CYBER WARFARE

Julian Richards

[au: We have provided a Table of Contents for you. Please confirm that the heading levels are correct.] [Yes happy, although we might take out the General Issues and General Debates sub-headings – see below.]

Introduction

Since the mid-1990s, discussion around the prospect of cyber war has become an increasingly hot topic. Many countries now place defense against cyber attacks at the highest level of priority in their national security strategies. The normative view of the threat is that, for those countries with a high level of dependence on information technology and networked infrastructure, a major cyber attack has the potential to level the playing field of military capability to devastating effect, whether it emanates from a hostile state or a non-state actor such as a terrorist group. Events such as the cyber attacks against Estonian networks in 2007 have been seized upon by many as early salvoes in the new global cyber war. Critical perspectives, however, suggest that cyber activity is fundamentally different from activity in the physical world, and cyber attacks cannot be classified as acts of war as such. There is further suspicion that the level of threat has been overly militarized when its civil dimensions may be more important, and that military and corporate interest groups may be hypersecuritizing the threat for their own gain. Most of the analysis has been conducted in the dominant military power and one of the most network-dependent countries in the world, the US. Perhaps not surprisingly, many of the normative views of the military cyber threat point the finger squarely at China and, to a lesser extent, Russia, suggesting a new Cold War. Throughout the debate, most accept that cyber threats are real and are growing in complexity and potential impact. Analyzing the nature of cyber threat in the military realm delivers a number of complexities. Much has been written about the legal aspects of "acts of war", both from offensive and defensive perspectives, and how existing domestic and international regulation may be poorly designed to deal with cyber attacks. Governance of cyber capabilities and cyber defences is proving to be a complicated affair, cutting across traditional boundaries of public/private, civil/military and national/international. How to deliver deterrence in a cyber context has been considered extensively, with parallels often being drawn with the rise of the nuclear threat in the twentieth century. It is recognized in this fast-moving subject area that analysis of case studies of what may constitute cyber attacks will be important. These are examined from the perspectives of both specific incidents in space and time; and of specific technologies being used and how to counter them. Generally, cyber war is proving to be a very interdisciplinary subject, spanning ~~across~~ technical, legal, sociological and political realms. This makes it a vibrant new subject, but also a challenging one for academia, since the subject does not very easily sit within a single identifiable department. Within the general domain of Security Studies, most of the socio-political analysis has been rooted either in conflict studies, and especially the changing nature of postmodern conflict; or in securitization theory, and the manner in which the threat is emerging from political discourse. But these are not the only directions from which the subject is being, or should be approached.

General Overviews ~~Books~~ [au: We suggest simply including the 'books' here in the main "general overviews" section and revising "reports" to stand alone as a level-one heading. This helps the ToC to be more descriptive and easier to navigate. Edit OK?] [Yes happy with that]

Given the heightened interest in cyber threats generally, a number of books have emerged recently on the perceived threat of cyber war. Most of these are written by US authors and take a US-centric perspective on the issue, noting the fact that the particular dependence on networked infrastructure in the US military and in society in general could prove to be the country's greatest weakness in the event of conflict. Many commentaries are also concerned with how the US government should position its cyber defense strategies, with many taking a critical view of progress made in this area. The normative view presented by most books in this field is that the threat of cyber war has gone beyond a hypothetical possibility and is present today. Clarke and Knake 2010, through the former's position as a National Coordinator on Security, Infrastructure Protection and Counterterrorism under four former US presidents, promotes this view and suggest that US cybersecurity policy is not yet fit for purpose. Geers 2011, working from a position within NATO's Cooperative Cyber Defence Center of Excellence in Estonia, agrees that the threat is a major one to international security. Kramer, Starr and Wentz 2009 present a similar thesis with some policy recommendations, as does Rosenzweig 2013. Carr 2010, and the edited volume Latham 2003, provide some deep analysis of the nature of the cyber war threat and its complex intermingling with other threat vectors such as crime, activisim and terrorism. Denning 1998 and Healey 2013 provide~~s~~ a similar analysis of the changing nature of threat in this area, drawing some interesting parallels with information warfare through history. Rid 2013 offers a rare critical reading of the normative view of cyber war, and does so from a non-US perspective. Richards 2014 is similarly sceptical about whether any of the events seen so far constitute acts of war, while suggesting that the pace of technological change means that such an eventuality in the future cannot be ruled out.

Carr, Jeffrey. *Inside Cyber Warfare.* Sebastopol CA: O'Reilly Media Inc (2010).

A comprehensive and valuable overview of the threat landscape, which notes the complex blurring of boundaries between different types of cyber threats and activities.

Clarke, Richard A., and Knake, Robert K. *Cyber War: The Next Threat to National Security and What to do About it.* New York: HarperCollins (2010).

A detailed and pessimistic assessment of the threats from cyber war to the US and its ability to formulate suitable policy responses.

Formatted: Indent: Left: 0 cm

Formatted: Font: Italic

Geers, Kenneth. *Strategic Cyber Security*. Tallinn: CCDCOE (2011)

Published by the US's representative at NATO's cyber security centre in Estonia, this study suggests the cyber threat has evolved from a computer security issue to a major strategic threat to national and international security.

Formatted: Indent: Left: 0 cm

Formatted: Font: Italic

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna VA; Cyber Conflict Studies Association (2013)

A fascinating historical account from a former cyber warrior in the US Air Force, which concludes with the assessment that a deadly cyber attack has not yet been seen.

Denning, Dorothy E. *Information Warfare and Security*. New York: ACM Press, 1998.

A data-rich overview of cases from a Professor of Computer Science at Georgetown University, which draws some interesting parallels with cases of information warfare in history.

Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry, eds. *Cyperpower and National Security*. Dulles VA: Potomac Books, 2009.

A useful edited volume, written in response to a requirement from the US Under Secretary for Defense, to establish national security policy guidelines in the face of cyber attacks.

Latham, Robert, ed. *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York: New Press (2003).

An edited volume containing chapters by many of the leading scholars in the field, which explore the changing boundaries between actors and sectors in traditional notions of security with the advent of the information revolution.

Formatted: Indent: Left: 0 cm

Formatted: Font: Italic

Richards, Julian. *Cyber War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan (2014)

A condensed overview of the question of how cyber war can be defined, taking a cautiously critical line that suggests it has not yet been seen in terms of a traditional understanding of acts of war.

Rid, Thomas. *Cyber War Will Not Take Place*. London: Hurst and Co (2013).

A ~~more s~~ceptical assessment of the threat of cyber warfare, while accepting that cyber threats of a different nature are real and potentially serious.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara CA: Praeger (2013).

Attempts to outline the seriousness of the risks while emphasising that there are also many benefits and opportunities in the Information Age.

Reports

In addition to books on the subject, a number of research institutes, think tanks and security companies with involvement in the IT industry have generated reports on the cyber threat. This is not surprising given that the topic is not only an academic one, but one of high and rapidly developing technical and policy interest. In some cases, major IT security companies such as Kaspersky, McAfee and Symantec Corporation produce regular bulletins on cyber threats, updating information on new exploits being seen in cyberspace. Cornish, Livingstone, Clemente and Yorke (Chatham House 2010) focus on cyber defense policy considerations from a transatlantic perspective, while Wilson (CRS 2007) does the same for the US government. Kurtz, DeCarlo and Simpson (McAfee 2009) present a detailed analysis based on extensive surveying of companies' experiences of cyber attacks, and stress the manner in which cyber defense governance will need to span public and private sectors. Meanwhile, one of the more infamous reports on cyber war appeared in 2013 from the US-based cyber security consultancy Mandiant, which pointed the finger resolutely and robustly at the Chinese People's Liberation Army's (PLA) sponsorship of continual and very large-scale cyber espionage and attack against the West, including the development of sophisticated Advanced Persistent Threats (APTs). The issue of confrontation between the West and China on cyber threat is explored further ~~below~~. [au: Please clarify this reference by instead mentioning the specific section you are referring to (e.g. "…Further explored in *Case Studies in Cyber War*").] in the section The New Cold War.

Cornish, Paul, Livingstone, David, Clemente, Dave and Yorke, Claire. *On Cyber Warfare*. London: Chatham House (November 2010).

A useful analysis of the complexity of the cyber threat, placing particular emphasis on the importance of transatlantic cooperation in confronting the threat.

Kurtz, Paul B., DeCarlo, David W. and Simpson, Stacey. *Virtually Here: The Age of Cyber Warfare.* Santa Clara CA: McAfee Virtual Criminology Report (2009).

Notes the gradual rise of attacks possibly connected to nation-states, and stresses that the private sector will find itself in the front line of protecting critical networks.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. Alexandria VA: Mandiant (2013)

A widely-publicised report which claimed to expose a PLA unit at the source of continual cyber espionage and attack against the West.

Wilson, Clay. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. Washington DC: CRS Report for Congress (20 March 2007).

A useful overview of the place of information operations (IO) within the US defense capability, including an awareness of psychological, ethical and policy considerations for the US government in undertaking offensive cyber operations.

Journals

The question of cyber threats, including cyber war, is proving to be a very multidisciplinary concern. At one level, the issues are deeply technical, relating to computer science and information networks. At the same time, the topic is generating a great deal of debate and analysis in law, politics, international relations, psychology and sociology. This means that debate and analysis about cyber war can be found scattered across a range of journals across several disciplines. The Institute of Electrical and Electronic Engineers (IEEE) publishes a range of magazines and journals at the more technical end of the spectrum, in which debates and analyses on various aspects of cyber war can be found. **IEEE Security and Privacy**, and **IEEE Network** are two good sources of debate. **Information Security Journal: A Global Perspective**, is one of the few journals that brings together technical discussions alongside bigger-picture analyses of political and sociological aspects of the cyber threat. Papers on these “human factor” elements of the cyber debate are otherwise spread across a wide range of political and sociological journals. Particularly useful sources include the **Journal of Strategic Studies**, which has recently published within its pages a wide-ranging and vibrant debate between normative and critical views of the threat of cyber war. Other good sources within the general security realm include **Security Dialogue**, and **Strategic Studies Quarterly**. Meanwhile, the proceedings of an increasing number of international conferences on the subject can be very fruitful sources of research. The International Conference on Cyber Warfare and Security is particularly vibrant, especially on technical issues, while NATO's annual conference at its Tallinn Center of Excellence offers both technical and strategic tracks, with high-level speakers in the field.

Information Security Journal: A Global Perspective[http://www.tandfonline.com/loi/uiss20#.UtR6MtJdXTo]

A Taylor and Francis journal aimed at information security professionals and government policy-makers in security and network defense. Focuses primarily on technical issues, but includes wider discussions about the threat.

Journal of Strategic Studies[http://www.tandfonline.com/loi/fjss20#.UtR6SdJdXTo]

First published in 1978, focusing on the strategic studies, politics and international relations end of the spectrum of debate about security more generally, with a healthy level of discussion about emerging cyber threat issues.

Network (IEEE)[http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=65]

A bi-monthly magazine published by the IEEE Communications Society, which focuses on network design and management issues, but includes more general perspectives on cyber attacks from a technical viewpoint.

Formatted: Indent: Left: 0 cm

Proceedings of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) International Cyber Conference [NATO, Tallinn]

Proceedings of the increasingly significant international conference on both technical and strategic aspects of cyber security, hosted by NATO's cyber centre of excellence, established in Tallinn in 2008.

Formatted: Indent: Left: 0 cm

Proceedings of the International Conference on Cyber Warfare and Security (formerly International Conference on Information Warfare and Security) [citations indexed by Thomson Reuters - http://thomsonreuters.com/conference-proceedings-citation-index/]

One of the more significant international conferences on the technical aspects of cyber warfare and security. Papers feed into the International Journal of Cyber Warfare and Terrorism [IGI Global] and International Journal of Electronic Security and Digital Forensics [Inderscience]

Security Dialogue[sdi.sagepub.com/]

Edited in the Peace Research Institute in Oslo, looks at changes and developments in global security from contemporary and historical perspectives.

Security and Privacy (IEEE)[http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013]

Published by the IEEE Computer Society, aims at a broad range of security practitioners and analysts across industry and academia.

Strategic Studies Quarterly[www.au.af.mil/au/ssq/]

Sponsored by the US Air Force, includes a wide range of debates and discussions about national and international security issues, primarily from the perspective of US national security practitioners and policy-makers.

Assessments ~~Standard views~~ of the threat

Assessments of the threat of cyber war tend to encompass two points of view. The standard and normative view of the threat of cyber war can be characterized as it being a real and present threat, of potentially disastrous consequences for the victim's state and society. Most of the proponents of this view are based in the US, where fear of cyber war is strong on account of how far the military and society generally have become network-dependent in recent years. ~~Many US-based analysts also take a fairly dim view of the US administration's perceived inability to develop an adequate cyber security strategy in the face of the threat, despite lofty official words about the seriousness of it. Arquilla and Ronfeldt 1993 offers an early assessment of the threat of cyber war, written on the back of the first Gulf War in 1991.~~ Choucri and Goldsmith 2012 warns about the international ramifications of cyber conflict~~, while Libicki 2009 highlights the attractiveness of offensive cyber approaches to nations with weaker military capabilities and resources~~. ~~Grant 2007 and~~ Lynn 2010 outlines how cyber war is being built into US military strategy. Stone 2013, in riposte to the critical thesis of Rid (cited under *General Overviews*), argues that cyber attacks *can* be classified as acts of war and are inevitable. McConnell 2010 fires a broadside at the US government's inability to develop an adequate counter-attack strategy to what he characterizes as a very real and present threat~~, while Stiennon 2010 further emphasises that the threat is large and imminent, and that China is the key threat~~. Meanwhile, critical analyses of cyber war confront the normative view in two main ways. Firstly, doubt is cast over the suggestion that cyber attacks that can realistically be described as acts of war have yet taken place. Secondly, there is a suggestion that official thinking on the emergence of the cyber threat has been over-militarized, and, in some cases, "hypersecuritized", using the Copenhagen School's constructivist notion of securitization, in order to suit bureaucratic and corporate agendas. Liff 2012 makes the claim that a true act of cyber war has not yet taken place, despite various events being labelled as such. Lawson 2011 and Samaan 2010 argue that the US in particular has tended to see the cyber threat inappropriately through military lenses and thus mischaracterized it. Rid's 2012 critical thesis about the true reality of the cyber war threat is directly countered by Arquilla 2012 and Stone 2013.

Arquilla, John. "Cyberwar is Already Upon Us." *Foreign Policy* 192 (March/April 2012): 84-85

In a rebuttal of Thomas Rid's article in the same edition of Foreign Policy (see below), and picking up on a seminal paper written jointly with David Ronfeldt in the early 1990s, argues that cyberwarfare is a contemporary reality.

~~Arquilla, John, and Ronfeldt, David. "Cyberwar is coming!" *Comparative Strategy* 12/2 (1993): 141-165~~

Formatted: Font: Italic

Formatted: Indent: Left: 1.27 cm

~~Written on the back of rapid victory in the 1991 conflict with Iraq, argues that future conflict will be all about information operations and information superiority.~~

Choucri, Nazli, and Goldsmith, Daniel. "Lost in Cyberspace: Harnessing the Internet, international relations, and global security." *Bulletin of the Atomic Scientists* 68/2 (2012): 70-77

Argues that the threat of cyberwar is real and potentially destabilizing to international relations and security.

Lawson, Sean. "Articulation, Antagonism and Intercalation in Western military imaginaries." Security Dialogue 42/1 (2011): 39-56.

A deeply theoretical paper that concludes that Western militaries may have over-securitized the threat of cyber war in order to justify military modernization and the use of force.

~~Grant, Rebecca. *Victory in Cyberspace.* Arlington VA: Air Force Association, 2007~~

~~Takes as a starting point the official US military doctrine that serious cyber attack is inevitable, and outlines the way in which the Air Force will tackle the threat.~~

~~Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica CA: RAND Corporation, 2009.~~

~~Argues that, because costs for an aggressor in cyberwar are cheaper than in conventional conflict, states will inevitably take the decision to embark on major cyberwar at some stage in the future.~~

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." Journal of Strategic Studies 35/3 (2012): 401-28.

Argues that much analysis of cyber war is "under-theorized", not least as a true act of cyber war has not yet taken place.

Lynn, William J. "Defending a New Domain." *Foreign Affairs* 89/5 (2010): 97-108.

The former US Deputy Secretary of Defense argues that the cyber domain has become just as critical to defense as land, sea, air and space.

McConnell, Mike. "How to win the cyber-war we're losing." *The Washington Post* (28 February 2010).

A seminal article by a former director of National Intelligence in the US, which argues that the US is sleep-walking into defeat in a real cyber-war.

Rid, Thomas. "Think Again: Cyberwar". *Foreign Policy* 192 (March/April 2012): 80-84

Critiques the notion put forward by Arquilla 2012 (in the same journal), among others, that the threat of cyber war is real and present.

Formatted: Indent: Left: 0 cm

Formatted: Font: Italic

Samaan, Jean-Loup. “Cyber Command: The Rift in US Military Strategy.” The RUSI Journal 155/6 (2010): 16-21

A useful article which outlines the two perspectives on cyber war within the US administration, and argues that the problem has been characterized inappropriately through the lens of previous experiences of war and military threat.

Stone, John. “Cyber War *Will* Take Place!” *The Journal of Strategic Studies* 36/1 (2013): 101-108.

Partly as a riposte to Rid’s earlier article in the same journal (repeated in ~~the book below~~ [au: Please specify which work you are referring to here.] his 2013 book of the same name: see General Overviews), and using strategic theory as a construct, Stone argues that cyber attacks could indeed be equated to acts of war.

~~Stiennon, Richard. *Surviving Cyber War.* Lanham MD: Government Institutes, 2010.~~

~~Offers a detailed standard view of the immediacy and seriousness of the cyber threat to the West, pointing the finger resolutely at China as the prime culprit.~~

~~**Critical views of the threat**~~

~~Critical analyses of cyber war confront the normative view in two main ways. Firstly, doubt is cast over the suggestion that cyber attacks that can realistically be described as acts of war have yet taken place. Secondly, there is a suggestion that official thinking on the emergence of the cyber threat has been over-militarized, and, in some cases, “hypersecuritized”, using the Copenhagen School’s constructivist notion of securitization, in order to suit bureaucratic and corporate agendas. It should be noted that, while these critiques are offered, many of their protagonists do accept that serious cyber threats are emerging. Lewis 2012, for example, recognizes the seriousness of developments while suggesting that threats to critical infrastructure have been overstated. Liff 2012 makes the claim that a true act of cyber war has not yet taken place, despite various events being labelled as such. Lawson 2011 and Samaan 2010 argue that the US in particular has tended to see the cyber threat inappropriately through military lenses and thus mischaracterized it, while the author of Schneier 2004, who is emerging as one of the most vocal and public critics of the normative view of imminent cyber catastrophe, suggests that the problem is not technical but one of user behaviour and management.~~

~~Lawson, Sean. “Articulation, Antagonism and Intercalation in Western military imaginaries.” Security Dialogue 42/1 (2011): 39-56.~~

~~A deeply theoretical paper that concludes that Western militaries may have over-securitized the threat of cyber war in order to justify military modernization and the use of force.~~

~~Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington DC: Center for Strategic and International Studies (CSIS), 2012~~

~~Argues that, while society is becoming more networked and thus more vulnerable in one sense, the risk of catastrophic threats to critical national infrastructure has been overstated.~~

~~Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." Journal of Strategic Studies 35/3 (2012): 401-28.~~

~~Argues that much analysis of cyber war is "under-theorized", not least as a true act of cyber war has not yet taken place.~~

~~Samaan, Jean-Loup. "Cyber Command: The Rift in US Military Strategy." The RUSI Journal 155/6 (2010): 16-21~~

~~A useful article which outlines the two perspectives on cyber war within the US administration, and argues that the problem has been characterized inappropriately through the lens of previous experiences of war and military threat.~~

~~Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. Indianapolis: Wiley, 2004.~~

~~From the arch-critic of traditional views of cybersecurity threats, argues that cyber threat is not a technical problem at all but one of sensible risk management.~~

Cyber and the changing nature of conflict

A number of security analysts have observed how threats in the cyber realm appear to be developing in ways which challenge traditional notions of military conflict between states, and, rather like globalization generally, threaten to challenge Westphalian notions of nation-states and their jurisdiction over conflict. Cyber war promises such developments through the complex and often anonymized nature of actors in the conflict, taking much further the difficulties of combatant status that have started to emerge in post-Cold War asymmetric conflicts. Ayers 1999 offers an early assessment of how conflict could evolve with cyber attacks and the sort of challenges this will present, while Mumford 2013, Rattray and Healey 2010, and Korns 2009 develop these ideas a decade later, focusing particularly on the confusing roles of combatants, civilians, and victims in the new conflict arena. Arquilla and Ronfeldt's 1997 edited volume presages what are perceived to be destructive new possibilities for states considering cyber attacks on their adversaries. Nye 2010 also highlights the new power possibilities for smaller and weaker states presented by cyber capabilities, while Kohlmann 2008 notes how network connectivity and the information economy allow the local conflict to be taken to the global stage. Brenner 2009 argues that the traditional defensive structures of nation-states look increasingly inappropriate to defend against cyber attacks.

Arquilla, John and Ronfeldt, David. "A New Epoch – and Spectrum – of Conflict." In ~~In~~ *Athena's Camp: Preparing for Conflict in the Information Age*. Edited by John Arquilla and David Ronfeldt, 1-20. Santa Monica CA, RAND Corporation, 1997.

Formatted: Font: Italic

The opening chapter of an edited volume which takes as a given that cyber operations will present new and destructive opportunities for conflict.

Ayers, Robert. “The New Threat: Information Warfare.” The RUSI Journal 144/5 (1999): 23-27

Based on a speech delivered at an Information Warfare conference at RUSI in 1998, usefully outlines the changing nature of actors in cyber war as opposed to traditional state-on-state war, and the challenges this presents.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press, 2009.

Formatted: Font: Italic

Outlines the changing nature of actors and modalities in cyber attacks, and argues that it is becoming virtually impossible for state militaries and law enforcement agencies to adequately counter the problem.

Kohlmann, Evan F. “Homegrown Terrorists: Theory and Cases in the War on Terror’s Newest Front.” The Annals of the American Academy of Political and Social Science 618/1 (2008): 95-109.

Focusing on transnational terrorist threats, argues that information technology allows previously local disputes and issues to be internationalized and to become wider transnational threats.

Korns, Stephen W. “Cyber Operations: The New Balance.” Joint Force Quarterly 54 (2009): 97-102

Suggests that the West needs to grasp the “new normalcy” in conflict, where civilian noncombatants and industry will increasingly be at the centre of the military theater.

Mumford, Andrew. “Proxy Warfare and the Future of Conflict.” The RUSI Journal 158/2 (2013): 40-46

An interesting article which argues that cyber capabilities will contribute to a rapidly changing nature of conflict, alongside other factors such as a reluctance to become embroiled in asymmetric counter-insurgencies.

Nye, Joseph S. “Cyber Power”. Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

Argues that the nature of cyberspace offers new opportunities for smaller actors in the global space to exercise both hard and soft power more effectively.

Rattray, Gregory, and Healey, Jason. “Categorizing and Understanding Offensive Cyber Capabilities and their Use.” Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy (2010): 77-97

Notes that cyber operations need to be conceptualized differently from those in existing military domains, since they comprise both physical and logical components.

Crossovers with other threats

One of the key premises of critical approaches to the question of cyber war is the suggestion that cyber threats have been characterized as military threats, when they should more appropriately fall into other categories. At the same time, it seems to be the case that offensive activities over networks blur many of the traditional threat boundaries, and, in many cases, may not be easily categorised at all using traditional frameworks. A number of analysts lay claim to other types of cyber threat being more important than military threats. Filshtinskiy 2013, for example, suggests that cyber crime is far more prevalent and potentially damaging to economies. Stohl 2006 argues that activist activity over the internet has often been mischaracterized as serious cyber attack, although Sterner 2012 warns of the manner in which cyber capabilities are increasing the disruptive power of political protest (albeit in a somewhat paradoxical way for the protestors). Applegate 2011 explores the increasingly blurred crossover between cyber activists and combatants. With a particular reference to the threat of cyber terrorism, Weimann 2004 suggests that social and psychological anxieties have caused cyber threats in general to be exaggerated, while Klimburg 2011 argues persuasively that it may be increasingly impossible to disentangle acts of war, terrorism and crime in the cyber realm. Lachow 2009, meanwhile, assesses that the true threat of serious cyber terrorist attacks is very low at the present time.

Applegate, Scott D. "Cybermilitias and Political Hackers – Use of irregular Forces in Cyberwarfare". IEEE Security and Privacy 9/5 (2011): 16-22

A useful article which explores the manner in which cyber methods are blurring the boundaries between activists and combatants in contemporary conclict scenarios.

Formatted: Indent: Left: 1.27 cm

Filshtinskiy, S. "Cybercrime, Cyberweapons, Cyber Wars: Is there too much of it in the air?" Communications of the Association for Computing Machinery 56/6 (June 2013): 28-30

Suggests that the debate has been hijacked by military considerations, when cybercrime is far more advanced and more of a reality than cyber warfare.

Klimburg, Alexander. "Mobilising Cyber Power." Survival 53/1 (2011): 41-60

Suggests that the boundary between cyber crime, terrorism and war is often "razor thin", and will determine the way that states use cyber power in the future.

Formatted: Indent: Left: 0 cm

Formatted: Font: Italic

Lachow, Irving. "Cyber Terrorism: Menace or Myth?" In *Cyberpower and National Security.* Edited by Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry. Dulles VA: Potomac Books, 2009

Assesses that the threat of cyber terrorism is very low at the current time, given the difficulty of mounting a sophisticated attack and the lack of expertise available to terrorist groups.

Formatted: Indent: Left: 0 cm

Sterner, Eric. "The Paradox of Cyber Protest". Arlington VA: George C Marshall Institute, Policy Outlook, April 2012

Argues that the newly emerging cyber dimension to political protest could make this a more damaging threat to internal security than has traditionally been the case.

Stohl, Michael. “Cyber terrorism: a clear and present danger, the sum of all fears, or breaking point or patriot games?” Crime Law Social Change 46/4-5 (2006): 223-238

Suggests that the cyber threat debate has become confused over the use of digital technologies for organization and activism, and the actual risk of cyber attacks.

Weimann, Gabriel. “Cyberterrorism: How real is the threat?” Washington DC, United States Institute for Peace. Special Report no.119, December 2004.

Argues that psychological, political and economic drivers concerning the fear of cyber attacks on public and defense infrastructure have caused the threat of cyber terrorism to become exaggerated.

~~Cyber war and ~~T~~t~~he New Cold War~~?~~ [au: Revised to avoid taking the form of a question in the heading, and to avoid repetition of the article’s title in the TOC wherever possible, per House guidelines. Edit OK?] [Yes fine]

An over-militarization of thinking about cyber threats, coupled with a predominantly US-centric viewpoint in much of the analysis, may be leading to a characterization of the threat of cyber war in distinctly Cold War rhetoric. In particular, apparent evidence that much offensive cyber activity appears to be emanating from networks in China and Russia (notwithstanding attribution problems outlined in *The Attribution Problem*) has led many analysts and governments in the West to suggest that the new Cyber War, if it comes, will be between the US and its former Cold War adversaries. Wortzel’s 2010 testimony to the US House of Representatives is one of many examples of the scale and nature of the purported wave of attacks from China. Much of the anti-China normative thesis in the US centers around a short publication purportedly published by two senior People’s Liberation Army (PLA) colonels, Liang and Wang 1999, called Unrestricted Warfare. This appears to be a manifesto for making cyber attack a lynch pin in a future confrontation with the US. Newmyer 2010 picks up on this theory, while Hjortdal 2011 suggests that such an approach makes perfect sense to an expansionist China. Thomas 2012 suggests that a blurring of the boundaries between espionage, activism and cyber attack makes perfect sense for the Chinese as an asymmetric strategy to use against its adversaries. Barrett 2005 suggests that a US-Sino conflict with cyber dimensions is inevitable in the medium term. From a Chinese perspective, Xu 2011 offers a rare word of moderation, noting that mutual recriminations over cyber attacks are not helping to lower diplomatic temperatures. On the Russian front, meanwhile, Anderson 2007 and Giles 2011 both note the Russian military’s efforts to develop advanced information warfare capabilities, not least to ensure parity with the West; a distinctly Cold War notion of security dilemma.

Anderson, Julie. “The HUMINT Offensive from Putin’s Chekist State.” International Journal of Intelligence and Counterintelligence 20/2 (2007): 258-316.

Argues that Russian Human Intelligence-gathering (HUMINT) activities are continuing apace, and that cyber-espionage and positioning for cyber-attack against the US are enabled by such factors as collaboration with Cuba.

Barrett Jr., Barrington M. “Information Warfare: China’s Response to US Technological Advantages.” International Journal of Intelligence and Counterintelligence 18 (2005): 682-706.

Suggests that a US-Sino conflict over Taiwan is “inevitable in the next five to ten years” (p.703), and that understanding Chinese Information Operations and Warfare capabilities is therefore a high priority. [au: Please provide page number for this quotation.]

Giles, Keir. “”Information Troops” – A Russian Cyber Command?” In 3rd International Conference on Cyber Conflict (ICCC), 2011. Edited by Czosseck, C., Tyugu, E. and Wingfield, T. 45-60. Tallinn: CDD COE Publications, 2011.

Argues that there is evidence of Russia increasingly seeing the need to integrate information warfare capabilities into its military, largely as a reaction to developments in the US and elsewhere on this issue.

Hjortdal, Magnus. “China’s Use of Cyber Warfare: Espionage meets Strategic Deterrence.” Journal of Strategic Security 4/2 (2011): 1-24.

Argues that China has good reason to use cyber warfare as part of its policy of power accumulation, and presents examples of where it has already purportedly attacked and spied upon US military capabilities using cyber means.

Liang, Qiao, and Wang, Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House (1999).

Formatted: Font: Italic

Written by two senior People’s Liberation Army (PLA) colonels, claims to be a manifesto for countries such as China to use asymmetric tactics in a major conflict with the US, and in particular promotes the merits of striking at the US’s much greater dependence on electronic networks.

Newmyer, Jacqueline. “The Revolution in Military Affairs with Chinese Characteristics.” The Journal of Strategic Studies 33/4 (2010): 483-504.

Picks up on a widespread theory that China sees new opportunities in asymmetric war with cyber capabilities at the vanguard, but suggests that such optimism vis-a-vis supremacy over the US will prove to be misplaced.

Formatted: Indent: Left: 0 cm

Thomas, Timothy L. *Three Faces of the Cyber Dragon*: *Cyber Peace Activist, Spook, Attacker*. Leavenworth KA, Foreign Military Studies Office, 2012

Formatted: Font: Italic

Formatted: Font: Italic

Using a deep analysis of Chinese culture, suggests that China will use skilful strategies to conduct asymmetric cyber warfare by blurring the boundaries between espionage, activism and attack.

Formatted: Indent: Left: 0 cm

Wortzel, Larry M. “China’s Approach to Cyber Operations: Implications for the United States”. Testimony before the House of Representatives Committee on Foreign Affairs, Washington DC, 10 March 2010

Testimony from a former military intelligence officer, and commissioner in the US-China Economic Security Review Commission, underlining apparent evidence of a continual flow of malicious cyber attacks emanating from China and directed towards American government, business and infrastructure.

Xu, Ting. “China and the United States; Hacking away at Cyber Warfare.” Asia Pacific Bulletin 135 (2011): 1-2

Suggests that mutual recriminations between China and the US over cyber attacks are raising the diplomatic temperature, and argues that the subject must become a meaningful part of dialogue between the two nations.

Case Studies ~~in cyber war~~

The fact that there is disagreement over whether cyber attacks can appropriately be characterized as acts of war means that detailed analysis of specific case studies of cyber attacks are important. The general view appears to be emerging that cyber war comprises two activities: direct attacks over networks on military or civilian assets leading to real or potential injury and damage; and activities that accompany and enable physical military activities, such as suppression of air defences, or information operations. Good examples of the latter include the ongoing offensive cyber activity between Hezbollah and Israel, as described in Al-Rizzo 2008, and Israel’s suppression of Syrian air defences in its 2007 attack on a nuclear reactor, described in Fulghum 2007. Deibert, Rohozinski and Crete-Nishihata 2012 also describes the panoply of cyber attacks that appeared to support Russia’s military attack on Georgia in 2008. This conflict, and the 2007 attacks on Estonian networks that appear to have originated in Russia, as described in Herzog 2011, are much-quoted - and much debated – examples of real acts of cyber war, although attribution of the authors of the attacks is hotly contested. In terms of more direct and potentially more serious cyber attacks on infrastructure, Bronk and Tikk-Ringas 2013 examines the 2012 attack on computers at an Aramco oil refinery in Saudi Arabia, which had the potential to cause serious disruption to global energy supplies. The king of cyber attacks to date, however, and described by many as the first real act of cyber war, is the “Stuxnet” malware attack on the Natanz nuclear installation in Iran, discovered in 2010. Farwell and Rohzinski 2011, and Langner 2011 both examine the Stuxnet episode and both describe the malware as the first “cyber weapon” worthy of the name.

Al-Rizzo, Hasan M. “The undeclared cyberspace war between Hezbollah and Israel.” Contemporary Arab Affairs 1/3 (2008): 391-405.

Explores the gradual development of persistent cyber attacks in the low-level conflict between Hezbollah and the Israeli state.

Bronk, Christopher, and Tikk-Ringas, Eneken. “The Cyber Attack on Saudi Aramco.” Survival: Global Politics and Strategy 55/2 (2013): 81-96

Outlines a 2012 attack on a Saudi Aramco facility using a self-replicating virus called “Shamoon”. Although the operations of the plant were not seriously disrupted, the attack reflected a potentially serious attack on an element of critical infrastructure.

Deibert, Ronald J., Rohozinski, Rafal and Crete-Nishihata, Masashi. “Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war.” Security Dialogue 43/1 (2012): 3-24

Analyses in useful detail the multiple layers of cyber activity in the 2008 Russia-Georgia war, and suggests that knowledge of these events will inform analysis of future conflicts.

Farwell, James P., and Rohozinski, R. “Stuxnet and the Future of Cyber War”. Survival: Global Politics and Strategy 53/1 (2001): 23-40

Picks up on the characterisation of Stuxnet as a “military grade cyber missile” and suggests that this episode shows the connection between advanced states and offensive cyber capabilities.

Fulghum, David A., Wall, R., and Butler, A. “Cyber-Combat’s First Shot.” Aviation Week and Space Technology 167 (16 November 2007): 28-31.

A detailed and useful account of the Israeli air force’s cyber-enabled attack on Syria’s Dayr-Ez Zor nuclear reactor in 2007.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” Journal of Strategic Security 4/2 (2011): 49-60.

Argues that the activities of “hacktivists” in the Estonian case suggests a potential capability to attack a range of targets, including weapons systems and military infrastructure.

Langner, Ralph. “Stuxnet: Dissecting a Cyberwarfare Weapon.” IEEE Security and Privacy 9/3 (2011): 49-51.

Argues that Stuxnet represented a new high water-mark of malware complexity, and constituted the “first cyber warfare weapon” (p.49). [au: Please provide page number for this quotation.]

Techniques and approaches ~~in cyber warfare~~

One of the complexities of cyber war is that, while many nations perceive themselves at threat of cyber attack and at pains to develop effective defensive strategies and capabilities, most of those same nations are avowedly developing offensive cyber capabilities to use against adversaries themselves. Rather like the Cold War characterization, this follows the logic that the best form of defense, and indeed of deterrence (~~on which more below~~See *Deterrence Strategies* [au: Please confirm this is the correct section being referenced.]) [Yes that's right] may be attack. Indeed, a symbiotic relationship exists between cyber attack and cyber defence: understanding the former better, allows states to develop counter-strategies and their own offensive capabilities. Parks and Duggan 2001, and Andress and Winterfield 2011, offer~~s~~ a good analysis of this symbiotic relationship, coupling an overview of attack capabilities with an assessment of how best to defend against them. Leed 2012 suggests that offensive cyber thinking, at least in the US, has been overshadowed by the defensive agenda. Using Cold War terminology, Chen 2010 considers how a capability such as Stuxnet could represent a "first strike" cyber weapon, while Kumagai 2001 presages how the internet will inevitably become the vehicle for attacks on infrastructure. Peterson's 2013 more recent paper picks up on Stuxnet and considers ways in which malware could be used to attack Industrial Control Systems (ICS). Meanwhile, Lin 2009 usefully places the technical elements of waging cyber war within the wider framework of ethical, legal and policy considerations.

Andress, Jason, and Winterfield, Steve. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham MA: Elsevier (2011).

Formatted: Font: Italic

A useful general overview of the cyber warfare domain, which goes into some detail on technical exploits which could be used, and how to protect against them.

Chen, Thomas M. "Stuxnet: The Real Start of Cyber Warfare?" IEEE Network (November/December 2010): 2-3.

A short article by the editor of IEEE Network considering the potential of Stuxnet and similar malware as a "first strike" military capability.

Kumagai, Jean. "The Web as a Weapon." IEEE Spectrum (January 2001): 118-121.

A useful early article which highlights the way in which attacks on web resources increasingly accompany civil and military conflicts, highlighting the normative view that serious threat to critical infrastructures will eventually become inevitable.

Formatted: Indent: Left: 0 cm

Leed, Maren. "Offensive Cyber Capabilities at the Operational Level: The Way Ahead". Washington DC: Center for Strategic and International Studies (CSIS), 2013

A detailed study that offers some proposals for a broader-based offensive military cyber strategy in the US than has been considered thus far.

Lin, Herbert. "Lifting the Veil on Cyber Offense." IEEE Security and Privacy 7/4 (2009): 15-21.

A useful paper placing the technical considerations of a cyber attack strategy within the wider policy, legal and ethical contexts.

Formatted: Indent: Left: 0 cm

Parks, Raymond C., and Duggan, David P. “Principles of Cyber Warfare”. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, Westpoint NY

An interesting think-piece which explores the strategic military thinking required to maximise cyber capabilities.

Peterson, Dale. “Offensive Cyber Weapons: Construction, Development, and Employment.” Journal of Strategic Studies 36/1 (2013): 120-124.

Discusses offensive exploits that could be used to attack Industrial Control Systems (ICS) such as SCADA (Supervisory Control and Data Acquisition networks).

Critical infrastructure vulnerabilities

The key targets of a major cyber war are assumed to be either the adversary’s military capabilities, or critical national infrastructure such as electricity or water supplies, communications or transport networks. The question of exactly how vulnerable such infrastructural facilities are to catastrophic cyber attack is, however, another area of vibrant debate. The reality or otherwise of such threats aside, there is general agreement that the specter of cyber war brings into focus the manner in which military capabilities and installations will be integrally bound up with civilian and corporate networks and capabilities, since the three dimensions are now intertwined to a unique degree in history. On specific infrastructure threats and vulnerabilities, Kramek 2013 highlights the particular vulnerability of major port facilities to cyber attack, which could affect the rest of the distribution network considerably. Stamp, Dillinger and Young’s 2003 report provides a detailed examination of network vulnerabilities in the control systems of key utilities. Miller and Dale 2012 provides a detailed chronology of cyber attacks on infrastructure up to 2012, analysing the method and nature of each attack. On the policy front, Yusta, Correa and Lacal-Arántegui’s 2011 paper provides a useful overview of the strategies being adopted in OECD countries to protect against cyber attacks on critical infrastructure, while in the US, Cordesman and Cordesman 2002 offers an optimistic view that the government is (or was at the time of writing) thinking along the right lines in recognising the importance of engaging across sectors and levels of government in developing an infrastructure protection strategy. On a more critical note, Dunn Cavelty 2007 refers back to the purported over-securitization of cyber attacks, which may be clouding an appropriate understanding of the real level and nature of threat to critical infrastructure.

Cordesman, Anthony H., and Cordesman, Justin D. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the US Homeland*. Westport CT: Praeger (2002).

Formatted: Font: Italic

A useful general commentary on the changing nature of infrastructure protection, which is fairly supportive of the US's level of recognition that government at all levels and the private sector need to work together on the new cyber-threats.

Dunn Cavelty, Myriam. "Critical Information Infrastructure: vulnerabilities, threats and responses." Disarmament Forum 3 (2007): 15-22.

A measured article arguing that infrastructure threats from cyber warfare may have been over-securitized, thus deflecting attention from a good understanding of the complexity of infrastructure threats from cyber attack.

Kramek, Joseph. "The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities". Washington DC: Brookings, Center for 21st Century Security and Intelligence (2013).

A pessimistic paper which highlights the particular vulnerability of port facilities to cyber attack and the effects this could have on the overall US economy and infrastructure.

Formatted: Indent: Left: 0 cm

Miller, Bill, and Rowe, Dale C. "A Survey of SCADA and Critical Infrastructure Incidents". Proceedings of the 1st Annual Conference on Research in Information Technology, Calgary, 11 October 2012

Formatted: Superscript

A detailed technical analysis of a range of critical infrastructure attacks, from the 1980s right up to FLAME attacks in 2012.

Stamp, Jason, Dillinger, John, and Young, William. "Common Vulnerabilities in Critical Infrastructure Control Systems". Albuquerque NM: Sandia National Laboratories (2003)

A report sponsored by Sandia National Laboratories in the US, which provides a detailed overview of vulnerabilities in the automated control systems for sectors such as energy and water distribution.

Yusta, Jose A., Correa, Gabriel J. and Lacal-Arántegui, Roberto. "Methodologies and applications for critical infrastructure protection: State-of-the-Art." Energy Policy 39 (2011): 6100-19.

A useful survey of energy security policies in the area of critical infrastructure protection in OECD countries.

Deterrence strategies

[au: Please provide here a commentary paragraph that introduces the sub-topic and the sub-sections that follow. Or, perhaps "general issues" should simply be collapsed into this main heading (like we did for "books" into "general overviews")?] [The paragraph below would act as a general commentary for the section so you could lose the "general issues" sub-heading as suggested. If you did that, however, could you still have the "nuclear" sub-heading below? The nuclear debate is a little sub-element of deterrence strategy in its own right so I would ideally like to keep it as a sub-heading,

although there are 5 refs in these two sections so you could equally combine them into one 10-ref section. I would prefer not on balance, but don't feel strongly.]

General issues

If modern nations need to consider defense against cyber attacks, then deterrence probably needs to be an important pillar of policy. However, many commentators note the dangers of thinking about deterrence strategies developed from earlier notions based on more traditional military threats, when the threat of cyber attack may be fundamentally different in nature and scale. Lupovici 2011 provides a particularly useful overview of research in the area of cyber deterrence, noting the frequent tendency to use Cold War thinking. Morgan 2010 levies the same accusation, and suggests that deterrence strategies need to draw in a wider range of actors beyond central government than would have applied previously. Libicki 2009 warns policy-makers to be aware of the fact that cyberwar is relatively cheap to wage, so will become increasingly likely. Wheatley and Hayes's 1996 report of an early workshop on the subject noted the need for a much more multi-layered deterrence strategy, as does Kramer and Teplinsky 2013 more recently. ~~while, more than 15 years on,~~ Stevens 2012 notes that there is still a paucity of clear thinking and solid policy on how cyber deterrence should look. Sterner 2011, meanwhile, takes a different approach and suggests that attack is the best form of defence and of deterrence, in this case directed at third parties that wittingly or otherwise enable cyber attacks over their networks. Conversely, Schneier 2004 suggests that the problem is not a technical one at all, but one of sensible user awareness of the risks.

Kramer, Franklin D., and Teplinsky, Melanie J. "Cybersecurity and Tailored Deterrence". Atlantic Council, Brent Scowcroft Center on International Security, Issue Brief, December 2013

Puts forward a strategy for a multi-layered deterrent strategy that combines the threat of counter-attack with denial of service, and strengthened partnerships.

Formatted: Indent: Left: 1.27 cm

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica CA: RAND Corporation, 2009.

Argues that, because costs for an aggressor in cyberwar are cheaper than in conventional conflict, states will inevitably take the decision to embark on major cyberwar at some stage in the future.

Lupovici, Amir. "Cyber Warfare and Deterrence: Trends and Challenges in Research." Military and Strategic Affairs 3/3 (2011): 49-62

A useful overview of research in this area which notes that much of the thinking on cyber deterrence starts from a Cold War perspective, and is heavily US-centric.

Morgan, Patrick M. "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm." Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy (2010): 55-76

Argues for a cyber deterrence policy not based on concepts derived from the Cold War, but in which “cooperative security management” is central.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World.* Indianapolis: Wiley, 2004.

Formatted: Font: Italic

From the arch-critic of traditional views of cybersecurity threats, argues that cyber threat is not a technical problem at all but one of sensible risk management.

Sterner, Eric. “Retaliatory Deterrence in Cyberspace.” Strategic Studies Quarterly (Spring 2011): 62-80.

Robustly argues that offensive cyber operations, particularly against complicit third parties, are the only realistic defence and deterrence against cyber attack.

Tim Stevens (2012): “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”, Contemporary Security Policy, 33:1, 148-170

Argues that deterrence in cyberspace is still very much a work in progress, and will involve a complex interplay of technical, political and behavioural dimensions.

Wheatley, Gary F., and Hayes, Richard E. *Information Warfare and Deterrence*. Washington DC: National Defense University Press (1996).

Formatted: Font: Italic

Resulting from an early series of workshops organised by the National Defense University in Washington DC, an interesting overview which paints a black picture about the potential impact of attacks and the pressing need to develop a multi-layered deterrence strategy.

Comparisons with the nuclear threat

A sub-component of the deterrence strategy debate is the question of whether the manner in which the threat of nuclear attack was conceptualized in the past could act as a model for how to think about the threat of cyber attack today. For those pessimists who see the potential of cyber warfare as being as destructive and complete as a nuclear attack, this thinking has some logic, although such commentators could equally be accused of using old-fashioned Cold War thinking to apply to a fundamentally different and postmodern threat picture. Sharma 2010 argues that the deterrent logic of Mutually Assured Destruction (MAD) is a suitable corollary for cyber deterrence, as does Geers 2010, albeit adapted to Mutually Assured Disruption. Young 2010 also sees many useful parallels with nuclear deterrence policy, and Nye 2011 argues that, even if the two threats bear some important differences, the initial uncertainty over cyber deterrence strategy is very reminiscent of the early days of nuclear strategizing in the Cold War. Meanwhile, Elliott 2011 offers the counter-argument that the two threats are sufficiently different that they really should not be seen in the same vein.

Elliott, David. “Deterring Strategic Cyberattack.” IEEE Security and Privacy 9/5 (2011): 36-40.

Argues that the lessons from nuclear deterrence do not transfer well to the realm of cyber warfare, and that “deterrence by denial” is a more appropriate model (p.36). [au: Please provide page numbers for this quotation.]

Geers, Kenneth. “The challenge of cyber attack deterrence.” Computer Law and Security Review 26/3 (2010): 298-303.

Argues that the notion of Mutually Assured Destruction (MAD) in the Cold War could be adapted for the contemporary age as Mutually Assured Disruption.

Nye Jr., Joseph S. “Nuclear Lessons for Cyber Security?” Strategic Studies Quarterly (Winter 2011): 18-38

Suggests that the initial uncertainty over nuclear strategy and deterrence offers a useful parallel for the current situation over cyber strategy, even though there are some important differences between the two threats.

Sharma, Amit. “Cyber Wars: A Paradigm Shift from Means to Ends.” Strategic Analysis, 34/1 (2010): 62-73

Proposes that a second-strike cyber capability can be developed, mirroring nuclear policy in the Cold War, and thus establishing a similar notion of Mutually Assured Destruction (MAD).

Young, Mark D. “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power.” Journal of National Security Law and Policy 4 (2010): 173-196.

Suggests there are many parallels with nuclear response policies and those relating to network attacks, not least in the imperative of responding quickly and comprehensively.

~~Cyber war and ~~T~~t~~he law [au: Perhaps this should be something along the lines of “Legal Domain”, etc.?] [Legal Domain or Legal Aspects would be fine.]

One of the most vibrant and extensive areas of debate around the issue of cyber war is in the legal domain. Questions of whether and how cyber attacks can be considered acts of war under traditional legal notions are important when states are considering how they can or should respond to such attacks; how they can work together to frame international controls and regulations on offensive cyber activity; and, indeed, what they are authorized to do in an offensive capacity. As discussed in Cyber and the Changing Nature of Conflict ~~above~~ [au: Please specify which section you are referring to.], the essentially asymmetric and anonymized nature of much cyber activity, and the manner in which it cuts across civil, military and governmental channels in terms of actors, poses a set of extraordinary challenges to existing legal norms and frameworks in the area of conflict and violence. Much of the debate relates back to the wider normative and critical approaches to the question of cyber war, and namely whether cyber attacks can really be classified as acts of war. Waxman 2011 flags up the difficulties of so classifying cyber attacks in a useful survey of legal discussions in this area, while Schmitt 2004 notes that most cyber attacks do not cause physical damage to humans or property, and thus cannot be viewed the same way as physical military attacks. Kelsey 2008 argues, however, that cyber attacks can and do violate principles of distinction and neutrality and thus should be subject to humanitarian law. Hollis 2007 echoes a view held by many that, just as cyber attacks represent a fundamental shift in the nature of conflict, so legal frameworks under which they operate need to be fundamentally altered also, and primarily at the international level if they are to be effective. Maurer 2011 notes a perhaps surprising level of discussion about the need for regulation governing international cyber threats at the UN. Graham 2010 flags up the problem of violent or pre-emptive response to cyber attacks when it is so difficult to identify the authors of such attacks, while Dunlap 2011 examines the specific legal issue of defining “combatants” in offensive cyber activity, many of whom will be civilians working in civilian agencies such as the NSA in the US. Whatever the questions of whether and how legal frameworks should evolve to deal with the new situation, Prescott 2011 suggests that extensive experience of testing and experimenting at the US Department of Defense’s Cyber Range should allow answers to be formulated.

Dunlap Jr., Maj.Gen. Charles J. “Perspectives for Cyber Strategists on Law for Cyberwar.” Strategic Studies Quarterly (Spring 2011): 81-99

Flags up the problem, under existing military law, of civilian operators at an agency such as the NSA undertaking cyber activities equating to acts of war.

Graham, David E. “Cyber Threats and the Law of War.” Journal of National Security Law and Policy 4/1 (2010): 87-102

Notes that offensive cyber responses to attacks are problematic under existing laws of war, given the problems with identification and attribution of the authors of attacks.

Hollis, Duncan B. “Why States need an International Law for Information Operations.” Lewis and Clark Law Review 11 (2007): 1023-1061

A detailed article which proposes that a new international legal framework is needed for information operations, since existing rules regarding the use of force and the laws of war are inadequate to deal with the new landscape.

Kelsey, Jeffrey T.G. “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.” Michigan Law Review 106 (May 2008): 1427-1451

Argues that acts of cyber warfare do violate the traditional notions of distinction and neutrality in humanitarian law, but that the non-lethal nature of such acts suggests that the law needs to adjust to accommodate the new reality.

Maurer, Tim. “Cyber Norm Emergence at the United Nations: An Analysis of the Activities of the UN regarding Cyber-Security”. Cambridge MA: Belfer Center for Science and International Affairs, September 2011

Focusing on the level of international law, identifies two active strands of discussion at the UN about the need for international agreements on regulation governing cyber warfare, and cyber crime.

Formatted: Indent: Left: 1.27 cm

Prescott, Jody. “War by Analogy: US Cyberspace Strategy and International Humanitarian Law.” The RUSI Journal 156/6 (2011): 32-39

Argues that, despite the difficulties and complexities of establishing how military cyber operations could or should relate to humanitarian law, a growing experience through such facilities as the US Department of Defense’s Cyber Range will quickly provide some answers.

Schmitt, Michael N. 2004. ““Direct Participation in Hostilities” and 21st Century Armed Conflict.” In Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck. Edited by Horst Fischer and Dieter Fleck, 505-529, Berlin: BWV (2004).

Analyses the complex role of civilians in the new landscape of cyber war. Argues that cyber attacks against civilians are not necessarily prohibited as long as they do not cause direct physical damage to them or their property.

Waxman, Matthew C. “Cyber-Attacks and the Use of Force.” The Yale Journal of International Law 36 (2011): 421-59.

A very useful discussion of the legal debates around how cyber attacks are complicated when applied to traditional legal notions of acts of war and violence.

The Attribution Problem

One of the specific problems which accompanies cyber attacks of all natures, and which affects not only the question of how to regulate offensive cyber activity but also how to develop deterrence and response strategies, is the question of the “Attribution Problem”. This is the problem of identifying who the author of an attack is, which is usually shrouded in multiple and complex layers of obfuscation. How can both soft and hard power take the problem to perceived aggressors or press for agreement in international circles that such activity should be strictly regulated, when aggressors can easily deny that attacks were not of their doing? This has generated much debate in technical, legal and military spheres, and has been subject to a great deal of brainstorming and lateral thinking. Hunker, Hutchinson and Margulies 2008 suggests that the problem is a multi-layered one that requires a multi-layered approach including user involvement and international cooperation, and Clark and Landau 2010 generally agrees that this is a policy problem rather than necessarily a technical one. However, those in the technical community such as Kalutarage, Shaikh, Qin Zhou and James 2012 argues that technical approaches of modelling unusual behaviour on networks can and should also provide much of the answer. Boebert 2010 takes a different and somewhat more bullish approach, suggesting that only robust covert operations and counter-attacks will have any realistic effect in deterrence.

Boebert, W. Earl. “A Survey of Challenges in Attribution.” Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy (2010): 41-52

Argues that, such are the technical and political problems with establishing reliable attribution, only “preemptive covert operations” (p.49) and counter-attacks will have substantial deterrent affects on aggressors. [au: Please provide page number for this quotation.]

Clark, David D. and Landau, Susan. “Untangling Attribution.” Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy (2010): 25-40.

A useful article which suggests that solving the attribution problem is not a technical challenge, but a policy one, in terms of establishing international agreements.

Hunker, Jeffrey, Hutchinson, Bob and Margulies, Jonathan. “Role and Challenges for Sufficient Cyber-Attack Attribution”. Dartmouth College: Institute for Information Infrastructure Protection (2008).

A detailed document which usefully outlines the size of the attribution challenge, and argues that solving it requires a multi-layered approach on technical, policy and political levels, with user acceptance and international cooperation both being key to success.

Kalutarage, Harsha K., Shaikh, Siraj A., Qin Zhou and James, Anne E. “Sensing for Suspicion at Scale: A Bayesian Approach for Cyber Conflict Attribution and Reasoning.” 2012 4th International Conference on Cyber Conflict. Tallinn: CCD COE (2012)

Based on extensive experimentation, proposes a Bayesian modelling approach which allows a method for accurately monitoring activity and attribution over high-scale, high data-rate networks.

Governance ~~of cyber warfare~~

[au: Please provide here a commentary paragraph that introduces the sub-topics and the sub-sections that follow. (Or, we can simply collapse “general debates” into this main section.)] [Same issue as above with Deterrence Strategies: I am happy for the following paragraph to be the general introductory one, as long as we can retain the sub-heading of Public and Private below]

General debates

Given the multiple levels of complexity and debate surrounding cyber war, concerning legal definitions of attacks; appropriate strategies for defense and response; or even whether cyber war exists as a concept at all, it is hardly surprising that governments are finding it difficult to establish how best to organise the range of cyber activities and security priorities under their command. As has been noted in a number of places already, the cyber realm appears to cut across traditional boundaries in space and time to an extent that few threats have managed to do before, and this delivers concomitant complexities in the range of actors that could and should be involved in the activities and in delivering defensive strategies. Many, such as Bellovin 2009, Cohen 2010, Der Derian 2003, Hansen and Nissenbaum 2009 and Shackleford 2010 argue that the problem is a quintessentially transnational and “heteropolar” one, which can only be tackled effectively at the level of international agreement and regulation. Indeed, Deibert 2013 stresses the dangerous consequences of not doing so. In a general case study of security governance in the UK, Richards 2012 outlines how the government has assembled a complex and multi-faceted range of actors and strategies to try to deal with the broad waterfront of cyber threats, from military activity to public information campaigns. Deibert and Rohozinski 2010, and Brown 2006 identify two particular paradoxes within the whole debate around governance and regulation. The former note that governments do not want to regulate cyber activity too much as there are huge benefits to be had for the economy in the free flow of commerce and information. Brown 2006 notes, meanwhile, that many of the states calling for regulation want to be able to wield offensive cyber capabilities themselves without falling foul of domestic or international law, and this complicates the negotiations. This is indeed a paradox that the US in particular has faced in a number of areas of international law and regulation.

Bellovin, Steven M. "The Government and Cybersecurity." IEEE Security and Privacy 7/2 (March/April 2009): 96

A short article which argues that complications over jurisdictional responsibilities for cyber attacks mean that only international agreements will be workable in this area.

Brown, Davis. "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict." Harvard International Law Journal 47/1 (2006): 179-221

An interesting article that notes the difficulties over conflicts of interest between those states that want protection from cyber attacks while still wanting the offensive capability themselves: concludes that a weak enforcement regime with broad support is better than no enforcement at all.

Cohen, Geoff A. "Targeting Third Party Collaboration." Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy (2010): 313-325

Outlines the issue that effectively tackling cyber attacks means establishing agreements and regulations that involve third parties carrying traffic, often outside of national jurisdictions, who will agree to cooperate.

Formatted: Indent: Left: 0 cm

Deibert, Ronald J. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace". Center for International Governance Innovation, Internet Governance Paper no.6, October 2013

Suggests we are at a critical moment where the securitization of cyberspace could lead to unhelpful and even destabilizing moves to constrain privacy and openness, when the opposite needs to be achieved.

Deibert, Ronald J., and Rohozinski, R. "Risking Security: Policies and Paradoxes of Cyberspace Security." International Political Sociology 4 (2010): 15-32.

A detailed and useful exploration of the complexity of governance in the information society, which throws up paradoxes in the way that the state is attempting to protect against serious attack and other threats, while allowing the free flow of information across borders and between different strands of public and private actors.

Der Derian, James. “The Question of Information Technology in International Relations.” Millennium: Journal of International Studies 32/3 (2003): 441-456.

An analytical piece which nicely encapsulates the nature of cyberspace governance as one of “heteropolarity”.

Hansen, Lene and Nissenbaum, Helen. “Digital Disaster, Cyber Security, and the Copenhagen School.” International Studies Quarterly 53 (2009): 1155-1175.

Using the framework of Securitization Theory, argues that governance of cyber security has the potential to broaden both internationally, and thematically in terms of being both political and intensely technical.

Richards, Julian. *A Guide to National Security: Threats, Responses and Strategie*s. Oxford: Oxford University Press (2012).

Formatted: Font: Italic

Within the framework of national security policy across the board, considers the manner in which the UK government has prioritised cyber attacks as a “tier one” threat, and how the range of organizations and bodies charged with protecting against threats has evolved into a very complex picture.

Shackleford, Scott J. “Estonia Three Years Later: A Progress Report on Combating Cyber Attacks.” Journal of Internet Law (February 2010): 22-29

While recognizing that individual countries have thought about the issue domestically, criticises the lack of concerted and joined-up international cooperation on policy to combat cyber attacks.

Public and ~~/~~Private governance issues [au: Heading revised to avoid the use of a slash, as per House guidelines.] [OK]

In addition to the geographic complexity of cyber threat governance spanning national boundaries, there is a further structural complexity in that, while governments and militaries may be directly involved in cyber war, private companies and individuals own and regulate the majority of networks over which data passes and which may be subject to attack. In this sense, the issue of public~~/~~/private collaboration in governance and regulation is an active subset of the governance debate. Again, the issue seems to be that the strategic thinking is still sometimes mired in a traditional, Cold War mindset in which military networks and capabilities were very much the concern of the military alone, and the government was the source of, and actor in all regulation. Bendrath 2001 again focuses on the purported over-militarization of the cyber threat and suggests that this has delayed and disrupted thinking about the appropriate public~~/~~/private collaborative responses to the threat. Jensen’s 2010 later review suggests that the US government is still not delivering enough of a suitable strategy to protect civilian networks in the event of cyber attack. Meanwhile, Kleinwächter 2002/3 suggests that consensual international bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN) provides a model for governance, and that bodies of this nature, coupled with concerted public/private collaboration, are the only realistic way forward in cyber security.

Bendrath, Ralf. “The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection.” Information and Security 7 (2001): 80-103.

A useful early survey of the complexity of infrastructure protection requirements, suggesting that the risk has been “over-militarized” and this has not delivered appropriate public-private collaborative responses.

Jensen, Eric Talbot. “Cyber Warfare and Precautions Against the Effects of Attacks.” Texas Law Review 88 (2010): 1533-69.

Argues that, given the unprecedented intermingling of civilian and government networks, the US government is not yet going far enough to ensure against collateral damage of civilian networks in the event of cyber attack on military or governmental targets.

Kleinwächter, Wolfgang. “From Self-Governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet’s Core Resources.” Loyola of Los Angeles Law Review 36 (2002/3): 1103-1126.

Explores the role of the Internet Corporation for Assigned Names and Numbers (ICANN) in internet governance, and argues that similar “co-regulatory” and flexible approaches involving consensual public-private partnership are the only realistic way forward.

~~Cyber war and~~ NATO

Most of the public debate and analysis about the threat of cyber war has been happening in the West, and disproportionately in the US. This has fed into a strand of debate about whether and how NATO should be involved in cyber war and cyber defense. Indeed, the cyber question formed part of the general soul-searching within NATO following the Cold War as to its continued purpose in a time of changing threats and power polarities, and economic pressures on defense budgets. For NATO, the debate was given a particular spin following the wave of cyber attacks on Estonia in 2007. As a NATO member country itself and an aggrieved victim of attack, many in Estonia called upon the Alliance to develop a robust cyber attack and defense capability. Partly as a result of this, the new Cooperative Cyber Defense Center of Excellence (CCDCOE) was situated in Tallinn, and has been the source of much analysis and research on cyber threats subsequently. The 2010 NATO Strategic Concept also talked about the seriousness of “emerging security challenges” to the Alliance. Yost 2010 notes that NATO has been increasingly talking of cyber attack within an Article 5 context, namely as an attack worthy of a collective and concerted military response. Tikk 2010 suggests that NATO is in a particularly strong position among international organisations to be able to strategize effectively over the cyber threat, since it has a focused and specific function of defense. Hughes 2009 is very complimentary about the moves that NATO have made in this area, such as the establishment of the CCDCOE in Tallinn, while Dandurand 2011 suggests they could do even better with some red team analysis of the complex picture. A more critical reading would be that, given the complexities and difficulties outlined ~~above~~ [au: Please specify which section] [can say “in various sections” here?] surrounding the whole cyber threat picture, not least difficulties of attribution (see Governance), it will remain difficult for NATO to develop an appropriate military response strategy against cyber attack. Indeed, a detailed analysis by Tikk, Kaska, Rünnimeri, Talihärm and Vihul 2008 of the CCDCOE, notes that attribution of authorship to the Estonian and Georgian attacks remains difficult to establish.

Dandurand, Luc. “Rationale and Blueprint for a Cyber Red Team within NATO.” In 3rd International Conference on Cyber Conflict (ICCC), 2011. Edited by Czosseck, C., Tyugu, E. and Wingfield, T. 71-86. Tallinn: CDD COE Publications, 2011.

Argues that a dedicated Red Team would greatly enhance NATO’s cyber defence capabilities and understanding.

Hughes, Rex B. “NATO and Cyber Defence.” Atlantisch Perspectief (April 2009): 4-8

Written shortly after the 2007 attacks on Estonia, argues that NATO is moving in the right direction with the establishment of the Cyber Defence Management Authority (CDMA), and Cooperative Cyber Defence Center of Excellence (CCDCOE) in Tallinn.

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A. and Vihul, L. Cyber Attacks against Georgia. Tallinn: CCDCOE (2008).

An interesting and measured report from NATO’s cyber-security center in Tallinn, which notes that there is no proof as to who was behind the attacks in Estonia or in Georgia.

Tikk, Eneken. “Global Cybersecurity – Thinking about the Niche for NATO.” SAIS Review 30/2 (2010): 105-119.

Argues that NATO is in a particularly strong position amongst international organizations to be able to deal with cyber threats effectively and objectively.

Yost, David. “NATO’s evolving purposes and the next Strategic Concept.” International Affairs 86/2 (2010): 489-522

Reflects the fact that NATO has been increasingly considering cyber-attack to be an Article 5 issue, namely one that involves collective defence and collective response.