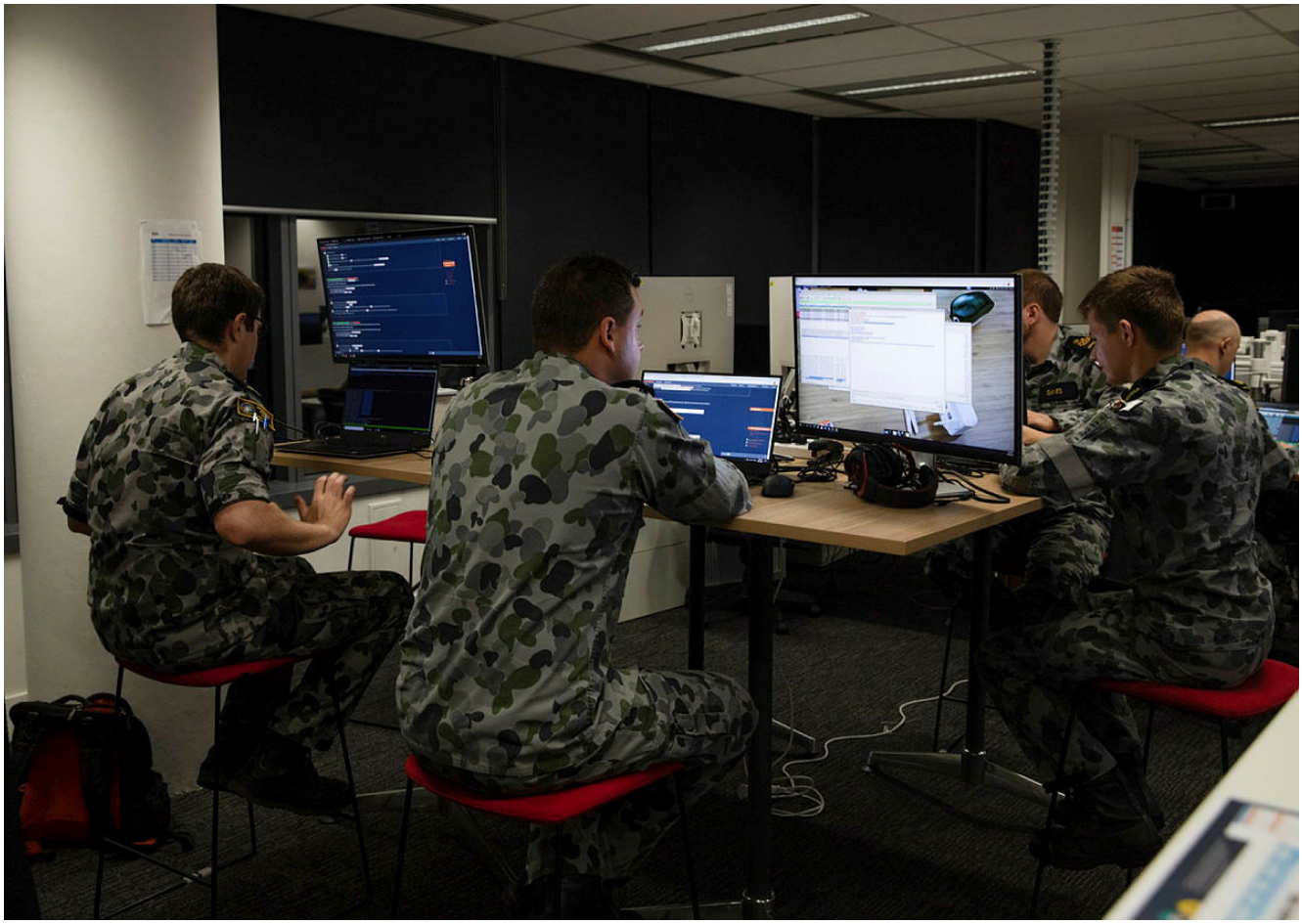
Issue: 38 | 2021

Can a cyber-operation be considered an act of war?

LEUT Max Westwood

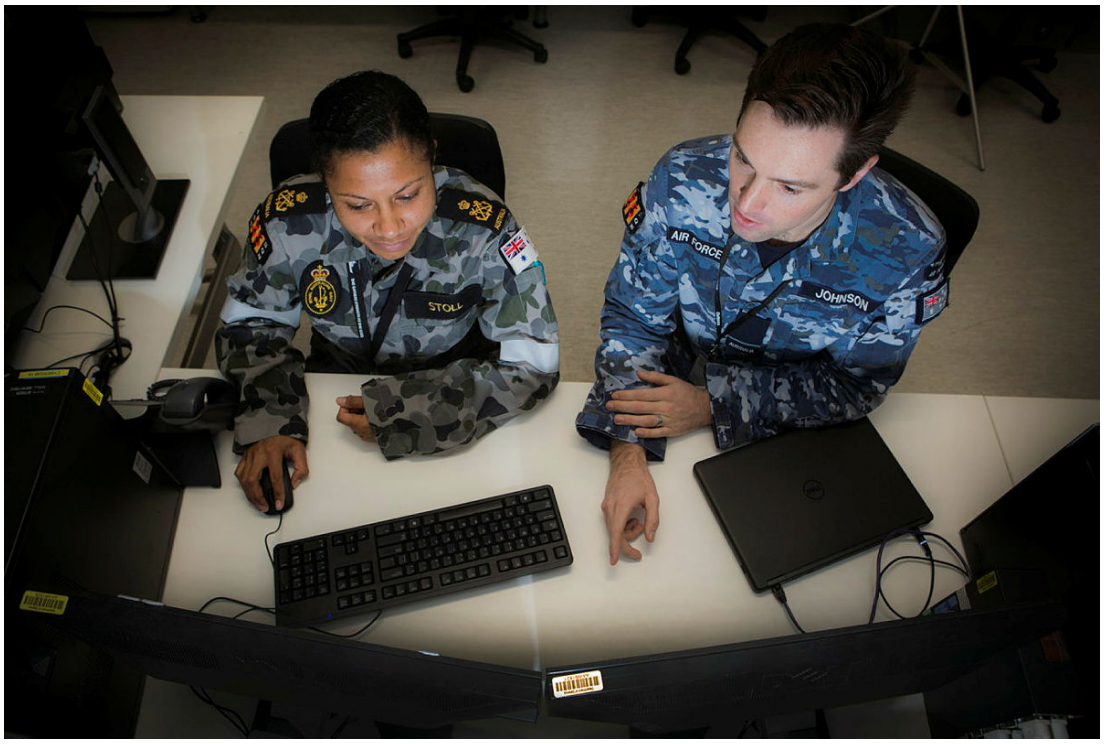
Military cyber operations take many guises and in the operational domain remain shrouded in extreme secrecy. As defined by the United States Department of Defense (DoD) Law of War Manual (2015) cyber operations employ "cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." Examples of military cyber operations include destruction, manipulation, or denial of information, computer networks or hardware. Cyber operations include actions usually resident within the intelligence community such as espionage, sabotage and subversion. Cyber operations do not include kinetic attacks against the above targets, as they are normally considered legitimate objectives for traditional military action.

The potential for military cyber operations to be declared an act of war has been a topic of debate for over 20 years. Scholars writing on the topic generally fall into one of two camps. Those who follow the classic definition of war, as defined by Clausewitz assert that war 'must be or have the potential to be violent, it must be instrumental in achieving an end state and it must be politically motivated and attributable'. Following this rigid definition, it is easy to assert that cyberwar will never take place, as cyber operations by their nature are non-violent and clandestine, targeting information and information systems rather than individual units. The other side of the debate argues that while war has legal grounds and a basis in law, not every act of war follows these laws; and indeed, a trigger for war between nations may be as simple as a rouge pig in a potato field. The DoD (2015) notes that 'war' (and thus an act of war) may encompass a plethora of situations that a state may find its self in, including armed conflict, warlike actions or hostilities, with a single condition that all of the above will be an act of force to assert a political will. For this paper, these terms will therefore be used interchangeably. Through this paper, I will present the argument that cyber operations do have the capacity to be an act of force for political will and therefore an act of war. In doing this I will compare high profile cyber operations to analogous kinetic operations that could fit the DoD (2015) definition of war.



Personnel from the Fleet Cyber Unit compete in the NetWars International Services Cup at Defence Plaza in Sydney. Photographer: LSIS Ryan Tascas.

Stuxnet is perhaps the most notorious of all cyber-attacks deployed to date. While its exact origins are cause for much debate in the cybersecurity community, the intentions of the malware have become abundantly clear. Stuxnet was a highly complex piece of malware with several features which at the time had not been seen by the cybersecurity community. Its ability to spread, hide its intentions and breach air gaps designed to protect sensitive networks made the worm extremely dangerous. Stuxnet was released in 2009 and deliberately targeted uranium enrichment centrifuges at Natanz, Iran. The worm altered code in programmable logic controllers (PLC) controlling the centrifuges, causing them to spin at higher speeds than they were designed to, leading to significant damage. The malware also included code designed to hide the actual speed and thus hide the presence of the malware within the system. Stuxnet used stolen digital certificates to mask its illegitimacy and contained a code for termination of operation on a specific date. Crucially, it also contained code that would limit any collateral damage. The worm was highly complex and shifted the bar for cybersecurity requirements of vulnerable and potentially dangerous systems, such as nuclear facilities worldwide.



Communications Information Specialist, Petty Officer Talei Stoll (left) and Intelligence Officer, Flying Officer Phillip Johnson, discuss Information Assurance procedures within No 462 Squadron located in the Edinburgh Defence Precinct, South Australia. Photographer: CPL Craig Barrett.

The political reaction from the international community to Stuxnet has been surprisingly benign. The attack cause damage to over 1000 centrifuges and had the potential to cause civilian casualties, and yet, Iran as the victim, and all other cyber-enabled states have been reluctant to classify the operation as an act of war. DoD (2015) quotes United Nations Article 2(4) saying that:

> …if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad Bellum*, then such cyber operations would likely also be regarded as a use of force.

DoD (2015) goes further, stating that should the United States (US) consider a cyber-attack as the illegal use of force it will respond with armed attack and has no legal requirement to respond to a cyber-attack with another cyber-attack. It is clear from this that the US at least considers the threat of force in the cyber domain as genuine as the threat of force in the physical domain.

The International Court of Justice has adopted a doctrine commonly known as Schmitt's analysis that is used to determine if an action constitutes a use of force. Schmitt's analysis uses seven

factors to subjectively guide a state to determine whether or not a cyber-attack meets the definition. Applying this analysis to Stuxnet it can be argued that the deployment of the worm constituted an illegal use of force and is therefore subject to retaliation by armed attacked. This retaliation never came. It is postulated that the major powers in cyberspace have deliberately remained silent on the effect of Stuxnet in hopes of pushing the threshold of allowable cyber operations. It is difficult to believe that had Natanz been subject to a kinetic attack (which would have been illegal under the Geneva Convention) that there would have been no repercussions for the perpetrators.

While there is a surprising abundance of information on Stuxnet there is very little information regarding the cold war era cyber-attack on the Trans-Siberian natural gas pipeline. The publically available information has been gleaned from an insider whistleblower and although confirmed by the Central Intelligence Agency in 2004 is very scarce. The Siberian Pipeline attack shares many similarities with Stuxnet, in that it targeted control sub-systems within a critical civilian infrastructure. US government hackers deployed the malware targeting systems controlling the operating pressure of the pipeline. The malware attacked a range of sub-systems including supervisory control and data acquisition systems, distributed control systems and PLCs. Unlike Stuxnet, the Siberian pipeline malware contained no termination code or collateral damage limiting code. The effect of this is that the malware was essentially deployed and left to run under its course. The malware functioned as intended, the PLCs controlling pressure within the pipeline malfunctioned allowing pressure to build leading to the eventual explosion. This attack certainly had kinetic effects similar to those of traditional warfare.

R-L: Royal Australian Navy sailor Leading Seaman Combat Systems Operator Travis Onley shows Royal Australian Navy Chaplain Franco Siani where to find the new podcasts on Navy history. Photographer: POIS Yuri Ramsey.

This attack again could be considered to meet the definition of an act of force using the Schmitt analysis. The victim state (The United Soviet Socialist Republic (USSR)) initially laid blame on the US while the US denied any involvement. Later the USSR denied that such an explosion had even occurred. The Siberian pipeline explosion is an example of a cyber-attack with physical consequences analogous to those of a kinetic attack. Because of this, it is safe to assume that by DoD (2015) this kind of action would trigger an armed response from the US. However, due to the un-attributable nature of the attack, like Stuxnet, there was no retaliation.

Pipeline sabotage costs the economy of some nations billions of USD a year. Ease of access to pipelines and relative ease of extraction have generated enormous profits for criminal organisations on the black market. It is estimated that pipeline sabotage costs the Nigerian government 15 billion USD per year. Because of this, armed military personnel are deployed to protect the pipelines running through the country. This situation is comparable (though more ongoing) to the Siberian pipeline attack. The key difference being that in Nigeria there is a physical target to protect against; this has subsequently attracted an armed response by the Nigerian government.

The Siberian pipeline attacks and Stuxnet both manifested in the physical domain and both meet the Schmitt analysis conditions to be classed as a use of force. Is it possible for an operation that remains purely in cyberspace to be classed as an act of war?

In 2007 several websites owned by the Estonian government, as well as private companies fell victim to a distributed denial of service (DDOS) attack perpetrated by entities within Russia. DDOS attacks, as their name suggests, aim to disrupt service or access to a particular website. This is achieved by flooding the target with traffic far above what it was designed to support. DDOS attacks utilise multiple computers, often without the owner's knowledge (botnets), and multiple internet protocol addresses. This makes countering or attributing the attack particularly difficult. It is theorised that the initial impetus for the attacks was the removal of a Russian Military memorial statue before Victory in Europe celebrations in the Estonian city of Tallinn. This action triggered demonstrations both in the physical domain and cyberspace, commencing the day after the statue was removed and continuing for three weeks. DoD (2015) clearly states that disrupting acts such as those discussed above will not trigger an armed response. It specifically mentions that brief disruption of services and defacement of government websites do not constitute an attack under the Law of War.

Following the Estonian attack, Georgia was also a victim of a DDOS attack. The attack commenced in August 2008 and again targeted government-owned websites. 24 hours after the first attack Russian forces moved into Georgia. This mobilisation of traditional military forces following a direct cyber-attack is described in the literature as the first example of a military cyber operation complementing a traditional military manoeuvre. Unlike the above examples, this attack was a precursor to physical war and the Russian occupation of South Ossetia. Could this then qualify the action as an act of war, given that Russia had intentions of engaging in a traditional war when it launched the attacks? Legally, no. The use of DDOS attacks in this way can be seen as analogous to physical instances of espionage, psychological operations or sabotage which often precede large scale mobilisation of military forces. While not an act of war in themselves, these operations are often undertaken before traditional military campaigns to increase the advantage one side may have over the other by decreasing an opposing forces appetite for war.

Cyber operations are a key part of military operations in the 21st century. Cyber operations have the potential to generate very real effects in the physical domain and as such should, given the appropriate analysis, be considered acts of war in the traditional sense. Despite this, and despite what the DoD (2015) indicates it seems that many countries are unwilling to accept cyber operations as acts of war and are unwilling to retaliate with traditional kinetic attacks. The world of military cyber operations, as stated previously is largely classified with only glimpses available to the general public for analysis. Perhaps the examples above did draw retaliation of the victim states and it was simply unreported at the unclassified level. The literature suggests that states are unwilling to define cyber operations as acts of war in the hopes of shifting the accepted threshold further and thereby allowing their acts of cyber sabotage or espionage to continue unmolested and unquestioned.

While cyber operations, in general, are not regarded as acts of war in and of themselves, it is clear that they have the potential to complement traditional warfare as we have seen in Georgia. The psychological effect of a DDOS attack on a population can reduce the appetite for war significantly and provide an advantage to a military that can effectively deploy them. Ultimately though, an act of war, use of force, warlike action, or hostile act are in the eye of the states involved: defined by international law and interpreted as required by states to meet their ends. In the end, if a war can be fought over a pig in a potato field it can be fought over virtually anything.

Reference list

Bawany, Z & Shamsi, J & Slah, K 2017, 'DDoS attack detection and mitigations using SDN: methods, practices and solutions', *Arab Journal of Science and Engineering,* vol. 42, pp 425-441.

Clausewitz, C. V, Howard, M, Paret, P, & Brodie, B 1984, *On War.* 18th edn, Princeton, NJ, Princeton University Press.

Department of Defense 2015, *Department of Defense Law of War Manual,* DoD, Washington.

Dickman, F 2009, 'Hacking the industrial SCADA network', *Pipeline & Gas Journal,* Nov 2009; 236, 11, pp 77-79.

Fidler, D 2011, 'Was Stuxnet and act of War? Decoding a Cyberattack', *Privacy Interests,* July-August 2011, pp, 56-59.

Gordon, L 2015, 'From imbroglio to Pig War: The San Juan Island dispute, 1853-71, in History and Memory', *BC Studies*, Summer 2015, Issue 186, pp.73-93.

Keely, D 2011, *Cyber attack! Crime or act of war?,* US Army War College, Carlisle Barracks, PA

Onuoha, F 2008, 'Oil pipeline sabotage in Nigeria: Dimensions, actors and implications for national security', *African Security Review*, vol, 17 no, 3, pp, 99-115.

Rid, T 2012, 'Cyber war will not take place', *Journal of Strategic Studies*, Vol.35 no, 1, pp, 5-32

Sagers, C 2011, 'The terrifying progeny of Stuxnet', *Diplomatic Courier,* Fall 2011, pp, 78-79.

Shakarian, P 2011, 'The 2008 Russian cyber campaign against Georgia', *Military Review,* Nov-Dec 2011, pp, 64-68.