doi:10.1093/jcsl/krs017

Cyber Security without Cyber War

Mary Ellen O'Connell*

Abstract

Which government agency should have primary responsibility for the Internet? The USA seems to have decided this question in favour of the military—the US military today has the largest concentration of expertise and legal authority with respect to cyberspace. Those in the legal community who support this development are divided as to the appropriate legal rules to guide the military in its oversight of the Internet. Specialists on the international law on the use of force argue that with analogy and interpretation, current international law can be applied in a way that allows great freedom without sending the message that the USA is acting lawlessly when it comes to the Internet. Others reject this argument as unnecessary and potentially too restrictive. The USA need not observe international law rules, especially not with respect to the Internet. The way forward is to follow the Cold War strategy of threatening enemies with overwhelming force and preparing to act on these threats. This article also questions the application of international law on the use of force to the Internet. Rather than rejecting international law in general, however, the thesis here is that international law rules governing economic activity and communications are the relevant ones for activity on the Internet. Moving away from military analogy in general and Cold War deterrence in particular, will result in the identification and application of rules with a far better chance of keeping the Internet open and safer for all.

1. Introduction

'Cyber' is one of the most frequently used terms in international security discussions today. It is certainly a word of increasing importance in the international lawyer's lexicon. It is not a new term in international law. International lawyers have been discussing computers and the law governing their use for several decades.[1] For specialists in the area of international law on the use of

* Robert and Marion Short Chair in Law and Research Professor of International Dispute Resolution—Kroc Institute, University of Notre Dame, Notre Dame, IN, USA. Email: MaryEllenOConnell@nd.edu. With thanks for research assistance to Cate Behles, Max Gaston, and Conor McGuinness.

1 Scholarly articles on the international law of cyberspace began to appear in the mid-1990s. These would, of course, have reflected developments and discussions of the previous years. See, eg, A Mefford, 'Lex Informatica: Foundations of Law on the Internet' (1997/1998) 5 Ind J Global Legal Studies 211 and DR Johnson and D Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48 Stanford L Rev 1367.

force, however, certain developments since at least 2007 have pushed the term and what it stands for to a top position on their agendas.[2] Within the broader discussion, the key issue is how to achieve security on the Internet. Governments, organizations, and commercial interests want people to have access to the Internet and all that it offers but not to be harmed by it. Achieving security is, in turn, leading to the question of how to characterize the Internet under international law. It could be characterized primarily as a sphere of economic and communication activity where civil law enforcement officials have primary jurisdiction. The Internet could, alternatively, be characterized as primarily under the jurisdiction of military defence authorities.

In 2007, Estonia experienced extensive computer hacking attacks that lasted several weeks.[3] Since then, support has been growing to give priority to military solutions to cyber security concerns. Soon after the attacks on Estonia, NATO[4] began developing policies and capacity aimed at cyber security.[5] In 2008, during the brief Georgia–Russia War over South Ossetia, Georgia experienced cyber-attacks similar to those suffered by Estonia in the previous year.[6] In 2009, the USA began releasing a number of policies on cyber security that were predominantly military in orientation.[7] More tangibly, the USA announced in 2009 that it would establish Cyber Command as a subunit of Strategic Command, one of its nine combat commands, within the Department of Defense.[8] Also, in 2009, computer malware, known as the Stuxnet worm, was released apparently by one or more governments, most likely the USA and Israel, to slow the progress of Iran's nuclear program, a problem otherwise being addressed by the Security Council and through negotiations.[9] In 2010, commentators began to reference the Cold War security policy of threatening massive retaliation to achieve deterrence as a policy to

[2] See, eg, R Brust, 'Cyberattacks: Computer Warfare Looms as the Next Big Conflict in International Law' (1 May 2012) <http://www.abajournal.com/mobile/article/cyberattacks_computer_warfare_looms_as_next_big_conflict> (accessed 20 June 2012). See further R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' and N Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' in this volume.

[3] See s 2.A below and accompanying notes.

[4] The North Atlantic Treaty Organization was founded in 1949 for the collective self-defence of Western European states, the USA and Canada. See <www.nato.int> (accessed 20 June 2012).

[5] According to the NATO website: 'Cyber attacks continue to pose a real threat to NATO and cyber defence will continue to be a core capability of the Alliance.' <http://www.nato.int/cps/en/natolive/75747.htm> (accessed 20 June 2012).

[6] See s 2.B below and accompanying notes.

[7] See, eg, M Clayton, 'The New Cyber Arms Race' *Christian Science Monitor* (7 March 2011), <http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race> (accessed 20 June 2012). See also ns 51–53 and accompanying text.

[8] See n 51 and accompanying text.

[9] See s 2.C and accompanying notes.

apply by analogy to Internet security.[10] In 2011, the USA Congress began debating new legislation that would give even more authority to the Department of Defense for cyber security, at the expense of the Department of Homeland Security (DHS). [11]

Within the debate over security in cyberspace, it should be recognized as a preliminary matter that cyber space is international space. Activity in cyberspace and domestic legislation with respect to it must comply with the relevant international law. Some looking to the military to defend cyberspace are seeking to exclude considerations of international law either because they are international law sceptics in general or they believe international law cannot be applied to the Internet as a practical matter. Stewart Baker, a Washington DC lawyer who was an Assistant Secretary for Policy and Technology in the DHS in the Bush administration, dismisses international law in general and its role in cyber security in particular. In an online debate sponsored by the American Bar Association in 2012, he indicated scant regard for the use of international law 'norms' respecting cyberspace and went on to argue: 'Lawyers across the [US] government have raised so many show-stopping legal questions about cyberwar that they've left our military unable to fight, or even plan for, a war in cyberspace'.[12] In 2011, Baker voiced a similar position in the respected international affairs journal, *Foreign Policy*.[13]

Other scholars who apparently understand that international law is generally the relevant law for cyber security questions may still argue that it is difficult to fit cyber problems into the rules on international law with respect to the use of force.[14] Instead of concluding, therefore, that it is necessary to look at other

[10] See, eg, M McConnell, 'To Win the Cyber-War, Look to the Cold War' *Washington Post* (Washington, 28 February 2010) at B1. (The op-ed's online version has a different title: 'How to Win the Cyber War We Are Losing' <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR20100225024> (accessed 20 June 2012).) For a law journal article advocating a return to Cold War thinking about cyber security and international law, see M Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale J Intl L 421, eg at 425–26.

[11] See ns 55–59 and accompanying text.

[12] SA Baker and CJ Dunlap Jr, 'What is the Role of Lawyers in Cyberwarfare?' (1 May 2012) <http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare> (accessed 20 June 2012).

[13] Writing in a recent online edition of the main stream international affairs journal, *Foreign Policy*, Baker wrote that 'State Department and National Security Council lawyers are implementing an international cyber war strategy that relies on international law "norms" to restrict cyberwar.' S Baker, 'Denial of Service, Against Cyberwar with Arcane Rules and Regulations' *Foreign Policy* (30 September 2011) <http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service?hidecomments=yes> (accessed 20 June 2012).

[14] See, eg, Waxman, who takes issue with both Schmitt's attempt to devise criteria that could equate cyber attacks with the armed attack necessary to trigger UN Charter art 51 and Dinstein who is confident that the Internet can be regulated under existing weapons conventions and other rules. Waxman (n 10) fns 156–61 and accompanying text (Schmitt) and fn 64 and accompanying text (Dinstein), citing MN Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts

international rules, such as those on non-intervention, countermeasures, economic law, and the like, these scholars, advocate new interpretations of the rules on the use of force in order to have the right to respond to cyber problems with military force.[15]

Peter Singer, Noah Schachtman, John Mueller and other security analysts, however, argue that the threat of cyber-attacks has been blown out of proportion to the detriment of preventing the real challenges to cyber security: cybercrime and espionage.[16] Singer and Schachtman argue that rather than drawing from nuclear deterrence thinking, the better analogy is to maritime piracy.[17] Piracy is a costly and sometimes deadly problem, but is being addressed through law enforcement methods, which are sometimes carried out by the military, but the FBI and other national police agencies are active in the effort to stop Somali piracy. Another apt analogy is to the chemical sector. Chemicals are an indispensable part of everyday life in the 21st century, but chemicals can also be made into devastating weapons of mass destruction. To prevent this, the Chemical Weapons Convention prohibits the use and possession of chemical weapons.[18] The CWC is monitored by Organization for the Prohibition on Chemical Weapons (OPCW), as well as national defence ministries. Primary regulation and oversight of the chemical sector, however, is by civil authorities and such international organizations as the United Nations Environment Program.

This article discusses the growing emphasis on militarizing cyber security. The evidence shows that the USA, in particular, is building capacity and developing strategies that make the Department of Defense a major player in Internet use and protection. The concern with this development is that the Pentagon will conceive of cyber space as it does conventional space, with war fighting in mind. Yet, the international legal rules on the use of force, especially the rules on self-defence, raise important barriers to military solutions to cyber space problems. Indeed, the law of self-defence should have little bearing in discussions of

on a Normative Framework' (1999) 37 Colum J Transnatl L 885; Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 Intl Law Studies 99.

15 The very point of Waxman's article, for example, is to return to the advocacy of some scholars during the Cold War for expanded rights to use military force by resort to novel interpretations of the plain terms of the UN Charter and rules of customary international law. See Waxman (n 10) eg at 431.

16 P Singer and N Schachtman, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive' Brookings Institution (15 August 2011) <http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx> (accessed 20 June 2012); R Singel, White House Cyber Czar: 'There is No Cyberwar' *Wired Magazine* (4 March 2010).

17 ibid.

18 See the 1992 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (opened for signature 13 January 1993, entered into force 29 April 1997) 1974 UNTS 317 <www.opcw.org/chemical-weapons-convention> (accessed 20 June 2012). As of time of writing, the CWC had 188 state parties and over 70% of the world's chemical weapons stockpile had been destroyed.

cyber security. Even if some cyber incidents could fit a solid definition of what constitutes an armed attack, responding to such an attack will rarely be lawful or prudent if the response is a use of force. The emphasis, therefore, in terms of legal norms and commitment of resources should be in the non-military sphere.

In the USA and other States where the thinking is in conventional military terms respecting responses to cyber problems, the advocates of such thinking appear to be trapped by an ideology of militarism. The vast majority of cyber security incidents are carried out not by government-sponsored hackers causing deaths and brick and mortar destruction. The major challenge to Internet security is by private criminals interested in private gain. International law supports cyber security that is achieved through law enforcement cooperation, supported by shared legal norms governing the use of the Internet. Resources devoted to developing a comprehensive treaty on cyber security that de-militarizes cyberspace and emphasizes law enforcement cooperation, improved international governance, especially through the International Telecommunications Union, as well as good computer and network defences will go much farther than military force towards keeping the Internet open and available for peaceful communication and commerce.

2. Inventing a Cyber War Problem

Security concerns are as old as the Internet itself. Jeffrey Carr describes an organized attack by some 3000 Chinese hackers in 1998 on Indonesian government sites to protest anti-Chinese riots in the country.[19] Since then tens of thousands of attempts to hack into major computer networks belonging to defence ministries, banks, the media and the like are occurring daily. Most of these cyber intrusions have espionage or theft as the purpose and are typically categorized as 'computer network exploitation' or 'CNE'.[20] A smaller number have involved 'computer network attacks' or 'CNA'. The 2007 attacks on Estonia, NATO's response, and the attacks during the 2008 Russia-Georgia conflict are described below because they are regularly cited in military security discussions. These cases have undoubtedly influenced the turn to thinking about military solutions for cyberspace problems. A third CNA event, the use of the Stuxnet worm against Iran involved a destructive use of the Internet to address what had been approached as a diplomatic problem. The use of this malware

[19] J Carr, *Inside Cyberwarfare* (O'Reilly 2010) 2.

[20] For a helpful, general discussion of the current issues respecting cyber security, see Brookings Institution, 'The Cybersecurity Agenda: Policy Options and the Path Forward' (26 October 2011) <http://www.brookings.edu/topics/cybersecurity.aspx> (accessed 20 June 2012); Brookings Institution, 'Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch' (20 September 2011) <http://www.brookings.edu/topics/cybersecurity.aspx> (accessed 20 June 2012); SM Hersh, 'The Online Threat, Should We Be Worried About a Cyber War?' *New Yorker* (1 November 2010) 44.

indicates an interest by governments in developing cyber weapons. Additional evidence of the turn to militarization is found in developments in the USA, including the establishment of Cyber Command and the development of policies and legislation that emphasizes the military's role in cyber security.

A. Estonia and NATO

In response to the moving of a Soviet war memorial from the city of Tallinn in Estonia to its suburbs, hackers began attacking Estonian government websites through distributed denial of service (DDOS) attacks in April of 2007.[21] Seen as an affront to the memory of Soviet soldiers who died during the Second World War, the removal of the statue set off a series of riots within Estonia, while hackers attacked the government's websites by defacing them and redirecting users to images of Soviet soldiers.[22] These attacks lasted about a month. Attacks lasting several days were directed at Estonia's biggest bank as well as at several newspapers and reached the point of coming 'close to shutting down the country's digital infrastructure'.[23] Estonia's defence minister said the hacking had caused a national security situation and compared the attacks with the closing of all the country's ports.[24] Other officials have called the episode 'cyberwar'.[25]

Estonia has claimed that the Russian government instigated the attacks, while Russia has denied any involvement.[26] To support its charges, Estonia enlisted the aid of NATO, the EU, the USA and Israeli Internet experts to trace the attacks to their origin and to gather other information. However, despite the fact that a number of the computers initiating the attacks had Russian IP addresses, the hackers had hijacked computers around the globe to send the attacks. It remains uncertain from where exactly the attacks originated.[27] The Estonian experience raised serious questions about how governments can defend against cyber-attacks since governments do not control the Internet. Some argued that Estonia was attacked in a way that triggered the North Atlantic Treaty's Article 5. Article 5 commits NATO to respond to attacks on any member of the Alliance as permitted under the United Nations Charter provision in Article 51 for collective self-defence 'if an armed attack occurs'.[28]

[21] 'The Cyber Raiders Hitting Estonia' *BBC News* (17 May 2007) <http://news.bbc.co.uk/2/hi/europe/6665195.stm> (accessed 20 June 2012).

[22] 'Estonia Fines Man for Cyber War' *BBC News* (25 January 2008) <http://news.bbc.co.uk/2/hi/technology/7208511.stm> (accessed 20 June 2012).

[23] M Landler and J Markoff, 'Digital Fears Emerge After Data Siege in Estonia' *New York Times* (New York, 29 May 2007) <http://www.nytimes.com/2007/05/29/technology/29estonia.html?ref=estonia> (accessed 20 June 2012).

[24] ibid.

[25] ibid.

[26] ibid.

[27] J Davis, 'Hackers Take Down the Most Wired Country in Europe' *Wired Magazine* (21 August 2007) <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all> (accessed 20 June 2012).

[28] ibid.

NATO did not respond to the Estonia attacks with a counter-attack, but did establish an Internet defence facility in Estonia, called the Cooperative Cyber Defence Centre of Excellence (CCDCOE).[29] Estonia itself has created a volunteer unit of cyber-experts akin to the US National Guard and has become a leader in determining ways to defeat online attacks.

B. Georgia–Russia

The first known use of the Internet during a conventional armed conflict to interfere with civilian use of the Internet occurred in the 2008 conflict over the Georgian province of South Ossetia.[30] Georgia triggered the conflict by attacking Russian soldiers who were part of a peacekeeping contingent in South Ossetia under the terms of a Georgia–Russia treaty of 1991. In the night of 7–8 August, Georgia attacked, killing about a dozen Russian soldiers and wounding many others. Russia counter-attacked pushing to within 35 miles of the Georgian capital, Tbilisi. Georgia claimed that Russia initiated DDoS attacks against a number of Georgian websites, including government sites, media sites and commercial sites.[31] The computer attacks lasted nearly a month. The physical fighting had lasted about a week.

Under international law, Russian forces in South Ossetia would certainly have had the right to defend themselves personally from direct attack by Georgian forces. It is more questionable whether they had the right to defend their positions in South Ossetia since Georgia's attack clearly spelled the end of its consent to the 1991 treaty. On the other hand, Russian forces would arguably have a right to remain in the enclave until the treaty was terminated lawfully. The Russian move beyond South Ossetia into Georgia was excessive in relation to either the clearly lawful goal of immediate defence of self or even the more questionable goal of maintaining control of the enclave. Attacks on Georgian computer networks directly connected with its attacks on Russian troops would be typical of the type of objects that may be targeted during armed conflict hostilities under the law of armed conflict.

[29] J Benitz, 'Baltic States Urge NATO to Bolster Cyber-Defense' NATO Alliance (27 May 2011) <http://www.acus.org/natosource/baltic-states-urge-nato-bolster-cyber-defense> (accessed 20 June 2012).

[30] For details of the computer network attacks that occurred during the South Ossetia conflict, see S Watts, 'Combatant Status and Computer Network Attack' (2010) 50 Virginia J Intl L 391, 397–98.

[31] J Swaine, 'Georgia: Russia "conducting cyber war"' *The Telegraph* (London, 11 August 2008) <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> (accessed 20 June 2012). See also E Tikk and others, 'Cyber Attacks Against Georgia: Legal Lessons Identified' (Cooperative Cyber Defence Centre of Excellence 2008) 1, 4–15 at <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf> (accessed 20 June 2012).

Attacking non-military government, media and commercial sites are very difficult to justify under either the law regulating the conduct of armed conflict or the law on resort to armed force.[32]

C. Stuxnet

In 2009–10, a computer worm, dubbed Stuxnet (or Stutznet) attacked computers manufactured by Siemens and used in the Iranian nuclear program.[33] The worm is believed by experts to have been created by the USA with assistance from Israel and scientists at Siemens.[34] The effect of the worm in Iran was to cause centrifuges to turn far more rapidly than appropriate. In early 2011, officials in Israel and the USA announced that Iran's nuclear program had been set back 'by several years'.[35] The Stuxnet worm, however, affected computers in other countries as well, including India, Indonesia and Russia. Indeed, it is believed that 40% of the computers affected were outside Iran. Stuxnet is said to be 'the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units'.[36]

Ralph Langner, a German computer security expert, is convinced Stuxnet is a government-produced worm: 'This is not some hacker sitting in the basement of his parents' house. To me, it seems that the resources needed to stage this attack point to a nation state'.[37] In another interview, Langer added:

> Code analysis makes it clear that Stuxnet is not about sending a message or providing a concept. It is about destroying its targets with utmost determination in military style.... Stuxnet is the key for a very specific lock. In fact, there is only one lock in the world that it will open.... The whole attack is not at all about stealing data but about manipulation of a specific industrial process at a specific moment in time. This is not generic. It is about destroying that process.[38]

[32] See, generally, ME O'Connell, 'The Prohibition on the Use of Force' in C Henderson and N White (eds), *The Handbook of Conflict and Security Law* (forthcoming Edward Elgar Publishing); C Gray, *International Law and the Use of Force* (3rd edn, OUP 2008).

[33] J Markoff and DE Sanger, 'In a Computer Worm, a Possible Biblical Clue' *New York Times* (New York 30 September 2010).

[34] WJ Broad and others, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay' *New York Times* (New York, 15 January 2011).

[35] ibid.

[36] J Fildes, 'Stuxnet Work "Targeted high-value Iranian Assets"', *BBC News* (23 September 2010) <http://www.bbc.co.uk/news/technology-11388018> (accessed 20 June 2012).

[37] ibid.

[38] J Hilder, 'Computer Virus Used to Sabotage Iran's Nuclear Plan "Built by US and Israel"' *Australian* (27 January 2011).

D. Other Evidence of Militarization

NATO's CCDCOE facility in Estonia is part of the NATO military alliance's steadily increasing focus on cyber security. NATO has had cyber security on its agenda since the 2002 Prague Summit.[39] Since then, it has expanded its planning and capacity in the cyber security area, apparently assuming that it has a major role to play in cyber space. One NATO spokesman noted, '[i]t has become clear that the challenge we face has become quite significant and needs a more comprehensive approach. We need to be ahead of the bad guys; the threat can come from many sources: cybercrime, cyberterrorism or state activity'.[40] Suleyman Anil, Head of Cyber Defense at NATO explains that '[s]ince 2006, NATO has been running operational cyber defence capabilities and has established a good model in deployment and operating of cyber defence technologies and capabilities'.[41] Under the 2010 NATO Strategic Concept the Alliance commits to

> develop further [its] ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations....'[42]

It is fulfilling these commitments through the CCDCOE,[43] which 'conduct[s] research and training on cyber warfare';[44] the NATO Computer Incident Response Capability (NCIRC), which 'handles and reports cyber security incidents and disseminates important incident-related information to systems, security management and users';[45] and through the Cyber Defense Management

[39] 'NATO and Cyber Defence' NATO <http://www.nato.int/cps/en/SID-E61FF165-78BBC3C8/natolive/topics_78170.htm?> (accessed 20 June 2012).

[40] N Heath, 'NATO Creates Cyber-Defence Command' *ZD Net* (9 April 2008) <http://www.zdnet.co.uk/news/security-threats/2008/04/09/nato-creates-cyber-defence-command-39382597/> (accessed 20 June 2012).

[41] 'Working with the Private Sector to Deter Cyber Attacks' NATO (10 November 2011) <http://www.nato.int/cps/en/natolive/news_80764.htm> (accessed 20 June 2012).

[42] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization (19 November 2010) <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf> (accessed 20 June 2012) para 19.

[43] 'NATO Launches Cyber Defence Centre in Estonia' *Space Daily* (14 May 2008) <http://www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html> (accessed 20 June 2012).

[44] ibid.

[45] J Hunker, 'Cyber War and Cyber Power: Issues for NATO Doctrine' Research Division NATO Defence College, Working Paper No 62, 2010 <http://www.ndc.nato.int/research/series.php?icode=1> (accessed 20 June 2012) at 8.

Authority (CDMA), which 'has sole responsibility for coordinating cyber defence across the Alliance'.[46]

It is the view within NATO that '[g]overnments alone would not be able to respond to cyber threats. New and innovative cyber technologies are developed by the private sector. Sharing information and knowledge can (and should) be improved in this area and NATO is doing its part'.[47] Apparently, NATO will be putting ever greater emphasis on its role in cyber space as outlined in the June 2011 Policy on Cyber Defense.[48] NATO looks set to become the international organization with the most resources and authority devoted to cyber security, if it is not already.

Developments in the USA are following a similar path. While private business and civil agencies are the major players in cyber security, the Department of Defense is steadily taking the lead. In 2010, the Pentagon established Cyber Command. It is a subunit of Strategic Command, one of the nine combatant commands of the USA's Unified Command System.[49] In his announcement of the creation of Cyber Command, William Lynn said,

> Just as our military is prepared to respond to hostile acts on land, air and sea, we must be prepared to respond to hostile acts in cyberspace. Accordingly, the United States reserves the right, under the laws of armed conflict, to respond to serious cyber-attacks, with a proportional and justified military response, at the time and place of its choosing.[50]

Cyber Command has been given a wide mandate. It not only has responsibility for defending DOD information networks, it must 'prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries'.[51]

Singer and Schachtman believe that the DOD's cyber strategy is based on conceiving of cyber security in a way similar to the USA's Cold War strategy. They relate that the classified version of the cyber strategy presents

> a new doctrine of 'equivalence,' arguing that harmful action within the cyber domain can be met with parallel response in another domain. Swap in the 'conventional' and 'nuclear' for 'cyber' and 'kinetic' and the new

[46] ibid 8–9; see also 'NATO Launches Cyber Defence Centre in Estonia' (n 43).
[47] 'Working with the Private Sector to Deter Cyber Attacks' (n 41).
[48] ibid.
[49] 'US Department of Defense, Cyber Command Fact Sheet (21 May 2010) <http://www.stratcom.mil/factsheets/Cyber_Command/> (accessed 20 June 2012).
[50] W Lynn, Former Deputy Secretary of Defense, 'Announcement of the Department of Defense Cyberspace Strategy at the National Defense University' (14 July 2011) <http://www.pentagonchannel.mil/onestory_popup.aspx?pid=FttPuXny5i7D8p1hC0rgnXrveieDVeMW> (accessed 20 June 2012).
[51] ibid.

> doctrine is actually revealed to essentially be the old 1960s deterrence doctrine of 'flexible response,' where a conventional attack might be met with either a conventional and/or nuclear response. The Pentagon's Cyber Command and Beijing's People's Liberation Army's Third Army Department now fill in for the old Strategic Air Command and the Red Army's Strategic Rocket Forces.[52]

In another related development within the USA, in 2011–12, Congress began considering new legislation on cyber security.[53] One group in Congress prefers to keep the primary authority for cyber security in the DHS, but another group is adamant that the Pentagon take the lead.[54] Senator John McCain is one who objects to giving DHS more authority, preferring the emphasis to be with Cyber Command and the National Security Agency (NSA).[55] McCain has argued against turning DHS into a 'super regulator'. General Keith Alexander shares McCain's concern. General Alexander is, at time of writing, both the head of Cyber Command and the Director of the NSA.[56] McCain and Alexander point out that Cyber Command and the NSA already have greater technical expertise than DHS, and use this fact as an argument to continue to favour the military over DHS with resources and legal authority.[57]

Plainly some of the pressure to militarize cyber security is being driven by business concerns in the military security sector. Mike McConnell, for example, is a past director of the National Security Agency and is now an executive vice president of the private consulting firm, Booz Allen Hamilton. McConnell plainly has an interest in seeing that the Pentagon continues to need an extremely large budget. From that perspective, his op-ed on thinking about cyber security in terms of Cold War deterrence makes sense:

> The United States is fighting a cyber-war today, and we are losing. It's that simple.... What is the right strategy for this most modern of wars? Look to history. During the Cold War, when the United States faced an existential threat from the Soviet Union, we relied on deterrence to protect ourselves from nuclear attack. Later, as the East-West stalemate ended and nuclear weapons proliferated, some argued that preemption made more sense in an age of global terrorism. The cyber-war mirrors the

[52] Singer and Schachtman (n 16).

[53] T Carney, 'The Rise of the Cybersecurity Industrial Complex' *The Examiner* (22 April 2011) <http://washingtonexaminer.com/politics/2011/04/rise-cybersecurity-industrial-complex/113362> (accessed 20 June 2012).

[54] Hunton & Williams LLP, 'Senators Introduce Cybersecurity Act of 2012' Association of Corp Counsel (22 February 2012) <http://www.lexology.com/library/detail.aspx?g=d9fce919-5bc4-486b-a92a-685884ec9ea4> (accessed 20 June 2012).

[55] 'McCain Promises GOP Alternative to "Super Regulator" Cybersecurity Bill' The Daily Caller (20 February 2012) <http://dailycaller.com/2012/02/20/mccain-promises-gop-alternative-to-super-regulator-cybersecurity-bill/> (accessed 20 June 2012).

[56] ibid.

[57] ibid.

> nuclear challenge in terms of the potential economic and psychological effects. So, should our strategy be deterrence or preemption? The answer: both. Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace.[58]

Singer and Schachtman point to a similar perspective coming from other business sources: 'Even the network security firm McAfee is susceptible to such talk. "We believe we're seeing something a little like a cyber Cold War..." .'[59]

3. The Law Restricting Cyberwar

As already indicated at the outset of this article, the emphasis on cyber space as battle space is in tension with the international law governing the use of force. Some prefer to dismiss international law from the discussion altogether. Others do not exclude international law, but interpret it any way that it is in effect excluded. In May 2011, President Obama indicated that international law would play a role in US cyber security planning, indicating, however, that it would be international law as interpreted by those who advocate a broad—nearly unfettered—right of the USA to resort to force. In *International Strategy for Cyberspace*,[60] the White House announced:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an *inherent right to self-defense*, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.[61]

[58] McConnell (n 10).
[59] Singer and Schachtman (n 16).
[60] 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World' (May 2011) <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> (accessed 20 June 2012). (Emphasis added).
[61] ibid.

The reference to international law is admittedly constructive and even noteworthy given today's political climate where international law scepticism appears to be on the rise.[62] Yet, the paragraph's phrase 'inherent right to self-defence' signals adherence to a minority view of the relevant international law. This minority view countenances a reading of the United Nations Charter that side steps express restrictive terms for the purpose of justifying broader rights to use force than the Charter permits. While some might take comfort in the fact that at least the administration is citing international law in some guise, it should be recognized that in practice the administration has a poor record of adherence to even the minority view in its use of force for counter-terrorism. Indeed, its record of compliance with international law in military-security affairs in general is far from exemplary.[63] In the cyber area in particular, if the USA has released the Stuxnet virus, then the world already has an example of willingness to violate international law in cyberspace.

Even if the administration's record were better, even if it adhered to the mainstream position on the international law of self-defence, the relevance of this law to cyberspace is being exaggerated. When cyberspace is conceived of first and foremost as space for communications and economic activity, the international law on the use of force can be seen as largely irrelevant for cyber security. The relevant law is the law governing economic rights and non-intervention, not the law of self-defence. Recall the analogy above to chemical weapons. Yes, chemicals may be turned into a powerful weapon of mass destruction, which defence officials need to plan for, but the non-military sector is where most chemical use and regulation is found. The international community could not tolerate the immensely useful chemical sector also being part of the military sphere.

Part of the obstacle in persuading governments that the military paradigm is the wrong one for cyber security is the fact that most of the international law scholars working on cyber security questions from the early days of the Internet were in the military or had close ties to it. This is true of the first American authors on cyber security, Michael Schmitt, Walter Gary Sharp and George Walker. [64] After more than a decade of such analysis, few if any scholars publishing on international law and cyber security do so from a non-military

[62] See Baker (n 13); see also J Crawford, *Manley O Hudson Award Lecture* ASIL 2012 (on file with the author).

[63] Numerous examples come readily to mind: the continuing operation of the prison at Guantánamo Bay, Cuba; the continuing use of military commissions; the failure to enforce the Geneva Convention prohibition on torture, the failure to enforce the Convention Against Torture's obligations and the campaign of targeted killing far from zones of armed conflict hostilities, to name a few. See ME O'Connell, 'Adhering to Law and Values against Terrorism' (2012) Notre Dame J Intl & Comp Law (forthcoming).

[64] Schmitt (n 14).

perspective. Marco Roscini's 2010 article, 'World Wide Warfare—Jus Ad Bellum and the Use of Force', is a prominent example.[65]

This writing may well be hardening the view that cyber security is fundamentally military security. Approaching the question from a critical stance, however, reveals that the military security authors are relying on attenuated hypothetical cases, not the real world of cyber insecurity. The real world problems are crime and espionage. Stuxnet is a real world problem more obviously in the military defence category, but as will be explained below, Iran would not be able to meet several of the conditions of lawful resort to force in self-defence in the case of a response to Stuxnet. The Stuxnet example indicates that even advocates of a more relaxed reading of the international law on the use of force have difficulty showing how military force can be resorted to lawfully in response to cyber problems.

All writers on the use of force must start with Article 2(4) of the UN Charter as it is the general rule.[66] It generally prohibits the use of force except in the case of self-defence per Article 51 or Security Council authorization as per Articles 39–41.[67] Derek Bowett appears to have been the first to try to interpret the Charter as allowing the use of major military force against another State even in the absence of an armed attack. Writing in the wake of the 1956 Suez Crisis, he sought a justification for the Anglo-French–Israeli action that could not be found in prevailing interpretations of the UN Charter. States he asserted retained a right to act in self-defence consistently with the customary international law in place prior to the adoption of the Charter in 1945 as signalled by the term 'inherent right' in Article 51.[68] He dismissed Article 51's express condition that an

[65] M Roscini, 'World Wide Warfare—Jus Ad Bellum and the Use of Force' (2010) 14 Max Planck UN YBk 85. See also CJ Dunlap, Jr, 'Perspectives for Cyber Strategies on Law for Cyberwar' (Spring 2011) Strategic Studies Q 81, 81.

[66] See generally R Buchan, 'Cyber Attacks: Unlawful uses of Force or Prohibited Interventions?' in this volume.

[67] UN Charter Art 2(4): 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations'.
Article 39: 'the Security Council is given authority to 'determine the existence of any threat to the peace, breach of the peace, or act of aggression' and the responsibility to 'maintain or restore international peace'. It may do so by authorizing the use of force by member states'.
Article 51: 'Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.'

[68] D Bowett, *Self-Defence in International Law* (Manchester University Press 1958) 3, 184–85.

armed attack occurs by saying, 'there is no explanation of this curious proviso "if an armed attack occurs" '.[69] He then develops an argument for self-defence without an armed attack according to the 1841 correspondence over the sinking by British forces of an American ship called the *Caroline*. The correspondence confirmed that the customary international law of the time permitted the use of force in self-defence if the necessity was 'instant', 'overwhelming' and leaving 'no moment' for deliberation. Despite the clear deficiencies as a matter of legal analysis with Bowett's argument, it is still cited with impressive fidelity by a minority of scholars, mostly in the USA and UK.

Brownlie soon provided a point-by-point response to Bowett, inspiring the strict interpreters of the Charter ever since. Brownlie warned against the tendency by writers to claim justifications for the use of force found in the customary law prior to the 1920s. He singles out for particular criticism attempts to base rights of self-defence on the 1841 correspondence over the *Caroline*. He took a strict position on interpreting Article 51, ruling out resort to force in anticipatory self-defence or against actions not involving armed force. He points to the conditions on the exercise of self-defence beyond the Charter, namely, the principles of necessity and proportionality. He defended his strict stance saying, '[T]he dominant policy of the law and of the United Nations is to maintain international peace and to avoid creating possibilities of breaches of the peace, in the form of vague and extensive justifications for resort to force or otherwise.'[70]

The International Court of Justice in six cases relevant to the Charter rules on the use of force has supported Brownlie's understanding respecting interpretation. Not only must an armed attack or armed attack equivalent be in evidence to use military force in self-defence, the attack must be significant; it must be attributable to the state where the self-defence is being carried out; the use of force must be a last resort and must be likely to succeed in achieving defence, and must be proportional to the injury suffered.

Attempting to apply these conditions to cyber force actions is difficult, if not impossible—even for the followers of Bowett. First, in the three cases described earlier in the article, it is difficult to make the case that the computer network provocations amounted to an armed attack equivalent. No lives were lost directly. Damage to tangible objects occurred only in the case of the Stuxnet attack on Iran. This sort of damage does not meet the condition that an armed attack must be significant to trigger Article 51: 'The prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects would have been classified as an armed attack rather than a mere frontier incident had it been carried out by a regular armed forces.'[71] The ICJ made similar assessments of 'scale and

[69] ibid.

[70] I Brownlie, *International Law and the Use of Force by States* (OUP 1963) 428-36.

[71] *Military and Paramilitary Activities in and Against Nicaragua (Nicararagua v US)* [1986] ICJ Rep 14, 103–4 (the Nicaragua case).

effects' of violent action in the *Oil Platforms* case,[72] the *Wall* advisory opinion[73] and the *DRC v Uganda* case.[74] The Stuxnet attack while unlawful was not the equivalent of an Article 51 armed attack.

Second, attribution has not been affirmed at the international evidentiary standard in any of the three cases. State practice indicates the case for attribution would have to be made with clear and convincing evidence.[75] In the case of cyber-attacks generally, convincing evidence is hard to find:

> Given the anonymity of the technology involved, attribution of a cyber attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber attack to a specific server in another state, this can be an exceptionally time consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used these as 'zombies' in conducting attacks.[76]

We have good information that the Russians interfered with Georgian Internet sites, but we lack clear and convincing evidence respecting the other two cases discussed above.

Finally, necessity and proportionality may be the most difficult conditions to meet. Estonia and Iran have not even established who attacked their computers. That takes time, and there is the problem of proving that a counter-attack can achieve a defensive purpose. Finally, counter-attacks in self-defence with a computer application will be challenging to limit in terms of effects to the intended target. Over 40% of the computers attacked by Stuxnet were outside Iran.[77]

Just because a cyber-attack or cyber espionage do not amount to an armed attack does not mean that international law has no law against such wrongs. Interference with a State's economic sphere, air space, maritime space or territorial space, even if not prohibited by treaty is prohibited under the general principle of non-intervention. This is apparent in a number of treaties, UN resolutions and ICJ decisions that condemn coercion, interference or intervention that falls short of the use of force. The ICJ has referred to some of this conduct as 'less grave forms' of force that violate the principle of non-intervention

[72] *Oil Platforms (Iran v US)* [2003] ICJ Rep 161, 191.

[73] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136, 195.

[74] *Armed Activities on the Territory of the Congo (Congo v Uganda)* [2005] ICJ Rep 168, 301.

[75] See generally on the evidence standards of international law in use of force cases, ME O'Connell, 'Evidence of Terror' (2002) 7 JCSL 19. Also see N Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' s 3, in this volume.

[76] DE Graham, 'Cyber Threats and the Law of War' (2010) 4 J Natl Security L & Policy 87, 92 (citing E Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 Stanford J Intl L 232–35 and R Lehtinen and others, *Computer Security Basics* (2nd ed, O'Reilly 2006) 81).

[77] See n 36.

while not triggering rights of a victim State under Article 51.[78] In support, the court has referenced the UN General Assembly's Declaration on Friendly Relations,[79] the OAS Convention on the Rights and Duties of States in the Event of Civil Strife,[80] and other authoritative sources for the existence and content of the non-intervention principle.[81]

4. Achieving Cyber Security Lawfully

International law raises substantial barriers to both using cyber weapons and defending cyber space from cyber-attacks through the use of force. In general, international law supports regulating cyber space as an economic and communications sphere and contains coercive means of responding lawfully to cyber provocations of all types. The same sort of coercive measures that are lawful to use against economic wrongs and violations of arms control treaties will generally be lawful to use in the case of a cyber-attack. In the economic sphere, responses to violations tend to be known as 'countermeasures'; in the arms control sphere, they are known as 'sanctions'.[82] Both are the coercive enforcement measures, not involving the use of significant military force, available to States acting in response to an internationally wrongful act. In addition, various arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, provide for the Security Council to take action in the case of a violation. Despite the availability of these alternatives to the use of military force, it is important to reiterate that protecting cyber space, keeping it viable for economic and communication uses, will generally require defensive measures, not offensive ones. Good computer security cannot be replaced by countermeasures, let alone military measures.

78 *Nicaragua* paras 187–201.

79 See Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, GA Res 2625 (XXV), UN Doc N8028 (1970).

80 1928 OAS Convention on the Rights and Duties of States in the Event of Civil Strife 134 LNTS 45.

81 See *Nicaragua* para 203 (citing Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, GA Res 2131 (XX), UN Doc A/EES/36/103 (9 December 1981)). The Court also referred to the principle of State sovereignty under article 2(1) of the UN Charter, noting its close connection to the principles of the prohibition on the use of force and of non-intervention; *Nicaragua* para 212–14.

82 The definitions of the terms 'countermeasures' and 'sanctions' are not a settled matter in international law. White and Abass, for example, define countermeasures as non-forcible measures taken by States and sanctions as non-forcible measures taken by organizations. This would be a helpful distinction but for the fact that the USA, for example, labels its unilateral, non-forcible coercive measures 'sanctions'. See generally, N White and A Abass, 'Countermeasures and Sanctions' in M Evans (ed), *International Law* (3rd edn, OUP 2010) 531.

A. Unilateral Peacetime Countermeasures

The international law literature contains little on countermeasures as the lawful response to cyber-attacks. This is likely because legal scholars in the cyber security field tend to be divided among those who are expert in domestic Internet law issues, especially privacy rights and copyright,[83] and those who come from the world of the international law on the use of force.[84] As noted above, few generalists in international law are writing about Internet security. It is not surprising, therefore, that countermeasures are overlooked.[85]

Yet, countermeasures are the mechanisms through which international law allows parties to carry out self-help, coercive enforcement of their rights. Self-help plays a larger role in international law enforcement given the absence at the international level of both a central police force and compulsory courts.[86] The International Court of Justice, in the *Gabčíkovo – Nagymaros* case, laid out four elements of a lawful countermeasure:

1. In the first place it must be taken in response to a previous international wrongful act of another State and must be directed against that State.
2. The injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it.
3. The effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.
4. Its purpose must be to induce the wrongdoing State to comply with its obligations under international law, and the measure must therefore be reversible.

If a State is the victim of a cyber-attack or cyber espionage, and it has clear and convincing evidence that the wrong is attributable to a foreign sovereign

[83] In the USA the leading scholar in the area of the Internet is Lawrence Lessig of Harvard Law School. Lessig does comment on international and foreign law but his background and training are plainly in the area of US domestic law. Even Jack Goldsmith, also Harvard Law School, while being called the future of international law at the school is plainly from the domestic law arena. This is revealed by his comment that law governing military use of the Internet, is uncertain.
This fact about cyber scholars is changing, however, as intellectual property scholars, such as Graham Dinwoodie, with strong backgrounds in international and domestic law relevant to cyber space regulation.

[84] A number of scholars have already been cited working in the area of international law and the use of force, who have analysed military force in cyber space: see eg, Schmitt (n 14); Dinstein (n 14); Graham (n 77); and Dunlap (n 12).

[85] As White and Abass point out, it is also the case that international law scholars have paid relatively little attention to countermeasures and sanctions and the rules governing their use. White and Abass (n 83) 531. But see ME O'Connell, *The Power and Purpose of International Law, Insights from the Theory and Practice of Enforcement* (OUP 2008, paperback 2011) chs 4 and 5 and the citations therein.

[86] O'Connell (n 86) 264.

State, the victim State may itself commit a wrong against the attacking state, so long as the wrong is commensurate with the initial wrong (proportionality) and so long as the response is aimed at inducing an end to the initial wrong (necessity) or the provision of damages. In most cases of cyber wrongs, the evidence that a foreign State is behind a particular act, will be found only after the act is over or the damage is done. This fact indicates that most countermeasures aimed at cyber wrongs will be a demand for money damages. The international cyber community appears to be adept at estimating the amount of money to repair damage caused by a wrongful cyber event. Thus, a victim State should be able to meet the elements of lawful countermeasures in way comparable with States suffering trade injuries and having the right under WTO rules to apply countermeasures against the wrongdoing state.

B. Security Council Sanctions

If cyber-attacks threaten a State's security but do not amount to armed attacks under Article 51, it is also possible for the victim State to ask the Security Council to intervene. The Council has imposed sanctions in a variety of situations for decades.[87] It could clearly do so in the case of serious cyber-attacks. To make this clear and to get the benefit of wide notice of such a possibility so as to deter cyber misconduct, a treaty spelling out the parameters of lawful and unlawful Internet use would be invaluable.

The international community has adopted treaties in other 'dual-use' areas that are analogous to cyber space, such as the Chemical Weapons Convention[88] and the Nuclear Non-Proliferation Treaty.[89] Both of these treaties seek to end any use or even possession of chemical or nuclear weapons while at the same time promoting legitimate non-military uses of chemicals and nuclear power. In the case of both treaties, the Security Council may become involved if States violate the treaty. In the case of nuclear weapons, the Council has become involved in the case of North Korea's nuclear weapons despite the fact that North Korea has withdrawn from the NPT.

Russia has in fact promoted 'an international treaty along the lines of those negotiated for chemical weapons and has pushed for that approach....' to regulating cyberspace.[90] In a speech on 18 March 2012, Vladislav P Sherstyuk, a

[87] See V Gowlland-Debbas, *United Nations Sanctions and International Law* (Kluwer 2001).

[88] See n 18.

[89] 1970 Treaty on Nuclear Non-Proliferation (opened for signature 1 July 1968, entered into force 5 March 1970) 729 UNTS 161 <http://www.un.org/disarmament/WMD/Nuclear/NPT.html> (accessed 20 June 2012).

[90] J Markoff and AE Kramer, 'US and Russia Differ on a Treaty for Cyberspace' *New York Times* (New York, 27 June 2009) <http://www.nytimes.com/2009/06/28/world/28cyber.htm?_r=1> (accessed 20 June 2012). Waxman dismisses the Russian proposal because he believes the Russians are developing cyber weapons. This is an

deputy secretary of the Russian Security Council, laid out what he described as Russia's bedrock positions on disarmament in cyberspace. Russia's proposed treaty would ban a country from secretly embedding malicious codes or circuitry that could be later activated from afar in the event of war.

The USA, however, has resisted proposals for a treaty. This may relate to US plans to use the Internet for offensive purposes as it is believed to have done regarding the Stuxnet worm. US officials claim publicly that Cyber Command is primarily defensive, but the reluctance to entertain the idea of a cyberspace disarmament treaty is raising questions as the true US position. '[T]he Russian government [has] repeatedly introduced resolutions calling for cyberspace disarmament treaties before the United Nations. The United States [has] consistently opposed the idea.'[91]

C. Cyber Law Enforcement Cooperation

Whatever the reasons for the US position, drafting a treaty on disarmament and alternatives to military force for regulating cyberspace are essential for the future. In addition to establishing clear rules for national rights and duties on the Internet, a treaty can clarify what is permissible for individuals. A treaty can specify the sort of conduct that all States need to regulate through national law enforcement agencies and in cooperation with other national and international agencies. A model for this part of a comprehensive treaty is already available in the form of the Budapest Convention on Cybercrime.[92] Most cyber security breaches are caused by private criminals.

D. Good Cyber Hygiene

At the end of the day, countermeasures, sanctions and even law enforcement cannot substitute for frontline computer and network security measures. An essential step in maintaining a good cyber defence is applying best practices and educating everyone legitimately using the Internet on good network hygiene. In this respect, the analogy is better made to stopping pandemics than to crime or war.

unpersuasive reason not to pursue a convention. While the Chemical Weapons Convention was being negotiated, however, States continued to maintain chemical weapons and very likely to continue to develop them. Waxman (n 14). The Russian proposal has been part of the discussion within the United Nations about achieving security in cyberspace. This discussion dates to 1998. See Developments in the field of information and telecommunications in the context of international security, G.A. Res 53/70, U.N.Doc. A/RES/53/70 (4 January 1999).

[91] Markoff and Kramer (n 91).

[92] 2001 Budapest Convention on Cybercrime <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (accessed 20 June 2012).

The Internet has made it easier for hackers to steal information remotely. This is largely due to 'the proliferation of smartphones and the inclination of employees to plug their personal devices into workplace networks and cart proprietary information around'.[93] As a result standards for cyber hygiene have elevated, especially for those who have access to vital information.[94]

> Cybersecurity is more than any one individual step; it is a continuous process where you need to: Learn, Monitor, Analyse, Decide and Respond. The process must be applied in the context of risks to business assets and operational resilience.[95]

This approach, set out in a white paper published by IBM on cyber security is referred to as the lifecycle model to cyber security in which consideration must be given at each stage to technology, service management and risk.[96]

Navy Vice Adm Carl V Mauney, deputy commander of US Strategic Command has remarked, '[t]his is about setting people to high standards, and maintaining those standards... like hand washing, it should be second nature to *everyone* operating on the net'.[97] Marine Corps Maj Gen George J Allen said his biggest concern is educating all users about risks. According to Allen, '[y]oung people who have grown up with the Internet sometimes aren't cautious enough, such as some Marines who have posted their deployment dates on Facebook'.[98] He went on to say, '[o]ur biggest problem is... the digital natives who are very comfortable with YouTube and other things who don't understand the threats behind it.... [t]hat's not their fault—that's our fault. It's a matter of educating them'.[99]

Every State is heavily dependent on private companies for Internet security—just as they are for conventional military security.[100] The USA draws significantly on private corporations for ensuring national security. Corporations

[93] N Perlroth, 'Travelling Light in a Time of Digital Thievery' *New York Times* (New York, 10 February 2012) <http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?_r=2&pagewanted=1&ref=technology> (accessed 20 June 2012).

[94] ibid.

[95] M Borrett, 'Cyber Strategies Revealed' IBM Institute for Advanced Security (11 December 2011) <http://www.instituteforadvancedsecurity.com/expertblog/2011/12/11/cyber-strategies-revealed/> (accessed 20 June 2012).

[96] C Nott and others, 'Cyber Security: Protecting the Public Sector' IBM Institute for Advanced Security (September 2011) <http://www.instituteforadvancedsecurity.com/docs/CyberSecurity-protecting_the_Public_Sector.pdf> (accessed 20 June 2012) 1, 7.

[97] L Daniel, 'Cyber Command Synchronizes Services' Efforts' US Department of Defense (9 July 2010) <http://www.defense.gov/news/newsarticle.aspx?id=59965> (accessed 20 June 2012) (emphasis added).

[98] ibid.

[99] ibid.

[100] 'Much of cyberspace is owned and used by private companies. [Thus i]t is businesses that will drive the innovation required to keep pace with security challenges.' Borrett (n 96).

manufacture most of the nation's arms. They produce most of the software and hardware for the computers the government uses. Corporations, under contract with the government, carry out many other security functions, including the collection and processing of intelligence and the conduct of covert operations.[101] However, much of the business community strongly resists implementing cyber security per government mandate,[102] let alone international organization oversight.[103] Governments and organizations will need to find incentives to get private corporate cooperation and to lead in terms of promoting and supporting international cooperation, especially through international organizations such as the ITU.[104] This might be done by shifting resources away from the military sector to the Internet sector, both private commercial and international organizational. Best practices and promotion of a culture of security can be carried out most effectively for the Internet through a holistic approach that includes all actors with an interest in maintaining access to a safe Internet. The International

[101] A Etzioni, 'Private Sector Neglects Cyber Security' The National Interest (29 November 2011) <http://nationalinterest.org/commentary/private-sector-neglects-cyber-security-6196> (accessed 20 June 2012).

[102] ibid.

[103] The attitude of many in the private commercial cyber sector is captured in this opening sentence of an on-line article by two lawyers on behalf, presumably, of clients: 'Once again, many companies in the telecoms and information and communications technology (ICT) sector are facing the specter of a.United Nations agency (in this case the International Telecommunications Union (ITU)) regulating critically important aspects of the internet as well as substantially expanding its jurisdiction over the telecoms and ICT industries.' Ambassador DA Gross and E Lucarelli, 'The 2012 World Conference on International Telecommunications: Another Brewing Storm Over Potential Un Regulation of the Internet' Who'sWho Legal (30 April 2012) <http://www.whoswholegal.com/news/features/article/29378/the-2012-world-conference-international-telecommunications-brewing-storm-potential-un-regulation-internet/> (accessed 20 June 2012).

[104] The Brookings Institution (n 16). 'Being secure is not just about keeping 'bad guys on the outside; it's about making the systems inside less vulnerable.'

> Reducing vulnerability of internal systems includes ensuring: (1) Each application validates its input for reasonability before processing; and (2) Each application has a way of announcing an exception—whether it is a security intrusion or simply a failing intelligent Electronic Device (IED) sending bad input. It is for the security system to decide why the abnormal event occurred. (ibid)

Katz notes however that attention to architectural tenets is needed beyond just tactical measures. 'These can be applied specifically to cyber threat reduction in general hardware or software architectures. One conventional precept is to "build for the end solution" '. Following best practices and having up to date technology is still not enough says Katz. What is required is a change in how we think of security. 'In general, what is desired is a culture of security, not solely a culture of compliance with security regulations'. Jeffrey Katz, *Smart Grid Security and Architectural Thinking*, available at <http://www.ibm.com/smarterplanet/global/files/us__en_us__energy__smartgridsecurity_and_architecturalthinking_katz.pdf> (accessed 20 June 2012).

Telecommunications Union is the natural organization to lead on common security in cyber space.

5. Conclusion

To date, the problem of Internet security has been the domain of international law scholars with expertise in use of force questions. They have sent the message that the Internet may be protected through military force or the threat of military force, analogizing to Cold War deterrence strategy. Governments have followed this modelling, pouring resources into the military for keeping the Internet safe and for taking advantage of what it offers to attack opponents. Doing so has required strained analogies of cyber-attacks to conventional kinetic attacks. The Internet is now far less secure than before there was a Cyber Command or a NATO CCDCOE. It is time, therefore, to turn to cyber disarmament and a focus on peaceful protection of the Internet. The motto should be: a good cyber defence is good cyber defence.