A treaty for cyberspace

REX HUGHES*

'The next war will begin in cyberspace.' Those are the words of the nominee to lead the first United States Cyber-Command (USCYBERCOM).[1] Inside a nondescript building adjacent to the National Security Agency headquarters in Maryland, a small team under the direction of the Secretary of Defense has been working quietly to establish the world's first cyberspace command. Although its strategic objectives remain classified, its mission is clear: to ensure continued US primacy in cyberspace.

As cyberspace becomes what military strategists and futurists call the 'next battlespace', the world may indeed be witnessing not only the rise of a new zone of strategic competition but, more consequentially, ground zero for the next global arms race. Although cyber-warfare is still in its infancy, a new generation of cyber-weaponry and cyber-warriors promises to reshape how war is waged in the early twenty-first century. While the electromagnetic spectrum is not an entirely new zone of conflict, disruptive innovations and human dependence on machines make online targets increasingly attractive for states seeking to achieve greater impact at lower cost. This is especially true for small countries looking to gain an asymmetric edge on the twenty-first-century battlefield. The United States, still the world's pre-eminent military superpower, is not the only nation preparing to fight the 'next war' in cyberspace. By the start of 2010 China, India, and Russia alongside the US, the UK and South Korea are among the first group of countries to establish formal command and control (C2) over military assets in the cyber-domain.[2]

In addition, a host of non-state actors are engaged in cyber-warfare. Al-Qaeda, Hezbollah, Hamas, Zapatistas and a variety of 'patriotic' hacker-attackers are just

* The author is grateful for the numerous comments he received from his Chatham House and Cambridge University colleagues, and especially to Professors Paul Cornish, Geoffrey Edwards, and Jon Crowcroft for their countless hours of discussion and mentorship. He also thanks Dr Vinton G. Cerf, VP Google, for first advancing the idea of a cyber-treaty in the early stages of the author's PhD fieldwork; former US Ambassador Thomas Pickering for personal instruction on treaty-making; UK Major-General (Retd) Anthony Rogers for his prescient thoughts on the laws of war and cyberspace; and the staff of the NATO Parliamentary Assembly for facilitating interviews and consultations with senior alliance officials.

[1] In June 2009 the US Secretary of Defense formally recommended to the President that the United States establish the USCYBERCOM as part of the US Strategic Command (USSTRATCOM). At the time of writing, nominee Lt-Gen. Keith B. Alexander, who has served since 2005 as Director of the National Security Agency and Chief of the Central Security Service concurrently, awaits Senate confirmation.

[2] See details under 'Threats and national responses' below.

some of the known paramilitary, resistance or revolutionary groups that have used cyber-warfare or plan to engage in it, with or without specific state sanction. As numerous media accounts have attested, even a teenager armed with a consumer PC and a broadband connection can wreak havoc on both business and government organizations in cyberspace, as demonstrated in 1999 by teenage British hackers who altered British military secure satellite orbits and as reported early in 2008 a teenager in Poland who basically turned the Lodz 'tram system into his own personal train set'.[3]

If the next war will indeed be waged in cyberspace, then what if anything should international society do to govern or regulate this domain? In an attempt to bring greater attention to the growing interdependencies between cyber-warfare and international affairs, this article proposes that a multilateral regime is needed to govern cyber-warfare at the global level.[4] As the prospect of a prolonged interstate cyber-war increases, this article examines the role that a cyber-warfare treaty or 'Treaty for Cyberspace' could play in limiting the adverse human effects of interstate conflict in cyberspace.[5]

While the first all-out cyber-war has yet to be waged, cyber-experts and military strategists anticipate that a major interstate cyber-battle could be fought within the next few years.[6] Most worrisome from an international affairs perspective is the feeble system of regulation and governance that currently pertains to this emergent threat. As global society becomes ever more dependent on cyberspace for both its most basic and its most critical functions, the economic and social impact from a full-scale cyber-attack could cripple a modern networked state. More importantly, General Kevin Chilton of the US Strategic Command (USSTRATCOM) is representative of many military leaders in believing that a major cyber-attack on an advanced information economy could spur a substantial conventional or in some cases even a nuclear response.[7] He maintains that national strategists would not want to 'take any response options off the table' during a battle in the cyber-domain.[8]

This article is divided into four sections. The first examines the evolution of cyberspace from a 'geekspace' into a 'battlespace' and the relationship between the 'revolution in military affairs' (RMA) and cyber-warfare.[9] The second examines

[3] Shelley Smith, 'Teen hacker in Poland plays trains and derails city tram system', *Homeland Security*, 18 Feb. 2009, http://inhomelandsecurity.com/2008/02/teen_hacker_in_poland_plays_tr.html, accessed 12 Jan. 2010. Graeme Baker, 'School boy hacks into city's tram system', *Telegraph*, 11 Jan. 2008.

[4] See also Rex Hughes, 'Towards a global regime cyberspace', in Christian Czosseck and Kenneth Geers, eds, *The virtual battlefield: perspectives on cyber-warfare* (Amsterdam: IOS Press, 2009).

[5] The only treaty that comes close to addressing cyber-warfare is the European Convention on Cybercrime. However, as the title states, the treaty is designed to regulate only 'cyber-crime', not a state of 'cyber hostilities'.

[6] Nathan Hodge, 'General: we just might nuke those cyber-attackers', *WIRED,* 13 May 2009, http://www.wired.com/dangerroom/2009/05/general-we-just-might-nuke-those-cyber-attackers/, accessed 11 Dec. 2009.

[7] Kevin P. Chilton, speech for the 2009 Cyberspace Symposium, Omaha, 7 Apr. 2009, http://www.stratcom.mil/speeches/23/2009_Cyberspace_Symposium. USSTRATCOM represents all four services, plus Department of Defense contractors and civilian employees.

[8] Jeff Schogol, 'Official: no options "off the table" for US response to cyber-attacks', *Stars and Stripes* (mideast edn), 8 May 2009, http://www.stripes.com/article.asp?section=104&article=62555, accessed 11 Jan. 2010.

[9] The term 'geek' in this context refers to one adept and often absorbed with computers and digital devices. The 'geeks' of 'geekspace' in laboratories and universities largely comprised the online community of the early

some of the main vectors of cyber-attack, with a look at the early cyber-warfare capabilities held by the foremost cyber-powers. The third examines the leading debates surrounding the application of international law to cyber-warfare. The fourth outlines some basic principles that a multilateral cyber-treaty might contain.

This article, written from an international relations perspective, is intended to introduce the topic of cyber-warfare and its governance to international relations scholars and practitioners who are either new to or unfamiliar with the topic. The article does not evaluate or assess cyber-warfare strategy, operations or tactics; nor does it explore the international legalities of current manœuvres in cyberspace. The examples and evidence presented here are based mainly on cyber-defence developments in the US, which has taken a lead in confronting cyber-threats to its own systems and those of its allies. For the purposes of this article, the term 'cyber-warfare' is used to indicate broadly any warfare waged by states and significant non-state actors in cyberspace. It can include defending information and communications systems, critical infrastructure, weapons systems or military command centres from attack, as well as conducting equivalent offensive operations against an adversary. It does not refer to recreational or socially motivated hacking or 'hacktivism'.

From geekspace to battlespace

An immense structural challenge is facing international society in preventing a *bellum omnium contra omnes* or a 'war of all against all' in cyberspace. In less than a quarter of a century the term *cyberspace*, popularized by science fiction writer William Gibson, has evolved from the virtual world first colonized by pimply geeks and dweebs into the digital realm of a rapidly expanding networked society.[10] Rapid advancements in information and communications technology have connected nearly two billion digital citizens across the invisible ether of cyberspace.[11] But why has this digital domain of sophisticated circuits and software developed into a new theatre of war or battlespace? In order to begin addressing this question, it is useful to consider the evolution of US military strategy since the Vietnam War.

Cyberspace and the revolution in military affairs

In one sense, modern cyber-warfare is linked to early long-distance telecommunications. With the introduction of the telegraph, telephone and radio, both civilian and military leaders gained an unprecedented command-and-control authority

internet systems and communications. The term 'dweeb', often used with a more negative connotation, also refers to one with a computer-related obsession.

[10] The term 'cyber' was introduced by Norbert Wiener in his *Cybernetics: or control and communication in the animal and the machine* (Cambridge, MA: MIT Press, 1948). Having employed the term 'cyberspace' in an earlier short story, Gibson used it again in his popular novel *Neuromancer* (New York: Ace Books, 1984).

[11] The estimated total of internet users across the world at 30 September 2009 was estimated at 1,733,993,741: 'Internet usage statistics: the internet big picture', Internet World Stats, 30 Sept. 2009, http://www.internetworldstats.com/stats.htm, accessed 20 Jan. 2010.

International Affairs 86: 2, 2010

over troop movements and deployments. For good or ill, real-time communication systems revolutionized C2 by increasing political participation in battlefield decisions. US President Abraham Lincoln was the first commander-in-chief to use the telegraph for issuing direct orders to his generals during battle.[12] Telephone, telegraph and radio also gave political leaders unprecedented control over their representatives abroad: the government of Queen Victoria made extensive use of the telegraph for official communications between London and overseas military commanders, diplomats and viceroys.[13]

During the First World War, long-distance communications instruments became fully integrated into land, sea and air campaigns. In the Second World War, the sheer complexity and scale of the conflict increased the need for cybernetic-controlled weapons. As firepower increased once more across land, sea and air, so the need for more precision and predictability also increased. This was especially true in the areas of artillery and cryptology. Between 1943 and 1946 the US Army developed the first general purpose computer to improve the accuracy of its firing tables. During this same period the British code-breakers of Bletchley Park decrypted over 3,000 German Enigma messages, thanks to the cryptographic innovations of Alan Turing.[14] Long-distance communications and computational power coupled with the microwave were used by the British and Americans to develop an active air defence system to counter German air strikes.[15]

The atomic age only accelerated cybernetic development as the need for even more precise, reliable and speedy C2 operations increased exponentially. The deployment of nuclear weapons required the most sophisticated air and space communications networks ever developed. Between the 1950s and 1960s, the nuclear and space races helped propel a host of new information and communications technology breakthroughs with the invention of the transistor, microprocessor, laser, and packet-switching. From the 1970s onwards, many of these military and space technologies escaped from the lab to the civilian sector.

Information as a weapon

In the wake of setbacks in Vietnam, where attempts to apply tactics developed during the Second World War and the Korean War often failed, US military strategists eagerly sought new methods to achieve a decisive victory on the Cold War battlefield. In the early 1970s the innovative thinker Andrew Marshall was recruited from the RAND Corporation (*R*esearch *AN*d *D*evelopment) by the US

[12] Tom Wheeler, 'How the telegraph helped Lincoln win the Civil War', History News Network, George Mason University, 20 Nov. 2006: http://hnn.us/articles/30860.html, accessed 17 Dec. 2009. See also Tom Wheeler, *Leadership lessons from the Civil War: winning strategies for today's managers* (New York: Doubleday, 1999).

[13] Tom Standage, *The Victorian internet* (New York: Walker, 1998), pp. 154–7.

[14] Gregg Keizer, 'British Museum unveils WWII computer replica', *InformationWeek*, 8 Sept. 2006, http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=192700296, accessed 12 Jan. 2010.

[15] Steve Blank, 'The secret history of Silicon Valley, part 2: Every World War II movie was wrong', http://steveblank.com/2009/04/27/the-secret-history-of-silicon-valley-part-vi-the-secret-life-of-fred-terman-and-stanford/, accessed 10 Jan. 2010.

International Affairs 86: 2, 2010

Department of Defense to head its Office of Net Assessment.[16] At the Pentagon, Marshall was given the tall-order task of finding ways for NATO to defeat the Warsaw Pact short of a nuclear response. In his first departmental report Marshall told of the progress that US weapons labs were making on a new generation of 'smart' weaponry that would deliver substantially increased lethality with a lower loss of US life. The increased precision was made possible by a new generation of software and electronics built around the microprocessor. Moore's Law would soon alter the balance of information power on the Cold War battlefield.[17]

On the other side of the Iron Curtain, Soviet military planners also looked to the coming revolution in military affairs. These strategists procured similar studies that emphasized the growing interconnection between microelectronics and modern warfare. However, unlike the American planners who saw the US military benefiting from this silicon revolution, the Soviets were worried about their own economic inability to exploit the digital revolution. The USSR was rapidly losing ground to US prowess in microelectronics. In time the US would use its information technology advantage to overpower the Soviet military industrial base. [18] Reagan was determined to avoid the use of tactical nuclear weapons in Europe and willingly gave his military the extravagant budget requested to depower any strategic advantage held by the USSR.

Although the RMA is typically associated with technological advancements, it also involves changes in strategy, operations and tactics. The ancient Romans used information as a decisive element on the battlefield, and the element of surprise has always been a crucial tactic. On the heels of the rapid technological developments of the twentieth century, the military analysts and futurists responding to the weaknesses of and challenges to conventional warfare strategy discussed how the coming 'information age' would change the way wars were fought. This thinking was not exclusive to the US; but other countries could not match the depth and breadth of US investment in information warfare analysis and development. Much of this 'info-war' planning was used to justify a number of new weapons systems and programmes—including the US Department of Defense ARPANET (Advanced Research Projects Agency Network), the forerunner of today's internet.

An information doctrine

As information systems became more essential to military operations, a new US *information warfare* (IW) doctrine developed. Thus the electromagnetic spectrum

[16] Gordon Barrass, 'The renaissance in American strategy and the ending of the great cold war', *Military Review*, Jan.–Feb. 2010, p. 102, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20100228_art016.pdf, accessed 22 Dec. 2009.

[17] Moore's Law was introduced by Intel co-founder Gordon Moore in a 1965 paper in which he stated that computing trends in the long term find that the exponential increase of processing speed and memory is related to the doubling every two years of the number of processors that can be placed on an integrated circuit.

[18] John Arquilla, from statements to Mark Williams, 'Technology and the future of warfare', *Technology Review* (MIT) 23 Mar. 2006, http://www.technologyreview.com/BizTech/wtr_16620,295,p1.html, accessed 11 Dec. 2009;

International Affairs 86: 2, 2010

and information space were added to the physical battlespaces of air, surface and subsurface. The IW objective was to harness the power of information as a strategic weapon to outwit or outmanœuvre an opponent. While the information and computing technology underlying the early decades of cyberspace was primitive compared with what is available today, nonetheless there was strong belief among the US military leadership in information warfare as the future of warfighting in the twenty-first century. For the US, the RMA of the late 1990s encompassed change in three areas—information operations, weapons systems and space. To these Michael Schmitt adds a fourth RMA trend: militarization of civilian activities.[19] What Schmitt is referring to here is the integration of civilian personnel and infrastructure into the twenty-first-century battlespace. As presented later in this article, the militarization of civilian activities and infrastructures in cyberspace poses significant challenges to existing legal frameworks governing warfare.

Threats and national responses

While Cold War planners foresaw information warfare as playing out largely on the conventional battlefield, in the second decade of the twenty-first century many aspects of 'information warfare' shifted from the traditional military battlefield to the public sphere. The US Department of Homeland Security has issued statistics showing that reported attempts to breach security on both private and government computer systems increased from 24,000 in 2006 to 37,000 in 2007 (an increase of 58 per cent), according to a security awareness executive, Tom Kellerman. He also noted that that the FBI estimated that 108 countries had dedicated cyber attack capabilities.[20]

Since 2000, reported state-sponsored cyber-intrusions have ranged from attacks on government websites to critical infrastructure. In 2000, Israeli operatives disabled the public websites of Hezbollah and the Palestinian National Authority (PNA). This attack was viewed as sparking a 'cyber holy war' after the Palestinians responded with strikes against Israel's financial institutions and government systems. The 2001 maritime dispute in the South China Sea led China to launch a cyber attack against a California electricity plant causing the gird to nearly cease operations.[21] In September of 2007, Israel launched a successful cyber attack on Syria's air defense network which aided its Air Force in the bombing of a suspected nuclear plant under construction in Syria.[22] Several internet sites operated by Radio Free Europe/ Radio Liberty (RFE/RL) were brought to a

[19] Michael Schmitt, 'Bellum Americanum', in Michael Schmitt, ed., *The law of armed conflict into the next millennium* (Newport: Naval War College, 1998), pp. 394–400.

[20] Jack Germain, 'The art of cyber-warfare, part 1: the digital battlefield', *TechNewsWorld,* 29 April 2008, http://www.technewsworld.com/rsstory/62779.html?wlc=1263772777, accessed 9 Jan. 2010. Kellerman, a member of The Commission on Cyber Security for the 44th Presidency, served in the World Bank Treasury Security Team for cyber intelligence.

[21] Kenneth Geers, 'Cyberspace and the changing nature of warfare', *SC Magazine*, 27 Aug. 2008, http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/, accessed 11 Jan. 2010.

[22] Eshel, David, 'Israel adds cyber-attack to IDF', *Aviation Week's DTI*, 9 Feb. 2010, http://www.military.com/features/0,15240,210486,00.html, accessed 22 Feb. 2010.

standstill in 2008 through faked hits (estimated to occur at a rate of 50,000 per second). Such a scheme was highly sophisticated and has been attributed to the leader of Belarus, who with dedicated supporters was attempting to quash RFE/RL coverage of the activity of protesters against his government.[23]

The CIA reported that in 2007 several cyber-attacks on public electricity networks were carried out in a number of regions inside and outside the US. Managers of utilities are hesitant to talk about the dangers. Retired US Admiral Mike McConnell, who served as head of the CIA, the Defense Intelligence Agency and the National Security Agency, warned in late 2009 that he saw adversaries of the US possessing the capability to disable major segments of the US power grid.[24] Once inside the grid a sophisticated hacker may be able to assume the 'same access and powers as the systems administrator' of that grid.[25] Since 2005, attacks on SCADA (supervisory control and data acquisition) systems have been reported on electrical power networks in Brazilian cities.[26] John Mulder, a US Department of Energy security specialist at the Sandia Laboratories, has described how Sandia works to identify vulnerabilities by attempting—with the permission of power and water companies—to hack into these systems and other critical targets to strengthen respective defence measures.[27]

The widely publicized attacks on Estonian networks in 2007 and Georgia's state systems in 2008 have been attributed either to Russian patriotic hackers or to official Russian agents.[28] NATO responded to the Estonia network shutdown by convening an emergency meeting of the North Atlantic Council; and at the 2008 Bucharest summit, the alliance announced its first cyber-defence policy, marking the first occasion on which an international military organization had deemed cyber-security to be a collective defence obligation. NATO claims that, should a member state face a catastrophic cyber-attack, its new cyber-security policy gives it the tools to respond effectively.[29]

[23] 'Cyberjamming', *Wall Street Journal Europe*, 29 April 2008, http://online.wsj.com/article/SB120942466671951083.html, accessed 11 Jan. 2010.

[24] For an in-depth view of the real-world consequences of high-level cyber-attack, see 'Urgency of this cyber-security work', United States Cyber-Consequences Unit, http://www.usccu.us/#The_Urgency_of_This_Cyber-Security_Work, accessed 3 Jan. 2010.

[25] Siobhain Gorman, 'Electricity grid in US penetrated by spies', *Wall Street Journal*, 8 April 2009, http://online.wsj.com/article/SB123914805204099085.html, accessed 10 Jan. 2010.

[26] SCADA is the world standard for microprocessor controlled public infrastructure and is used widely in factories as well as public energy and transport networks. Information may be gathered in various locations and sent to a central computer.

[27] Mulder interviewed by Steve Kroft, 'Cyber-war: Sabotaging the system', *60 Minutes*, CBS broadcast, 8 Nov. 2009, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml, accessed 08 Jan. 2010. As a GOCO (government-owned/contractor-operated) enterprise, Sandia conducts research and assessments relating to nuclear weapons, defence systems and homeland security as well as energy resources.

[28] John Markoff and Andrew Kramer, 'US and Russia differ on a treaty for cyberspace', 27 June 2009, p. 1, http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1, accessed 11 Dec. 2009.

[29] Rex Hughes, 'NATO and global cyber defense', *The Bucharest Conference Papers,* German Marshall Fund & Chatham House, 2008, pp.51–2.

Attack as the best form of defence

Similar to terrorism, cyber-security is both a domestic law enforcement issue and a military defence issue, and the dividing line between the two is unclear. It is clear from the episodes mentioned above that interference in the workings of the internet is now far more than the plaything of cyber-teenagers or anti-social adults, with the potential to disable critical infrastructure or military networks.

As cyber-security finds its way into national security policy, many governments are ready to develop capabilities that 'take the fight' to their online opponents. Judge Advocate Colonel Charles Williamson of the US Air Force Intelligence, Surveillance and Reconnaissance Agency states that 'the world has abandoned a fortress mentality in the real world, and we need to move beyond it in cyberspace' because the US faces 'increasingly sophisticated threats against its military and civilian cyberspace'. He wants America to acquire the 'ability to carpet bomb in cyberspace' in order to create a 'credible deterrent'. To this end, he argues, it needs to build an 'af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries'. In other words, it is time to abandon the strategy of past conflicts and harness digital power and expertise to build a 'powerful, flexible deterrent that can reach far outside our fortresses and strike the enemy while he is still on the move'. [30] According to Brigadier General Charles Shugg, deputy commander of the 24th Air Force, the USAF is also looking to automate many layers of its cyber defence as well, posing an entirely new set of ethical and legal challenges.[31]

Although the US took the early lead in cyber-warfare policy and command initiatives, since 2007 a number of states have begun to bolster their cyber-defences, for the most part without attracting much international attention. These initiatives have included everything from recruiting future cyber-warriors to establishing full-blown cyber-commands. Typically, the creation of a military C2 architecture for cyberspace indicates that a state aspires to acquire offensive cyber-attack capabilities. This section chronicles what both advanced or advancing powers are doing to build both offensive and defensive capabilities in cyberspace.

United Kingdom

In summer 2009 the UK announced its programme for cyber-security within its larger National Security Strategy (NSS) with the formation of two new bodies. Policy is coordinated in the Office of Cyber-Security (OCS) of the Cabinet Office. This new office is tasked with coordinating policy across government, looking at ethical and legal issues, and reviewing relations with other nations in this area.

[30] Charles Williamson, 'Carpet bombing in cyberspace', *Armed Forces Journal*, 2010, http://www.armedforces-journal.com/2008/05/3375884, accessed 11 Jan. 2010.

[31] Mark Ballard, 'US automates cyber defences to offset skills crisis', *Computer Weekly*, 18 Feb. 2010, http://www.computerweekly.com/Articles/2010/02/18/240349/us-automates-cyber-defences-to-offset-skills-crisis.htm, accessed 19 Feb. 2010.

The effort to join resources and expertise from across the civil and government sectors is located in the new Cyber-Security Operations Centre (CSOC). On both initiatives the Labour government has indicated that it willingly coordinates with the US and other allies.[32] In January 2010 the Conservative party leader, David Cameron, declared cyber-security to be an important part of his party's national security strategy.[33] Together these actions make the UK the first EU member state to announce an actionable strategic framework for confronting national-level cyber-threats.

South Korea

South Korea announced in early January 2010 that it was preparing to launch a military cyber-warfare command to ward off attacks from North Korea and from other countries on its military and government IT systems. As one of the 'most wired societies' in the world, it has experienced a number of cyber-attacks and has claimed that China used viruses to steal information from its government systems in 2004.[34] Some NATO officials have expressed interest in incorporating South Korea and other East Asia countries into its cyber defence network via its Global Partnership Programme.[35]

India

In 2008 the Indian Army started preparing for 'battles in the digitized battlefield'. India had suffered numerous cyber-attacks, and claimed the strikes were carried out by 'China's cyber warfare army'.[36] India's commanders have embarked on the process of boosting its cyber-defence with over 15,000 division-level troops. In addition, they have announced the need for cyber-security audits to be performed periodically by India's Army Cyber-Security Establishment (ACSE).[37] India has also begun to develop a cyber-warfare doctrine based upon its strategic nuclear doctrine.[38] With guidance from the US CERT (Computer Emergency Response Team) the government in New Delhi has established an Indian CERT to assist in reporting incidents, recovering from attacks, and strengthening networks and

[32] Gordon Corera, 'Cyber-security strategy launched', BBC News, 25 June 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm, accessed 12 Jan. 2010.

[33] David Cameron, 'How Britain can best address the threats of the twenty-first century', address at Chatham House, London, 15 Jan. 2010, http://www.chathamhouse.org.uk/events/view/-/id/1419/, accessed 20 Jan. 2010.

[34] 'South Korea to launch cyber-warfare command', *Defense Technology News*, Agence France-Presse, 11 Jan. 2010, http://www.defencetalk.com/skorea-to-launch-cyber-warfare-command-23649/, accessed 12 Jan. 2010.

[35] From private consultations with members of the NATO Parliamentary Assembly, Annual Meeting, Edinburgh, 14 Nov. 2009.

[36] Indrana Bagchi, 'China mounts cyber-attacks on Indian sites', *Times of India*, 5 May 2008, http://timesofindia.indiatimes.com/China_mounts_cyber_attacks_on_Indian_sites/articleshow/3010288.cms, accessed 11 Dec. 2009.

[37] 'Indian army gears up for cyber, electronic warfare', *India Defence*, 5 Feb. 2008, http://www.india-defence.com/reports/3824, accessed 12 Jan. 2010.

[38] Amit Sharma, 'Cyber wars: a paradigm shift from means to ends', in Christian Czosseck and Kenneth Geers, eds, *The virtual battlefield: perspectives on cyber-warfare* (Amsterdam: IOS Press, 2009).

systems.[39] Given India's burgeoning IT sector and associated knowledge industries, in many respects it is on the way to becoming a 'cyber superpower'.

China

There are indications that the Chinese People's Liberation Army (PLA) aspires to challenge US dominance in the electromagnetic spectrum should the country become embroiled in bi-lateral military confrontation. The 2008 and 2009 reports to the US Congress by the US–China Economic and Security Review Commission show increased offensive capability by the Chinese government. An estimated 30,000 'cyber-cops' in China monitor public and state security, apparently possessing the 'training and expertise that would allow them to conduct such cyber-penetrations'.[40] The UDS joint strike fighter project and the USAF air traffic control systems have been reported as PLA targets.[41] In January 2010 Google accused China of facilitating hostile attacks on its information systems leading to a high-level diplomatic row with the US.[42] In response China has accused the US of fomenting cyber-warfare.[43] In 2003 the 'then-director of the PLA's electronic warfare department, Dai Qingmin, proposed a comprehensive information warfare effort, including cyber-attack, electronic attack and coordinated kinetic attacks in military operations'.[44]

Russia

Although accused of perpetrating the attacks on Estonia and Georgia mentioned above, the Russian government has denied any culpability.[45] Yet the country is home to a sizeable number of low-paid computer experts who are thought to exploit the Russian resentment of affluent foreign states by attacking their internet-based operations, targeting foreign financial sites as well as perceived Russia enemies. Rather than considered as criminals, Russian civilian network hackers are generally held in esteem and may be among the independent civilian 'patriotic hackers'. The attacks on Estonia and Georgia utilized network systems outside Russian borders were most likely sanctioned, indeed ordered, by elements

[39] Indian Computer Emergency Response Team, Ministry of Communications and Information Technology (Government of India), http://www.cert-in.org.in/roles.htm, accessed 11 Jan. 2010; 'Computer Security Incident Response Team & Center', Network Security Solutions, http://www.mynetsec.com/services/csirt-cert-setup, accessed 12 Jan. 2010.

[40] Larry Wortzel, 'China goes on the cyber-offensive', *Far Eastern Economic Review*, January 2009, on-line post 9 Jan. 2009, http://www.feer.com/essays/2009/january/china-goes-on-the-cyber-offensive, accessed 11 Jan. 2010.

[41] Siobhan Gorman, August Cole and Yochi Dreazen, 'Computer spies breach fighter-jet project', *Wall Street Journal*, 21 April 2009, http://online.wsj.com/article/SB124027491029837401.html , accessed 10 Jan. 2010.

[42] Michael Sheridan, 'China's great internet stand-off', *Sunday Times*, 17 Jan. 2010.

[43] 'China accuses US of cyberwar', *Wired Magazine*, 25 Jan. 2010, http://www.wired.com/threatlevel/2010/01/china-accuses-us/, accessed 25 Jan. 2010.

[44] Larry Wortzel, 'China's cyber-offensive', *Wall Street Journal*, 1 Nov. 2009, http://online.wsj.com/article/SB10001424052748703399204574508413849779406.html, accessed 19 Dec. 2009.

[45] Robert Coalson, 'Behind the Estonia cyber-attacks', *TransMission* (Radio Free Europe/Radio Liberty), 8 Mar. 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html, accessed 19 Dec. 2009.

within the Russian government.[46] Kevin Coleman explains the Russian cyber-strategy, or what he calls 'Russia's Cyber-Warfare Doctrine', as 'designed to be a force multiplier along with more traditional military actions including WMD attacks. A force multiplier is a military term that describes a weapon or tactic that, when added to and employed along with other combat forces, significantly increases the combat potential of that force.' Coleman further claims that the Russian Business Network is 'thought to own and operate the second largest BotNet in the world. Intelligence suggests there are organized groups of hackers tied to the Federal Security Bureau (FSB)'. It has been claimed that the bureau works closely with the Russian military.[47]

Israel

In Israel the ministry responsible for protecting the Israel Defense Forces networks is Matzob (the Hebrew acronym for Centre for Encryption and Information Security). It operates under the C41 Corps and is responsible for the Israel Security Agency and Mossad networks (Shin Bet), and also for mainframes of the national corporations responsible for electricity and water grids. C41 Corps regularly tests encryptions and firewalls. Defence leaders take pride in the cyber-ability of Israel's citizens and in the country's technological sophistication that renders it independent of foreign assistance or technology.[48]

Legal challenges

Despite the rush to amass national cyber-arsenals, at the time of writing there is no international consensus on the application of the 'law of armed conflict' (LOAC, referred in some instances as LOW or 'law of war') to cyber-warfare, most often considered a form of 'irregular warfare'.[49] This confusion stems from both the rapid spread of cyber-warfare and the lack of precedent to guide international regulation of cyberspace intrusions.

The LOAC as understood today originated in the mid-nineteenth century, as did the humanitarian regulation of conflict and violence.[50] Since their early beginnings these laws applied primarily to interstate conflict as carried out by uniformed armed forces between two or more states. The principles, rules and norms that guide today's LOAC can be found in a variety of sources: customary law, international treaties, judicial decisions, the works of legal philosophers and military manuals. Although the customs of the LOAC can be traced as far back as medieval

[46] Karta Flook, 'Russia and the cyber-threat', *Critical Threats*, 13 May 2009, http://www.criticalthreats.org/russia/russia-and-cyber-threat, accessed 19 Dec. 2009.

[47] Kevin Coleman, 'Russia's cyber-forces', *Defense Tech*, 27 May 2008, http://defensetech.org/2008/05/27/russias-cyber-forces/, accessed 20 Dec. 2009.

[48] Yaakov Katz, 'IDG bolstering computer defense', *Jerusalem Post*, 17 Dec. 2009, http://www.jpost.com/servlet/Satellite?cid=1260930892360&pagename=JPost%2FJPArticle%2FShowFull, accessed 11 Jan. 2010.

[49] LOAC or LOW doctrine is also identified using the legal term *jus in bello*, Latin for 'law/justice in war', to determine the just or unjust conduct of a war. See also n. 48 below.

[50] Sections of the LOAC that deal explicitly with civilians are commonly referred to as 'international humanitarian law'.

International Affairs 86: 2, 2010

Europe, its more modern origins date back to the American Civil War of 1861–5.[51] Until then, as Dale Stephens and Michael Lewis note, 'there was no meaningful *jus ad bellum* because the right to resort to force was essentially unchallenged'.[52]

In the Middle Ages, the ideals of knighthood provided some restraint against certain cruelties in warfare, but not until the seventeenth century was there a systematic legal code on war and peace. Hugo Grotius's work of 1625, *On the law of war and peace* (*De jure belli ac pacis*), was based on the natural law tradition, which was also the basis for the Golden Rule formulated by Emerich de Vattel in his 1758 work, *The law of nations* (*Droit des gens*). Another century passed until the American Civil War prompted the leading states of the world to codify and adopt the laws of armed conflict. The first Geneva Convention, agreed in 1864, employed the US Lieber Code (US War Department, General Order No. 100, 24 April 1863) as a baseline. In 1868 a treaty was signed in St Petersburg by leading nations and empires (but not the US) concerning regulation of the methods and means of warfare. It was with the ratification of this St Petersburg Declaration that for the first time emerging military technologies were subject to any type of international legal review. Among weapons of concern were exploding bullets, land mines, machine guns and dumdum bullets—all weapons regarded as causing unnecessary physical harm.

In 2009 the Committee on Offensive Information Warfare of the US National Research Council (NRC) produced an analysis of US cyber-attack capabilities. The committee states in the preface that it 'believes that the principles of the law of armed conflict (LOAC) and the Charter of the United Nations—including both law governing the legality of going to war (*jus ad bellum*) and law governing behavior during war (*jus in bello*)—do apply to cyber-attack, although new analytical work may be needed to understand how these principles do or should apply to cyber-weapons'.[53] Markoff and Kramer reported in the same year that the US State Department was looking to the Council of Europe Convention on Cybercrime as a model. This convention states that it recognizes the 'need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies'. To the Council's credit, it did take significant steps in attempting to deter cyber-crimes among its member states with the consideration of other states.[54]

[51] Jefferson Reynolds, 'Collateral damage on the twenty-first century battlefield', *Air Force Law Review* 56, 2005, p. 6.

[52] Dale Stephens and Michael Lewis, 'The law of armed conflict: a contemporary critique', *Melbourne Journal of International Law* 6: 1, May 2005, p. 4. For an interesting historical perspective on *jus ad bellum* and *jus in bello*, terms coined in the twentieth century, see Robert Kolb, 'Origin of the twin terms *jus ad bellum/jus in bello*', *International Review of the Red Cross*, no. 320, 31 Oct. 1997, http://www.icrc.org/web/eng/siteengo.nsf/iwplist163/d9dad4ee8533daefc1256b66005affef, accessed 15 Dec. 2010. Kolb writes in n. 1: '*Jus ad bellum* refers to the conditions under which one may resort to war or to force in general; *jus in bello* governs the conduct of belligerents during a war, and in a broader sense comprises the rights and obligations of neutral parties as well.'

[53] William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds, *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities* (Washington DC: National Academies Press, 2009), p. 3. http://www.nap.edu/openbook.php?record_id=12651&page=R9, accessed 11 Jan.2010.

[54] Markoff and Kramer, 'US and Russia differ on a treaty for cyberspace', p. 2. For the Council of Europe Convention on Cybercrime, see http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, accessed 11 Dec. 2009.

Treaty issues

In terms of constructing a multilateral treaty for cyberspace, one modern approach assumes that a treaty survives conflict if it does not pertain fundamentally to the conflict; in another, 'certain legal relations survive, treaties do not'. In classical international law 'treaties did not retain their effect during armed conflict; war existed beyond the realm of international relations—*bellum omnium contra omnes*'. A third approach asks 'whether the continued vitality of the treaty in question is consistent with the larger context in which it operates (such as the existence of Parties not involved in the conflict)'. Schmitt is concerned that twenty-first-century technology allows warriors to be isolated from their war acts. 'The further removed they are from their acts of war, the more difficult it will be for them to retain the humanitarian spirit that underlies the law of armed conflict.' Indeed, he warns that we may forget that the 'reality of armed conflict' is 'found only in the consequence of an act, not the act itself'.[55] Such a stark warning would seem to cry out for international society to explore more earnestly the formulation of conventions leading to a treaty for cyberspace. UN Secretary General Ban Ki-moon has called for more international engagement in cyber-warfare issues.[56]

Schmitt examines issues around the relation of the LOAC to cyber-warfare in terms of the principle of 'reverberating effects': 'The spreading dependence on highly interconnected information and communications systems implies particular risks of reverberating effects during information warfare.'[57] The open internet provides a venue where public and private, government and civilian networks and systems overlap and interpenetrate. Certain cyber-attacks may cause collateral damage grave enough to result in physical losses and injuries, whereas the damage or loss consequent on other cyber-disruptions may be difficult to demonstrate or quantify.

Regulating warfare post-Westphalia

Another challenge is that cyber-warfare, not unlike other means of twenty-first-century warfare, is coming of age in an era where the Westphalian state order is undergoing vast transformation. Since the borderless realm of cyberspace both ignores and challenges state boundaries, a hands-off policy may disrupt or destabilize cross-border transactions. As explained by US Navy Judge Advocate General Corps Vida Antolin-Jenkins,

> Cyberspace operations for the most part do not meet the criteria for 'use of force' as currently defined by international law. Defining the parameters of proportional response through analogy is possible, but creates clear dangers of definitional creep into other areas of international relations that have long been the subject of long and contentious debate.[58]

[55] Schmitt, 'Bellum Americanum', p. 411.
[56] Ban Ki-moon, 'Pay more attention to cyberwarfare, verification', remarks to Advisory Board on Disarmament Matters, United Nations, New York, 18 Feb. 2009, http://www.un.org/News/Press/docs/2009/sgsm12108.doc.htm, accessed 17 Dec. 2009.
[57] Schmitt, 'Bellum Americanum', p. 408.
[58] Vida M. Antolin-Jenkins, 'Defining the parameters of cyberwar operations: looking for law in all the wrong places?', *Naval Law Review* 51, 2005, p. 134.

International Affairs 86: 2, 2010

However, let us remember that US military leadership does not rule out responding with kinetic force to a cyber-attack. Upon formation of the USCYBERCOM, General Chilton declared in May 2009 that 'The Law of Armed Conflict will apply to this domain.'[59] USSTRATCOM defends the Pentagon's Global Information Grid at home and abroad through its Strategic Command Joint Task Force-Global Network Operations. Attempted penetrations of public and private systems number in the tens of thousands a day. General Chilton also noted that many attacks have been for the purposes of espionage, and that there can be an argument about the 'semantics of attack versus espionage and intrusion'.[60]

Treaty principles

As with other laws of armed conflict, the primary objective of a multilateral cyber-warfare treaty should be to regulate this method of warfare and its consequences. The potential for a major cyber-war is real, considering the number of countries currently committed to erecting offensive capabilities in cyberspace and from the comments and examples presented in the preceding sections of this article. This section reviews how some of the core LOAC principles could be used to guide future cyber-treaty discussions.[61]

Military necessity

According to the principle of military necessity, enemy forces are declared 'hostile'. So defined, they may be attacked at will, along with their equipment and supplies. A controversial aspect of this principle means that any civilians or civilian properties that directly contribute to the war effort may also be attacked. These targets include objects whose damage or destruction could be used to yield a military advantage. A corollary of this principle is that non-combatants and civilians making no direct contribution to the war effort, and whose destruction would provide no significant military advantage to the attacker, are immune from intentional attack. Thus, according to this principle, schools, banks and shops are not legitimate targets.

A particularly troubling aspect of military necessity when applied to cyber-warfare is where to draw the distinction between military and non-military systems and property. In conventional battle, there is generally a bright line that distinguishes civilian from military assets (e.g. green tanks carry soldiers; yellow buses carry children). In the borderless realm of cyberspace, the line is less than clear. Since the end of the Cold War, there has been a big push to offload a major share of military communications from defence to civilian networks. Essentially,

[59] Schogol, 'Official: No options "off the table" for U.S. response to cyber-attacks'.
[60] Bill Gertz, 'Cyber-warfare plans', *Inside the Ring*, 4 June 2009, http://www.gertzfile.com/gertsfile/InsidetheRing.html, accessed 11 Jan. 2010.
[61] The treaty principles stated in this section are adapted from the following studies: Anthony Aust, *Modern treaty law and practice* (Cambridge: Cambridge University Press, 2007); Michael Byers, *War law* (New York: Grove, 2005); W. Michael Reisman and Chris T. Antoniou, *The laws of war* (New York: Vintage, 1994); Anthony P. Rogers, *Law on the battlefield* (Manchester: Manchester University Press, 2004).

International Affairs 86: 2, 2010

economics drove this shift, although the military also sought to take advantage of new innovations offered by civilian networks.

However, as military and civilian networks become blurred, large swaths of public information infrastructure come to be at risk during an actual state of hostilities. In the heat of battle it may be extremely difficult for military commanders to sort out which nodes on the network service strategic purposes and which service civilian. Thus, digital convergence presents a direct challenge to the principle of military necessity. Resolving this issue will require greater engagement between international legal experts, military strategists and electronics engineers.

Distinction

The principle of distinction is designed to designate combatants from non-combatants. Under the current application of the LOAC, only members of a nation's regular armed forces are entitled to use force against the enemy. In an actual engagement, combatants must distinguish themselves from non-combatants. They must not use non-combatants or civilian property to shield themselves from attack. If lawful combatants are captured by the enemy, they may not be punished for their combatant acts, so long as they complied with the law of war. Lawful combatants are also required to be treated humanely in accordance with agreed standards for the treatment of prisoners of war, and they must be released promptly at the cessation of hostilities. Persons who commit combatant acts without authorization are subject to criminal prosecution.

Applying this principle to twenty-first-century cyber-warfare is especially difficult because many online attacks are launched far from any location where the enemy is present. Military lawyers have already struggled to apply this principle to drone warfare over ungoverned spaces, let alone cyberspace. If a cyber-attack is launched from thousands of miles away by an anonymous or covert force, there is no reliable way to apply this principle. The principle's applicability is further challenged if the attackers are non-military personnel, let alone civilians. According to the LOAC, lawful combatants must be trained in the law of war, serve under a genuine military command and be under the command of legitimate military officers. No state of hostilities was declared between Estonia and Russia in spring 2007; but had there been, non-uniformed Russian cyber-attackers acting under the direction of their state could be charged as in violation of the traditional LOAC.[62] The same charge would apply to the 2007 PLA attackers thought to have launched operation 'Titan Rain' in the UK against Whitehall, hitting several departments including the Foreign Office.[63]

[62] Coalson, 'Behind the Estonia cyber-attacks'.

[63] Richard Norton-Taylor, 'Titan Rain: how Chinese hackers targeted Whitehall', *Guardian*, 5 Sept. 2007, http://www.guardian.co.uk/technology/2007/sep/04/news.internet, accessed 29 Dec. 2009.

International Affairs 86: 2, 2010

Proportionality

The principle of proportionality prohibits the use of any kind or degree of force in excess of that needed to accomplish the military objective. It weighs the military advantage obtained against the corresponding harm inflicted. Proportionality requires a balancing test between the concrete and direct military advantage anticipated in attacking a legitimate military target and the expected incidental civilian injury. Attacks may be carried out against lawful military targets even if some collateral damage is foreseeable, unless this collateral damage is disproportionate to the military advantage likely to be attained. Typically, military advantage is not restricted to tactical gains, but is linked to the full context of war strategy.

As with military necessity, the fundamental challenge in applying proportionality to a cyber-attack is how to differentiate between civilian and military targets. During the 2003 US-led war on Iraq, coalition forces had to weigh the principle of proportionality when targeting large swaths of dual-use infrastructure such as water, energy and transport networks. Again, as with military necessity, there are many ambiguities when applying this principle to cyberspace attacks. For example, when coalition forces bomb an electricity plant in Baghdad, they must make sure that the damage done to the Iraqi military far outweighs that damage or injury to civilian users. The same principle would also have to be applied if a cyber-attack were used to disable a critical component of an energy or telecommunications network.[64] However, if the cyber-attack is launched against a piece of critical dual-use infrastructure from thousands of miles away, then the expected military benefit may be unclear. Once again, the increasing use of civilian infrastructure by the military, especially in the online world, makes the principle of proportionality especially difficult to apply to cyber-attacks.

Indiscriminate weapons

Since the First World War, nations have come together through the LOAC to ban the use of certain weapons with potential to cause grave damage beyond their original targets. Examples of banned indiscriminate weapons are poison gas and lasers. Both of these highly effective weapons, one old, one new, had the potential to cause massive injury and damage beyond their intended targets. Thus, militaries that use the public internet to distribute malicious code or malware could be viewed as violating the indiscriminate weapons principle.[65] For example, if a cyber force embedded malicious code on a public website that infected many more non-combatant than combatant systems, the act could be viewed as an indiscriminate weapons violation. Or if a country embeds 'back doors' or 'logic bombs' into hardware that is distributed well beyond their intended targets, the fouled

[64] Anthony P. Rogers, from explanation and comments during conversation with Rex Hughes, Lauterpacht Centre for International Law, Cambridge University, 2 Dec. 2009.

[65] Dorothy Denning, 'Ethics of cyber-conflict' (draft copy), Department of Defense Analysis of the Naval Postgraduate School, 27 Mar 2007, p. 16, http://faculty.nps.edu/dedennin/.../Ethics%20of%20Cyber%20Conflict.pdf, accessed 11 Dec. 2009.

International Affairs 86: 2, 2010

hardware could be considered an indiscriminate weapon. Again, because there is little consensus as to what constitutes a cyber-weapon, it is difficult to apply this principle meaningfully. Thus, it will likely take a major real world cyber event to reduce the ambiguity surrounding this principle.

Perfidy

Under the LOAC, the principle of perfidy is designed to regulate the targeting of certain facilities that are historically considered legal sanctuaries during a time of war, examples being all medical personnel and facilities, shelters and prisons of war. Typically these types of facilities are clearly marked with internationally recognized symbols (e.g. the Red Cross or Red Crescent). Military commanders or personnel are accordingly forbidden to transform legitimate military targets into *faux* sanctuaries by misusing symbols or their locations on military maps.

In cyberspace, the perfidy principle may apply should false sanctuary markings be placed on online systems used for military purposes. For example, were a state to re-brand an online military supply chain portal with Tesco logos, that act would be likely to constitute a violation of this principle. Military use of an academic network such as the UK JANET to facilitate the transfer of real-time command and control orders would also be viewed as a perfidy violation. Conversely, critical information systems serving hospitals or schools would need to be clearly identified in cyberspace in order to prevent these institutions falling prey to hostile cyber-attack. Issues of identification and authentication abound cyberspace, making virtually any attack a high risk venture.

Neutrality

The principle of neutrality was established to keep separate countries that wish to seek immunity from attack by withholding support for any particular side during open hostilities.[66] Switzerland, whose neutrality was established by the Congress of Vienna, has not fought a foreign war since 1815. National neutrality for EU member states has been debated since the Treaty of Lisbon, which came into force in December 2009, accepted the framework for a common foreign policy.[67] Declaration of neutrality imposes obligations on both foreign belligerents and the neutral country. The belligerents refrain from attacking the neutral country in exchange for a guarantee that the neutral country will not support the opposing force in terms of weapons, personnel or territory.

Like the other codes discussed above, the principle of neutrality is difficult to apply during actual cyber-hostilities because of the high degree of systems integration associated with most twenty-first-century communications networks. Since cyberspace is often described as a 'virtual' or borderless global commons, the

[66] The rights and duties of a neutral power are defined in the 1907 Hague Convention, nos.V & XIII, http://wwi.lib.byu.edu/index.php/Hague_Convention, accessed 17 Jan. 2010.

[67] 'Lisbon treaty: a fresh start for the EU', European Commission, 1 Dec. 2009, http://ec.europa.eu/news/eu_explained/091201_en.htm, accessed 17 Dec. 2009.

International Affairs 86: 2, 2010

task of applying the territoriality standard to cyberspace is difficult if not impossible.[68] The harsh reality is that most cyber-attacks, when orchestrated via the internet or other networked systems, may make use of network infrastructure in multiple countries. The coordinated attacks on Estonia in 2007 are estimated to have involved one million computers from 75 countries. Many, possibly most of those services were located in the US with the owners unaware of the intrusions.[69]

By way of a hypothetical situation, if Israel or South Korea mounted a military-sanctioned DOS attack on a known enemy via the internet, those TCP/IP (Transmission Control Protocol/Internet Protocol) packets would probably flow through routers in both allied and neutral countries. The choice of the word 'protocol' by the originators of the early internet connectivity standards is interesting, indicating a diplomatic handshake.[70] Foreign ministries and defence departments carry out their national duties through agreements, standards, treaties, protocols and/or handshakes. Thus, the TCP/IP standard underlies the internet that passes through the ether of countries around the globe.

In applying the classical standard of neutrality to cyber-intrusions, a neutral country could risk its neutral status.[71] A parallel could be found in the neutrality concept governing shipping to and from neutral country ports and related ctivities, including repairs and blockades. A highly globalized and networked world presents definite challenges to the application of the classic neutrality concept.

Even this brief review of the treaty principles that confront the thinkers and policy-makers concerned to maintain a peaceful, workable global networked society makes it clear that we face cyber-governance challenges vast in both number and scale. The considerable global challenges coming from cyberspace will not diminish.

Conclusion

As this article has attempted to show, rightly or wrongly cyberspace has indeed become the fifth battlespace. While much of the early thinking defining cyberspace as a war domain was carried out in the US during the final years of the Cold War, other leading cyber-powers have embraced this notion and are in the process of creating credible military capabilities for waging counter-attacks or offensive war in cyberspace. It is now up to international society to determine how best to regulate warfare or hostilities in this fifth battlespace.

[68] John R. Mathiason and Charles C. Kuhlman, 'International public regulation of the internet', paper presented to International Studies Association panel on 'Cyberhype or the deterritorialization of politics? The internet in a post-Westphalian order', 21 Mar. 1998, http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/mathiason.htm, accessed 11 Dec. 2009.

[69] Stew Magnuson, 'Cyber-attack: US plans to destroy enemy computer networks questioned', *National Defense*, 1 July 2009, http://www.thefreelibrary.com/Cyber-attack:+U.S.+plans+to+destroy+enemy+computer+networks...-a02035390 59, accessed 11 Dec. 2009.

[70] 'Vinton Cerf: internet protocols (TCP/IP)', Lemelson-MIT Program, http://web.mit.edu/invent/iow/cerf.html, accessed 11 Jan. 2010; 'Explanation of the three-way handshake via TCP/IP', Microsoft Support, http://support.microsoft.com/kb/172983, accessed 10 Jan. 2010.

[71] International Telecommunications Union, *A comparative analysis of cybersecurity initiatives worldwide* (Geneva, 10 June 2005), http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf, 23, accessed 11 Jan.2010.

In recent years cyber-weapons have constituted major aspects of RMA tactics and strategy. While some weapons have been hailed over the years as means to reduce casualties, few have made similar claims about cyber-arms. The truth is that no one truly knows what long-term impact information weapons will have in the practice of state aggression or declared war. Unlike warfare in the other four domains, thus far cyber-war is both relatively cheap and readily available, making it all the more alluring for small states and non-state actors to deploy their weapons of technological knowledge, information and skill. States, for their part, are fully capable of quietly exploiting the skills of hackers or so-called patriotic cyber-warriors. Cyber-warfare is also attractive as a means of circumventing the laws of war governing conventional arms. Therefore, it is imperative that international society consider how classic war principles can guide a new cyber-warfare regime.

While there is no guarantee that a cyber-treaty will prevent the digital equivalent of Pearl Harbor, the Blitz, Hiroshima or 9/11, the complete absence of any meaningful regulation or treaty infrastructure leaves the way open for a digital 'war against all'. Correcting this imbalance will take a concerted effort on the part of international society, especially the United States and the other cyber-powers—China, Russia, India and Japan. In the near term they could well look to the member states of the EU, middle powers like Israel, and South Korea, as well as NATO and other international military alliances, for assistance in shaping a new regime. While anarchy has always been a feature of the international system, it need not be the defining element of the global networked society. Time will tell what role a convention or a treaty might play in regulating or limiting the 'next war in cyberspace'.

International Affairs 86: 2, 2010