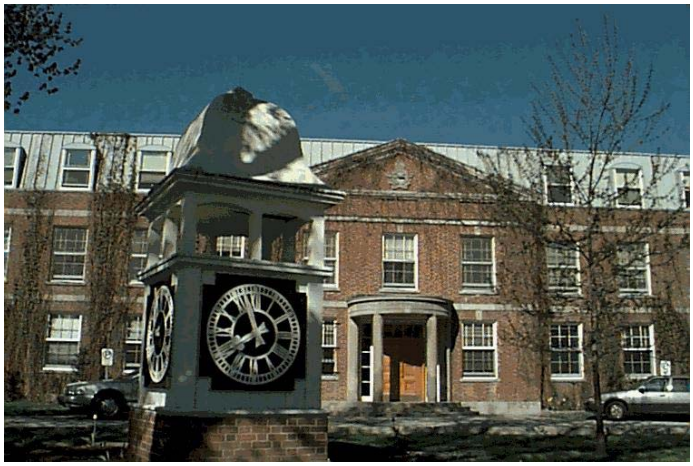
National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes



CYBER WARFARE SCHOOLS OF THOUGHT: BRIDGING THE EPISTEMOLOGICAL/ONTOLOGICAL DIVIDE

LCol P.E.C. Martin

JCSP 41

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 41

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

CYBER WARFARE SCHOOLS OF THOUGHT: BRIDGING THE EPISTEMOLOGICAL/ONTOLOGICAL DIVIDE

By LCol P.E.C. Martin

Word Count: 17890

Compte de mots : 17890

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Martin, Paul Edwin Charles. M.D.S. Canadian Forces College – JCSP 41, April 2015.
Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide.
Supervised by Dr. Paul T. Mitchell.

There are tangible ontological influences of modern day communications and computerization on our daily lives. An important consequence of the increasing dependence on networked communications is that it presents opportunities for agents wishing to exploit system vulnerabilities. These agents range from nation states to non-state actors. The most basic question a modern military confronts from the challenge of cyber threats is: "what is to be done?" Purely technological responses are available, but the implications of their use often raise more questions than they answer. Governments and militaries are presented with a basic epistemological problem which hinders their ability to answer the question already posed. Analyzing the existing body of relevant literature offers a process by which the uncertainties posed by these questions can be sorted out. However, the rapid pace of developments bedevils those who seek to "keep up" with this evolving issue. This study seeks to rectify this situation by proposing a schema for classifying the different epistemological conceptions in terms of discrete, "Cyber Warfare Schools of Thought." By so doing, a better understanding of the differing conceptions is both possible and achievable. Ultimately, the purpose of such a typology is to help bridge the epistemological/ontological divide that exists in different understandings and conception of "cyber."

The nations, of course, that are most at risk of a destructive digital attack are the ones with the greatest connectivity.

- Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*

CHAPTER 1 – INTRODUCTION

The activities and capabilities of the cyber realm are often influenced by exposure to popular culture and visionary writers of science fiction. An example of this the 1983 movie "War Games" in which a high school student hacks into a military system to play online games but almost initiates global thermonuclear war by accident. In the 2015 movie "Blackhat," nuclear plant safety and trade exchange security are imperiled by evil individuals with cyber exploitation skills. These sorts of fears and concerns related to the possible implications of the wired world on human existence are shaping opinions on what cyber connectivity represents. Does the interconnected environment hosting the cyber activity represent a new arena, territory, or battlefield? Popular culture would seem to suggest that "cyberspace" is in fact a new construct for individuals to conduct daily tasks as well as to interact and exchange information with other individuals in a highly inter-connected fashion. With origins relating back to the ancient Greek term "kubernetes,"[1] cyberspace as a term was derived from Norbert Wiener's 1948 seminal work[2] on cybernetics and automation. Wiener's philosophy and pursuit of automation to improve people's lives has led to the current perceptions of cyberspace as a medium in which masses of people are interconnected and influenced by the activities within this realm.[3]

---

[1] Definition of kubernétés: a steersman, pilot – BibleHub, "2942. Kubernétés," last accessed 28 April 2015, http://biblehub.com/greek/2942.htm.

[2] Norbert Wiener, *Cybernetics* (Paris: Hermann, 1948).

[3] Chip Morningstar and F. Randall Farmer, "The Lessons of Lucasfilm's Habitat," *Journal for Virtual Worlds Research* 1, no. 1 (2008): 2.

Defence and Security Implications

Cyber security within the Canadian federal government is increasingly becoming a point of concern from not only a perspective of information confidentiality, integrity and availability but in terms of public safety. There are unambiguous ontological[4] influences of modern day communications and computerization on our daily lives. Alun Munslow, in his book *The Routledge Companion to Historical Studies*, defines the meaning of ontology as:

> … that branch of metaphysics that addresses the general state of being, the nature of existence, and how the human mind apprehends, comprehends, judges, categorizes, makes assumptions about and constructs reality. For the historian ontological questions arise when we address how to create historical facts within the larger ontology of our own existence, that is, the condition(s) of being under which we create or construct the-past-as-(the discipline of)-history.[5]

Human existence – the ontological – is progressively being supported by computerized information. The reality of increasing dependence on networked communications presents opportunities for those wishing to exploit system vulnerabilities ranging from nation states to non-state actors. In Canada today, the Department of National Defence (DND) and the Canadian Armed Forces (CAF) are responsible for providing defence intelligence as well as monitoring and providing military response options to cyber threats.[6]

The most basic question a modern military confronts from the challenge of cyber threats is: "*what is to be done?*" Information technology offers a host of new capabilities for military forces. They offer both new opportunities for acquiring information and executing action within

[4] "The historian is dedicated to discovering the reality of the past rather than debate metaphysics, that is, dispute the nature and construction of reality of being." - Alun Munslow, *The Routledge Companion to Historical Studies* (New York: Routledge, 2000), 184-185.

[5] Munslow, *The Routledge Companion …*, 184-185.

[6] Public Safety Canada, "Cyber Security in the Canadian Federal Government," *Government of Canada*, last modified 04 March 2014, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-eng.aspx.

a battlespace, and the potential for the generation of new threats. But events do not wait for us to have a systematic understanding of them before they occur, as the Stuxnet[7] and Buckshot Yankee[8] incidents illustrate. The daily news bring ever more lists of computer systems that have been hacked and compromised by malware, ever more lists of companies and governments who have lost information to spies, criminals and activists, [9] and ever more individuals whose privacy has been invaded.[10] Nearly every United States arms program tested in 2014 showed, "significant vulnerabilities to cyber-attacks,"[11] including some of the most sophisticated weapon systems in use or development. The United States Air Force saw the Predator and Reaper drone fleets infected with the "credential stealing" virus and the F-35 fighter was revealed to have a

[7] "Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries." - Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32. Stuxnet Dossier," *White Paper, Symantec Corp., Security Response* 5 (2011): 2. See also, "The appearance of Stuxnet 51 in 2010, as part of an apparent operation to cripple the Iranian nuclear program, raised the bar in what is publically known about the sophistication of cyber weapons. Stuxnet combined many known techniques, with some previously unknown ones, to produce an attack tool that could jump air-gaps using USB devices, automatically propagate an infection across Windows-based computer network, and use covert channel communication techniques to call home for more instructions." - Scott Knight, "War by Computer: Canadian Cyber Forces in 2025," in *The Canadian Forces in 2025 Prospects and Problems*, ed. J. L. Granatstein, First ed. (Victoria, B.C., Canada: FriesenPress, 2013): 78.

[8] "A USB flash memory drive containing malware created by a foreign intelligence agency was left in the parking lot of a Department of Defense facility at a base in the Middle East in 2008. It was found by an employee, taken into the facility, and connected to a DoD laptop computer. When the device was connected, the agent.btz malware began scanning the local host and other networked computers for classified and unclassified data, and initiated outbound connections to a command and control server to upload found data and receive instructions.[…] Undetected for many months, Pentagon officials described it in 2010 as "the most significant breach of U.S. military computers ever." Though characterized by its Trojan behavior, agent.btz malware is a variant of the SillyFDC worm, and has robust mechanisms for self-replication. In a response called "Operation Buckshot Yankee" the DoD spent nearly 14 months cleaning the worm from Pentagon offices and multiple military networks worldwide." - Jon Espenschied, "A Discussion of Threat Behavior: Attackers & Patterns," *Microsoft Corporation and NATO CyCon, June* (2012).

[9] David Paddon, "Cyber attacks have hit 36 per cent of Canadian businesses, study says," *The Globe and Mail*, last modified 18 August 2014, http://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/.

[10] Rosemary Barton, "Chinese cyberattack hits Canada's National Research Council," *CBC News*, last modified 29 July 2014, http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.

[11] Andrea Shalal, "Nearly every U.S. arms program found vulnerable to cyber attacks," *Reuters*, last modified 20 January 2015, http://www.reuters.com/article/2015/01/21/us-cybersecurity-pentagon-idUSKBN0KU02920150121.

cyber-vulnerability in the Autonomic Logistics Information System that could allow adversaries to defeat the plane without ever firing a round. [12]

Despite being a priority for action, the absence of doctrine for cyber warfare frustrates our ability to think about what should be done in terms of a military response to potential incidents or threats. Purely technological responses are available, but the implications of their use can raise more questions than they answer. Governments and militaries are presented with a basic epistemological problem which hinders their ability to answer the question of what a proper course of action might be. Alun Munslow defines the meaning of epistemology as:

> … the branch of philosophy that addresses the nature, theory and foundations of knowledge, its conditions, limits and possibilities. Historians, as the creatures of the modernist (Cartesian Enlightenment) revolution, have tended to stick with a particular vision of what history is, derived from a certain kind of analytical philosophy (this is often un-thought out as most historians are not actively engaged by philosophy of any sort).[13]

Has cyber interconnectivity changed our being and the conduct of military activities? The Canadian military involvement in cyber tests the very epistemological foundations of traditional military culture and the nature of warfare. Is cyber discrete and distinct enough that it has a cultural imperative strong enough to transcend land, sea and air domains? Sea, land and air forces have an internal logic to them by nature of the environment in which they operate. The sea

---

[12] Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet," *WIRED*, last modified 07 October 2011, http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/. See also, Noah Shachtman, "Military 'Not Quite Sure' How Drone Cockpits Got Infected," *WIRED*, last modified 19 October 2011, http://www.wired.com/2011/10/military-not-quite-sure-how-drone-cockpits-got-infected/. See also, 60 Minutes Overtime, "Can the U.S. military's new jet fighter be hacked?," last modified 01 June 2014, http://www.cbsnews.com/news/can-the-f-35-be-hacked/. See also, Andrea Shalal-Esa, "Pentagon downplays comment on F-35 fighter jet cyber threat," *Reuters*, last modified 25 April 2013, http://www.reuters.com/article/2013/04/25/us-lockheed-fighter-cyber-idUSBRE93O1HK20130425. See also, CyberWarZone, "New F-35 Fighter Jet is vulnerable to cyber-attacks," last modified 31 May 2014, http://cyberwarzone.com/new-f-35-fighter-jet-vulnerable-cyber-attacks/.

[13] Munslow, *The Routledge Companion …*, 88.

generates a different culture than the land or the air.[14] The nature of military based cyber operations may be so different than land, sea and air activities that it should be enculturated in a separate and distinct domain designation.[15] The absence of a clear typology for cyber conceptions generates uncertainty in determining a clear path for action.

Cyber Warfare Schools of Thought

Consulting the literature is typically a process by which the uncertainties posed by these questions can be sorted out. However, the rapid pace of developments in computer issues bedevils those who seek to "keep up" with this evolving issue. Even experts can express feelings of being overwhelmed by the rapid pace of events and the explosion of writing on the subject. Dorothy Denning, a well-known cryptologist, wrote of the challenge of completing her landmark book on Information Warfare in 1998:

> … a major challenge has been keeping up with developments in the field, including new technologies, methods of attack, laws, and studies and developments related to incidents covered in the book. On a typical day, I find another story or two in *The Washington Post* of some book or magazine. By the time this book goes to print, I no doubt will have accumulated a huge pile of material that I wish could have been included.[16]

This explosion of literature has to be organised in some way if any sense is to be made of the data. With no clear guideposts to the rapidly accumulating mass of material, it remains to the individual reader to make sense of the wealth of material and it is easy to become overwhelmed

---

[14] Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis: A RAND Corporation research study* (Baltimore: Johns Hopkins University Press, 1989), 17-30.

[15] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal: Canada's Journal of Global Policy Analysis* (2014). See also, R. Nicholas Burns, Jonathon Price, Joseph S. Nye, Brent Scowcroft, Aspen Institute, and Aspen Strategy Group. *Securing Cyberspace: A New Domain for National Security* (Washington, D.C.: Aspen Institute, 2012), 202.

[16] Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, Vol. 4. (Reading, MA: Addison-Wesley, 1999), xvi.

quickly. The epistemological understanding of what cyberspace is and how it relates to the ontological being of humanity varies greatly depending upon individual biases and perspectives. This study seeks to rectify this situation by proposing a schema for classifying the different opinions in terms of discrete "Cyber Warfare Schools of Thought."

If the literature for cyber warfare is examined, one can see clear delineations between three groups or Schools of Thought, each of which revolve around specific assumptions about the nature of how information technology is affecting the practice of warfare. The Schools can be placed on a spectrum of opinions along which one can measure a dialectical relationship between technological and human agency (Figure 1.1). The three Schools can be grouped in the following manner: revolutionary materialists, liberal materialists, and conservatives.

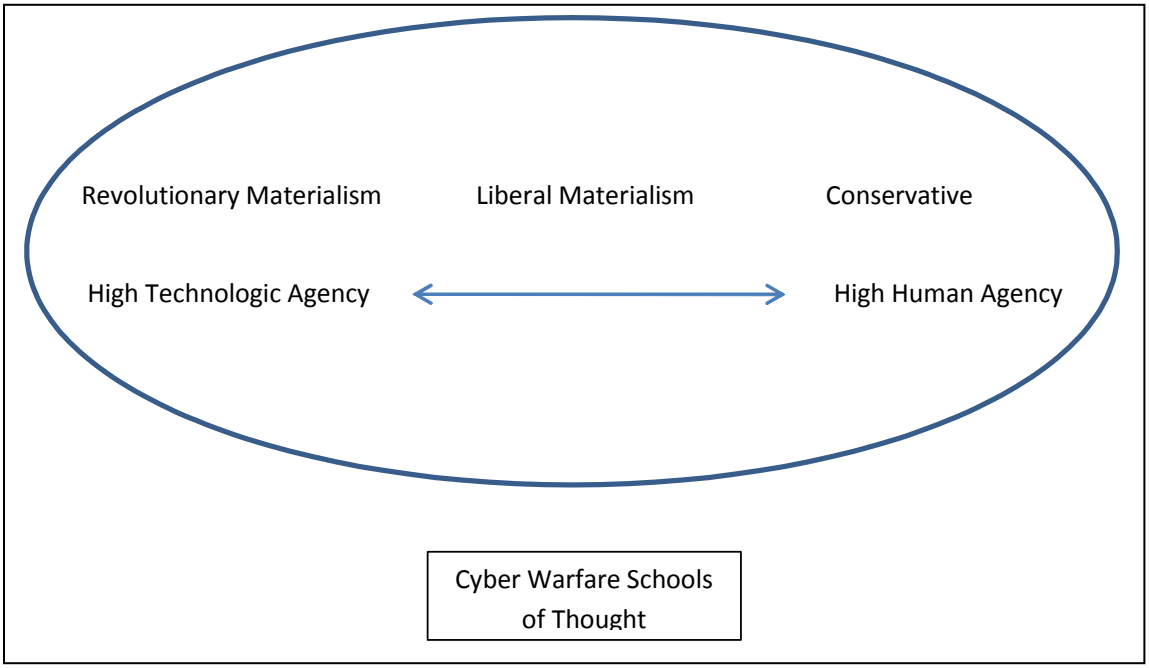


Figure 1.1: Cyber Warfare Schools of Thought

The Revolutionary Materialist School of Thought makes the basic assumption that information technology will change the *praxis*[17] of warfare, if not nature war itself. The Revolutionary School of Thought bears a close resemblance to air power theory in both its basic credo and its objectives. Revolutionaries, like the air power theorists before them, emphasise the possibilities for manoeuvre that information technology offers military forces. Cyber warfare can be used to go around or avoid confrontation between major military forces altogether. By attacking a state's critical infrastructure through a major event (frequently referred to as an "Electronic Pearl Harbor"), the state's ability to control both its regular military forces as well as society itself will be compromised. Financial markets are disrupted, transportation grids are rendered dysfunctional, electrical power is removed from broad swathes of the country, and information networks are collapsed. Social chaos results from these actions and the state loses its ability to act. A war effectively ends through basic governmental paralysis and/or regime change.

The Liberal Materialist School of Thought is closely related to the Revolutionary School in its focus on materialism, but it places a greater emphasis on the ability of human agency to control the effects of cyber warfare through the power of social institutions. Liberals emphasise the transformative power of technology on the nature of society itself. Unlike the Revolutionaries, however, Liberals emphasise a more evolutionary process in which technology produces new phenomena which both individuals and institutions can take advantage of as they see fit for their own ends. Globalisation is part of this process. Liberals, like Revolutionaries, see challenges to the ability of the state to control the issues confronting them. The emergence

[17] Praxis is defined by the merriam-webster online dictionary as either a) the exercise or practice of an art, science or skill; b) customary practice or conduct; or c) the practical application of theory. In the case of the Schools of Thought the term "praxis" is used to relate to the application of customary practice or conduct of warfare. - Merriam-Webster, "praxis," last accessed 28 April 2015, http://www.merriam-webster.com/dictionary/praxis.

of non-state actors, a feature that is facilitated by the lowered entry costs that IT affords, allows various and sundry individuals and groups to diffuse power away from the state. For them, the future is far more uncertain in terms of what will ultimately emerge because of the unplanned emergent nature of this free choice in terms of both technology and *praxis*. While they observe that things are changing because of this expansion of agency, the normative vector of that change is unpredictable – it could be good or bad for society. This highlights the centrality of human agency in the technical aspects of the evolutionary process. Liberalism speaks more to the enabling of agency than of any assumed progressive outcome associated with technological development. Cyber warfare is just one aspect of this process of societal evolution. It represents a risk for the future, but not one that is impossible to resist and might even be brought under the firm control of the state (either in terms of its ultimate rejection or its practical employment as just another tool).

Finally, the Conservative School of Thought is inherently reactive to the claims both the Revolutionaries and Liberals make. It makes the basic assumption that information technology has always been important to the conduct of warfare, and that its effects will not be revolutionary, but are more in the nature of additions to the existing models of warfare. Secondly, Conservatives emphasise the role of the state in its ability to impose local order on an otherwise anarchical system. In other words, this School accepts the increasing importance of information technology to the prosecution of war, but denies that it fundamentally changes everything. In this conception, change is incremental or evolutionary at best. It represents simply the steady increase of military capability that militaries have dealt with since at least the dawn of the industrial age and the advance of science in terms of weapons development. The

School tends to be heavily influenced by the writings of Carl von Clausewitz,[18] which it uses as a benchmark from which to observe the effects that information technology is having on the acts of war. However, some Conservatives also examine the fundamental nature of information technology and emphasize the operational limitations affecting the Revolutionary claims of the previous School of Thought. In particular, Conservatives tend to emphasize the human context of warfare, rather than its technological domain. Their challenges tend to be epistemologically based, raising basic questions about the implications stemming from future predictions of technological capability. Their observations tend to revolve around the *praxis* of warfare, rather than any theoretical or hypothetical predictions. History remains very much a guide to understanding the continuation of the essentials of human conflict. Finally, Conservatives seem to emphasize the social construction of military technology. Weapons serve specific political and organisational needs rather than driving military affairs in and of themselves. In this, the Conservatives make a definite break between their Materialist Revolutionary and Liberal challengers. Rather than stressing the scientific potential or the technical application of technological affordances, Conservatives focus on the practical questions which revolve around its use.

This paper will address the potential impacts of cyber warfare on the CAF by observing changes to the *praxis* of warfare through the different lenses and perspectives associated with the "Cyber Warfare Schools of Thought schema." Leveraging the School of Thought schema to acknowledge the potential biases toward cyber warfare, one can better bridge the divide between what one knows about this new technology through evidence-based epistemological induction and the changes/influences Cyber capabilities continue to have on our very existence from an

[18] Carl von Clausewitz, Michael Eliot Howard, Peter Paret, and Beatrice Heuser, *On War*, Oxford World's Classics. [Vom Kriege.] (Oxford: Oxford University Press, 2007), 284.

ontological perspective. In order to traverse the epistemological/ontological divide this document will conduct a comprehensive review of cyber warfare literature and arrange the key ideas by chapter according to the relevant Cyberwar School of Thought schema. Chapters 2, 3, and 4 will articulate the Conservatives, Revolutionaries, and Liberal Materialists Cyber Warfare Schools of Thought respectively. Finally, Chapter 5 will conclude this paper with the key points derived from the application of the Cyber Warfare Schools of Thought schema to the wealth of cyber based literature as well as consider how an institution may approach bridging the epistemological/ontological divide. In addition, the conclusion portion of Chapter 5 will provide some thoughts and recommendations for CAF leadership facing the challenges of exposure to and use of cyberspace in the future defence activities and the need for epistemological normalization to effectively bridge the divide.

Conservatism discards Prescription, shrinks from Principle, disavows Progress; having rejected all respect for antiquity, it offers no redress for the present, and makes no preparation for the future.

- Benjamin Disraeli

It is questionable if all the mechanical inventions yet made have lightened the day's toil of any human being.

- John Stuart Mill

CHAPTER 2 – THE CONSERVATIVE SCHOOL OF THOUGHT

Those who subscribe to the Conservative Cyber Warfare School of Thought are cautious in their perception and acceptance of technological changes to society and the conduct of war. Typically, Conservative perspectives are reluctant to change or to contemplate new concepts that challenge the nature and dogma of warfare. As a group, the Conservative School favours the preservation of established principles and *praxis* of warfare and in doing so opposes the contemplation of changing their perspectives based on any ontological changes that may be due to technology. This group tends to employ the writings of Clausewitz, Jomini or Sun Tzu as the foundation of their epistemological assessment of military affairs through historical evidence-based induction and reject things that do not conform to this framework of understanding.[19]

Being adverse to change, this School is resistant to the notion of technology-led Revolutions in Military Affairs[20] (RMA) siding with the more traditional concept of evolution in military technological innovation. Through incremental/evolutionary approaches to technological changes the Conservative School is able to defend traditional concepts of warfare and incorporate any modified *praxis* based on the advantages of the increase in technology.

---

[19] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Vol. 9 (Psychology Press, 2004), 20.

[20] MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution, 1300-2050* (New York: Cambridge University Press, 2001), 6.

Technical Evolution vice Revolution

In his book *Strategy for Chaos*, the British strategic thinker Professor Colin S. Gray discusses the concept of RMAs and their occurrences throughout history. Gray articulates how RMAs manifest themselves through "strategy" or the employment of "force and the threat of force"[21] in the achievement of political goals. Furthermore, Gray views war as "organized violence carried on by political units against each other for political motives."[22] From this train of thought Gray views an RMA as "a radical change in the character or conduct of war" that are not necessarily instigated by new technology.[23] Gray's theories of RMAs conform to the Conservative School of thinking by closely aligning with the Clausewitzian approach to strategy where warfare is both instrumental and political.[24] As Clausewitz stated in *On War*, "…war is not merely a political act but a real political instrument, a continuation of political intercourse, a carrying out of the same by other means."[25]

Gray offers a nine step framework to further explain how an RMA process "works" in altering the character or conduct of warfare.[26] First - Preparation: RMAs require time to manifest themselves as a non-linear change/reform and generally considered a radical alteration to the *praxis* of warfare. Second - Recognition of challenge: identification of an opportunity or challenge posed by an adversary that generates a reason requiring an RMA solution. Gray highlights that for there to be a true RMA there must be a belief in a real adversary offering a strategic challenge. Third - Parentage: An RMA requires revolutionary leadership in positions of

[21] Colin S. Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, Vol. 2 (Portland, OR: Frank Cass, 2002), 4.
[22] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 4.
[23] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 4.
[24] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 93..
[25] Clausewitz et al, *On War ...*, 87.
[26] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 75-81.

authority to facilitate the change. Fourth - Enabling Spark: A person or event that acts as a catalyst for the RMA to occur and deviate the *praxis* of warfare off of its linear evolutionary path. Fifth - Strategic Moment: The opportunity to convey the RMA possibilities to those open minded to receive the revolutionary messaging. Sixth - Institutional Agency: The requirement for a military institution to adopt, train on and implement with competence the innovative operational concepts fuelled by new technologies. Seventh - Instrument: The military instrument of the new RMA is established and institutionalized through the formalization within doctrine and training. The new military instrument/capability must also be grown and replicated in size to have significant impact on the *praxis* of the institution as well as its potential adversaries. The eighth step - Execution and Evolving Maturity: The application and employment of the RMA in battle will have an initially significant and destabilizing effect on its adversaries. The destabilizing effect will be reduced with subsequent uses and demonstrations of the RMA as adversaries learn from this new mode of warfare. Step Nine - Feedback and Adjustment: If an enemy is not overwhelmed by the first application of the RMA capability, it will study the and counter it with like capabilities or appropriate tactics to nullify the strategic effectiveness of the new and innovative way to conduct war. To be continually effective as a warfare instrument, the capability must be continually adjusted to counter adversarial adaptations. In effect, feedback and adjustment creates a new linear evolutionary path in the same direction forged by the non-linear radical change itself.

Comparing historical examples of RMAs such as the French revolutionary wars, the First World War, and the nuclear age with the potential Information-led (cyber) RMA of the 1990's, Gray concludes that cyber as an event in strategic history lacks political and human actions to be

considered an RMA. [27] The Conservative School position is that cyber represents increased technology but has done little to change the character or nature of war.[28]

The Conservative view of warfare is less technologic and very much human agency centric in thinking. Aligned with the writings of Clausewitz with respect to the intangible elements of human nature and morale in warfare the Conservative School is more concerned about the human element and not the weapons technology that impact strategy. Clausewitz states:

> Military activity is never directed against material force alone; it is always aimed simultaneously at the moral forces which give it life, and the two cannot be separated […] the moral elements are among the most important in war[…]. Unfortunately they will not yield to academic wisdom. They cannot be classified or counted. They have to be seen or felt.[29]

The revolutionist School that prefers technical over political solutions are often seen as a self-serving technocrats focusing on the means vice the ends of strategy.[30] Gray argues:

> When people and organizations are not required to think about difficult topics (in this case, policy assumptions and strategy), they will choose to focus on more congenial topics (e.g. a technically defined RMA).[31]

Others in the Conservative camp view cyber as an incremental/evolutionary increase in technology more akin to existing capabilities performing Electronic Warfare. With the advent of wireless networking and telephones that are also network appliances, the characteristics that distinguish electromagnetic spectrum issues from data network infrastructure issues are

---

[27] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 280-281.
[28] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 281.
[29] Clausewitz et al, *On War* …, 137; 184.
[30] Gray, *Strategy for Chaos: Revolutions in Military Affairs…*, 280-281.
[31] Gray, *Strategy for Chaos: Revolutions in Military Affairs…*, 282.

becoming common to both disciplines.[32] Others in the Conservative School consider that a "Cyber Electronic Warfare (CEW) concept which merges cyberspace capabilities with traditional EW methods, is a new and enhanced form of electronic attack."[33] The convergence between wireless communications and cyber leads the Conservative School to believe:

> … that the cyber environment is nothing new. Rather, it is simply a unique manifestation of the electromagnetic (EM) operating environment – a familiar component of military operations with integral operating concepts and principles that lend themselves well to cyber.[34]

The US Chief of US Naval Operations, Admiral Jonathan W. Greenert, argued in 2012 that wireless activity in the electromagnetic (EM) spectrum had become integral to cyberspace. Admiral Greenert stated:

> The EM-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a warfighting domain on par with- or perhaps even more important than-land, sea, air and space.[35]

Furthermore, the Conservative perspective would suggest that the foundations of modern communications including cyber began with the advent of wireless communication pioneered by Guglielmo Marconi in 1895.[36] It is from this incremental/evolutionary approach to modern-day communications that plays contrary to the Revolutionist camp claims that cyber is a new

---

[32] Keith B. Alexander, *Warfighting in cyberspace* (National Defense Univ Washington DC Inst for National Strategic Studies, 2007), 59.

[33] Nurgul Yasar, Fatih M. Yasar, and Yucel Topcu, "Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield," In *SPIE Defense, Security, and Sensing*, International Society for Optics and Photonics (2012).

[34] Jim Gash, "Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits," *Canadian Military Journal* 12, no. 3 (Summer 2012): 28.

[35] Admiral Jonathan W. Greenert and US Navy, "Imminent Domain," *U.S. Naval Institute Proceedings Magazine* 138, no. 12 (1) (2012): 318, last accessed 02 May 2015, http://www.usni.org/magazines/proceedings/2012-12/imminent-domain.

[36] Greenert et al, "Imminent Domain,"…, http://www.usni.org/magazines/proceedings/2012-12/imminent-domain. See also, Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Toronto: Knopf, 2011), 15-18.

technology and has changed the nature of warfare. Vincent Mosco in his book *The Digital Sublime* also argues that incremental/evolutionary increases in technology are regularly overstated.[37] Often influenced by society's collective short term recollection of history, Mosco cites a cyclical phenomenon in which any increase in technology is heralded as a revolution. In terms of cyber, Mosco states:

> The widely held beliefs that computer communication is ending history, geography, and politics are not at all new. […] Not only does this demonstrate that our response to computer communication is far from unique; it also documents our remarkable, almost willful, historical amnesia. One generation after another has renewed the belief that, whatever was said about earlier technologies, the latest one will fulfill a radical and revolutionary promise […] Cyberspace enthusiasts encourage us to think that we have reached the end of history, the end of geography, and the end of politics. Everything has changed. [38]

Claims of revolutionary changes in military technology in the eyes of the Conservative School are nothing more than incremental/evolutionary changes to the existing tenants of politics and warfare re-packaged with the buzz words of the day and sold as brand new. [39] In this context, Conservatives may employ the cliché expression "old wine in a new bottle" to articulate the evolutionary nature of technology on military affairs.

The Nature of Warfare and Cyberwar

Thomas Rid, in his book *Cyber War Will Not Take Place*, outlines a cautionary perspective on the future "cyber" prospects of state wars. Citing the writings of Carl Von Clausewitz as the foundation for his inductive reasoning, Rid makes the case that cyber activity

[37] Vincent Mosco, "The Digital Sublime," *Myth, Power, and Cyberspace* (2004): 8.
[38] Mosco, "The Digital Sublime,"…: 8; 117.
[39] Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics, 1851-1945* (New York: Oxford University Press, 1991), 18-20.

does not conform to the principles and nature of warfare. According to Clausewitz, "War is an act of force to compel the enemy to do our will,"[40] and the application of force in war must obey the three criteria: 1) the act is violent, 2) the act is instrumental, and 3) the act is also political in nature.[41] To be considered violent the application of physical force in war must inflict physical harm on citizens and state actors. For a force to be instrumental its application as a means must be the sole reason that compels an adversary to accept the terms of your envisioned end-state. Finally, war's actions are always political at a strategic level. Rid's primary message is that offensive cyber activity cannot be interpreted as acts of warfare as there is no evidence that supports the criterion of a Clauswitizian defined war. "If the use of force in war is violent, instrumental, and political, then there is no cyber offence that meets all three criteria."[42] From Rid's perspective, the term "Cyber War," is more a metaphorical figure of speech and less about describing the acts of war. The Conservative Cyber School of Thought regards cyber activity as more akin to acts of subversion, espionage, and sabotage than anything warlike in nature.[43]

Conservative thinkers see war as a violent and dangerous business and reject the notion of reducing harm and bloodshed through cyber acts. As Clausewitz argued in *On War*:

> Kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without much bloodshed, and might imagine this as the goal of the art of war. Pleasant as it sounds; it is a fallacy that must be exposed: war is such a dangerous business that the mistakes which come from kindness are the very worst.[44]

---

[40] Samuel B. Griffith and B. Liddell Hart, *The Art of War by Sun Tzu*, (New York: Oxford University Press, 1963), 75.
[41] Thomas Rid, *Cyber War Will Not Take Place* (Oxford ; New York: Oxford University Press, 2013), 1-2.
[42] Rid, *Cyber War Will Not Take Place* …, 4.
[43] Rid, *Cyber War Will Not Take Place* …, 10.
[44] Clausewitz et al, *On War*…, 75.

Admittedly Clausewitz in the early 1800's had no concept of the future ontological implications of technological integration and the dependence that cyber represents. The use of cyber capabilities to disarm or defeat an adversary is a futuristic concept more in line with a Revolutionary School scenario that articulates a potential outcome given the influence of technology on the *praxis* and nature of warfare. One extreme view of the potential influence of computers on warfare can be found in the original *Star Trek* science-fiction television series episode *A Taste of Armageddon*. The plot of the episode revolves around a society waging a computer based virtual war against an adversary on a nearby planet. In this visionary scenario, both warring parties comply with the results of the computer based virtual war and willfully submit to humane "disintegration booths" to avoid the Clausewitzian bloodshed and horrors of war. Regardless of how pleasant such a Revolutionary scenario may portray a possible future war, those in the Conservative School view the words of Clausewitz as immutable. They reject wholesale the notion that warfare would ever evolve to a point where computers would assume a highly technologic agency and fight wars on behalf of human beings.

In exploring the question of violence and its cyber implications, Rid argues that the majority of cyber "attacks" are not violent and cannot be considered acts of force. What force that results from cyber activities, such as causing a melt-down at a nuclear plant, would only take place indirectly through the kinetic potential of an existing system.[45] There is no direct link between the networked cyber environment and a human being. Therefore, a cyber-action in itself can not directly cause physical harm to an individual and is therefore non-violent: computer code is not explosive in the way that TNT is.[46]

[45] Rid, *Cyber War Will Not Take Place* …, 13.
[46] Rid, *Cyber War Will Not Take Place* …, 13.

Given that there is no direct threat to human life from cyber activity, the emotional coercive power that comes with the threat or use of cyber force is significantly reduced.[47] For example, the massive physical damage to a German steel mill caused by a digital cyber-attack on industrial control systems in 2014[48] went relatively unnoticed in the world media while killings of Canadian soldiers by individuals with extremist views made international headlines.[49] Furthermore, Rid argues that cyber weapons do not have the same symbolic and emotional impact as conventional weapons. Cyber capabilities cannot be physically paraded in a coercive show of force as with other weapons from the land, sea and air domains. Members of the Conservative School of Thought are highly focused on human agency and consider the human body as the true weapon or instrument of violence. In that context, if one were to look for symbolic examples of the potential threats posed by state-based cyber-power it would be a matter of considering the size and scope of a cyber-program in terms of personnel numbers and levels of expertise. The People's Liberation Army of China maintains the elite hacking Unit 61398 (also known as the Advanced Persistent Threat 1) alleged to be the focal point of Chinese cyber warfare.[50] Unit 61398 is alleged to employ thousands of skilled hackers in Shanghai to assert a "strategic hegemony in cyber space."[51] Despite the existence of thousands of skilled hackers in Unit 61398, such a symbol of intellectual capacity is less emotionally intimidating than the physical threat of violence posed by the same number of armed special operations force soldiers,

---

[47] Rid, *Cyber War Will Not Take Place* …, 17.

[48] Kim Zetter, "A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER," *WIRED*, last modified 01 January 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

[49] Philip Sherwell, "Canadian killer was recent convert to Islam identified as terror risk," *The Telegraph*, last modified 23 October 2014, http://www.telegraph.co.uk/news/worldnews/northamerica/canada/11181394/Soldier-killed-as-gunman-brings-terror-to-Canadian-Parliament.html.

[50] Pierluigi Paganini, "China vs US, cyber superpowers compared," *INFOSEC Institute*, last accessed 29 Apr 15, http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/.

[51] Paganini, "China vs US, cyber superpowers compared,"…, http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/.

tanks, fighter aircraft or warships. Therefore, the perceived threat of "code-induced violence is physically, emotionally and symbolically limited."[52]

Nevertheless, Rid admits that cyber-attacks can have the potential to achieve some political goals through non-violent means by undermining public trust in organizations, systems and institutions.[53] One such attack that conforms to this non-violent means paradigm is the Stuxnet malware on the Iranian nuclear program. A forensic review of the Stuxnet code determined that the malware was not created to cause physical damage to the Iranian facility but rather to destabilize the program by undermining the trust in the Iranian engineers to successfully produce low-enriched uranium.[54] It is not clear if the non-violent application of the Stuxnet malware contributed in any way to delay Iran's nuclear ambitions or encouraged international consensus on the Joint Action Plan on the Islamic Republic of Iran's Nuclear Program.[55] Interestingly, the Action Plan calls for the freezing of enriched uranium production and the deactivation of the centrifuges that were targeted in the Stuxnet attack.[56]

Rid argues that for "cyber weapons" to have any violent impact they must first "weaponize" a target system that indirectly inflicts violence on humans.[57] Rid defines cyber weapons "as computer code that is used, or designated to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems or living beings."[58] To inflict

---

[52] Rid, *Cyber War Will Not Take Place* …, 20.
[53] Rid, *Cyber War Will Not Take Place* …, 12.
[54] Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of what Stuxnet's Creators Tried to Achieve," (2013): 15.
[55] Executive Office of the President of the United States The White House, "Summary of Technical Understandings Related to the Implementation of the Joint Plan of Action on the Islamic Republic of Iran's Nuclear Program," last modified 16 January 2014, https://www.whitehouse.gov/the-press-office/2014/01/16/summary-technical-understandings-related-implementation-joint-plan-actio.
[56] BBC News, "Iran nuclear deal: Key points," last modified 20 January 2014, http://www.bbc.com/news/world-middle-east-25080217.
[57] Rid, *Cyber War Will Not Take Place* …, 25.
[58] Rid, *Cyber War Will Not Take Place* …, 37.

the maximum amount of damage and retain the maximum amount of flexibility, Rid suggests the thought of compromising weapons platforms such as Reaper or Predator drones would be far more attractive an exploit for attackers than an air traffic control system or nuclear power plant. Such a Revolutionary scenario of "weaponizing" a target system is similar to the main plot point in the James Bond movie *Tomorrow Never Dies* in which a media tycoon manipulates the Global Positioning System used by the Royal Navy to instigate conflict.[59] But in Rid's opinion, a lethal cyber scenario has never happened and due to a lack of proof remains the realm of Revolutionary fantasy, novels and science fiction movies.[60]

A common theme with the Conservative School is a need for public domain evidence that a particular cyber exploit exists before considering it as a potential weapon of warfare. Rooted in their evidence based epistemological process, Conservatives are fixated on past occurrences to understand the present. Extrapolation of concepts to consider the possibility of "the most dangerous" is difficult for this School. Instead, Conservatives tend to be content with adversarial assessments of "the most likely" future actions based on past observations. This type of inductive logic based solely on past evidence carries with it inherent challenges dealing with unexpected future events. Hume's Problem of Induction[61] often referred to as "Hume's Black Swan" or "Black Swan," outlines the pitfalls and complications that come from making predictive conclusions solely on observed facts.[62] Until a black swan was discovered in Australia by Dutch explorer Willem de Vlamingh in 1697, the common belief of the time was

[59] Rid, *Cyber War Will Not Take Place* …, 14.
[60] Rid, *Cyber War Will Not Take Place* …, 13.
[61] "That there is nothing in any object, considered in itself, which can afford us a reason for drawing a conclusion beyond it; and, that even after the observation of the frequent or constant conjunction of objects, we have no reason to draw any inference concerning any object beyond those of which we have had experience". Hume (1748) as quoted in Nassim Nicholas Taleb, "The Roots of Unfairness: The Black Swan in Arts and Literature," *Literary Research/Recherche Litteraire* 21, no. 41-42 (2005): 242.
[62] Taleb, "The Roots of Unfairness: The Black Swan in Arts and Literature,"…: 2.

that all swans were white in colour. Another simplistic analogy to understand the induction problem is to consider the life of a turkey.[63] From a turkey's perspective, life is wonderful based on the facts it has been fed regularly and protected by the farmer for its whole existence. The probability the turkey's lifestyle will "most likely" continue to be wonderful rings true right up until the day of its slaughter which it did not see coming. Similar to the lethality of cyber weapons, one cannot just discount the future possibility of a cyber-exploit that causes harm based on past public domain evidence.

Unfortunately, cyber warfare activities are being conducted in the shadows away from public scrutiny. As Noah Feldman states in his book *Cool War: The Future of Global Competition*, "Cyber war takes place largely in secret, unknown to the general public on both sides."[64] Fixated on the need for concrete public domain proof while scorning the abstract, Conservatives leave themselves vulnerable to surprise by "outlier" or "exceptional" cyber activity that carry potentially significant impacts for a nation's war fighting capability.[65] Black swans are a real epistemological quandary for members of the Conservative School.[66]

Additional Conservative Perspectives

Another key member of the Conservative School of Thought is David J. Lonsdale. In his book "The Nature of War in the Information Age: Clausewitzian Future," Lonsdale takes a slightly different conservative position on the nature of warfare and Cyberwar. Lonsdale (assisted by co-editor Colin S. Gray) argues that war possesses an "eternal nature" that does not

---

[63] Nassim Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed. (New York: Random House Trade Paperbacks, 2010), 40.
[64] Noah Feldman, *Cool War: The Future of Global Competition* (Random House Incorporated, 2013), 30.
[65] Taleb, *The Black Swan: The Impact of the Highly Improbable* …, xvii - xxvii.
[66] Taleb, "The Roots of Unfairness: The Black Swan in Arts and Literature,"…: 243.

change with the evolution of technology.[67] Instead, changes in technology may influence changes in the "character" or "material culture" of warfare but warfare's nature remains constant. The nature of warfare remains constant based on Clausewitz's primary trinity of hatred, primordial violence and enmity to impose one's will on an adversary.[68] True to the Conservative School of Thought, Lonsdale (and Grey) further argue that Clausewitz's thoughts on the nature of war are not limited to a particular historical period but can be applied to any context of warfare.[69]

Considering the nature of warfare in the information age, Lonsdale acknowledges that epistemological perspectives can be influenced by the culture and attitudes of a particular age.[70] In particular, western mind-sets in the information age that favour "clean," less destructive and more casualty sensitive forms of warfare. From the Conservative School perspective, such attitudes ignore the realities of war and reject the classical strategists Clausewitz, Sun Tzu, and Jomini.[71] Nevertheless, Lonsdale's vision of warfare is violent, uncertain and a high human agency that impacts both the physical and psychological.[72] Lonsdale further states:

> The human dimension of warfare is one area in which the character can affect its nature. If war remains an activity that is ultimately characterized by combat in which man is in conflict with man, then human factors and considerations will remain paramount.[73]

Lonsdale views the contribution of cyber in the conduct of war as an improved "means" to reduce the Clasuwitzian "uncertainty" or the "fog of war" by providing commanders with

---

[67] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, ix.
[68] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, x.
[69] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, x.
[70] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 22.
[71] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 22.
[72] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 28.
[73] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 38.

enhanced understanding of his adversary and the battlefield.[74] Lonsdale's views on cyber reducing uncertainty are consistent with the Conservative School perspectives on incremental/evolutionary approaches to technology. Information and knowledge of an adversary and battlefields have assisted commanders through the ages.[75] Modern day Information Technology (IT) is just an evolutionary step toward the same provision of information in the conduct effective military operations.

Unlike the perspectives proposed by Rid with respect to cyber warfare, Lonsdale does consider the possibility of paralysing cyber-attacks on society's interconnected infrastructure such as power generation, food distribution, finance and transportation. Lonsdale envisions this type of warfare (Strategic Information Warfare) can only be effective on heavily networked societies that that are unable to operate if the life sustaining infrastructure ceases to function.[76] Strategic Information Warfare (SIW) is viewed by Lonsdale as a complementary means of strategy to deny an adversary freedom of action. Paralleling Clauswitiz's view on the view of artillery winning battles:

> …the actual core of an engagement lies in the personal combat of man against man. An army composed simply of artillery, therefore, would be absurd in war.[77]

Lonsdale acknowledges the limitations of SIW as a sole means of strategy and admits troops on the ground are the typical means of strategy to achieve final victory.[78]

Conclusions

---

[74] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 41.
[75] Clausewitz et al, *On War*…, 117-121.
[76] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 142.
[77] Clausewitz et al, *On War*…, 285.
[78] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*…, 170.

This chapter considered Conservative perspectives within the Cyber Warfare Schools of Thought schema. Conservative perspectives are heavily influenced by classical war theorists such as Carl von Clausewitz for the foundation of their epistemological assessment of military affairs. In the eyes of Conservatives, the physical and brutal nature of war is an enduring truism. Citing the intangible elements of morale as the cornerstone of their epistemological approach to warfare, Conservatives are more focused on human agency and its influence on strategy. The Conservative School favours the preservation of the established praxis of warfare and in doing so opposes the contemplation of changing their perspectives based on any ontological changes that may be due to technology.

Stereotypically, Conservative perspectives are reluctant to contemplate new concepts that challenge the nature and dogma of warfare. They interpret increases in technology as incremental / evolutionary changes built on the groundwork of previous technological improvements. Some in the Conservative camp view cyber warfare as a technological extension of electronic warfare and not a revolutionary change in military communications. On the other hand, stauncher Conservatives view cyber activity as nothing more than subversion, espionage, and sabotage and not a means of warfare. Declarations of revolutionary breakthroughs in technology are met with considerable conservative scepticism. The Conservative approach to technology rejects revolutionary claims of breakthroughs and often regards such claims as “old wine in a new bottle.”

In the next chapter this paper will explore the fundamental characteristics of the Revolutionary Materialist School of Thought. A group at the opposite end of the School

of Thought spectrum from Conservatives, Revolutionaries are defined by their highly technologic agency perspectives. Instead of looking to the past for answers on our present day ontology, Revolutionaries look forward to potential futuristic outcomes. This paper will explore how Revolutionaries leverage "out of the box" non-traditional thought within their epistemological approach to more effectively understand humanity's relationship with technology and the potential implications on the praxis and nature of warfare.

> *If we have learned one thing from the history of invention and discovery, it is that, in the long run — and often in the short one — the most daring prophecies seem laughably conservative.*
>
> - Arthur C. Clarke

> *One of the biggest roles of science fiction is to prepare people to accept the future without pain and to encourage a flexibility of mind. Politicians should read science fiction, not westerns and detective stories.*
>
> - Arthur C. Clarke

CHAPTER 3 – THE REVOLUTIONARY MATERIALIST SCHOOL OF THOUGHT

Revolutionary Materialists are visionaries that look to potential future outcomes of technology to comprehend and better understand changes to society and our very being. Revolutionaries believe that humanity's integration with cyber technology will profoundly alter the character if not the nature of warfare. Contrary to Conservatives who refer back to classical war theorists and historical battle outcomes to understand the impact of technology and likely courses of action, the Revolutionary School considers potential future outcomes in terms of the worst case scenarios in order to adequately defend against the threats of tomorrow. This

particular School of Thought is heavily influenced by visionaries and science fiction figures such as Isaac Asimov, Author C. Clarke, Marshall McLuhan, and Gene Roddenberry. Despite successes at predicting technological trends and their impact on society, Revolutionary Materialists are often considered by Conservatives as alarmists, nerds, or "parrots"[79] spinning "[s]cience-fiction yarns"[80].

Nevertheless, Revolutionaries have had a tremendous impact on discussions of cyber warfare. Their predictions of the ease with which society can be brought to its knees through the tools of information technology make for good copy in newspapers, as well as profitable movies and other forms of entertainment. Many of the Revolutionary predictions on the dangers of cyberspace even predate the popular adoption of networking technologies such as the internet.[81] Authors found within the Revolutionary Materialist School of Thought include Richard Clarke, Winn Schwartau, Jeffrey Carr, Greg Rattray, Wayne Hall, John Arquilla, and David Ronfeldt.

Revolutionaries tend to be the most materialist of any School of Thought, focusing almost exclusively on the opportunities offered by information technology and the impact of logical interactions of electrical/electromagnetic impulses. Their approach closely resembles the predictions made by air power theorists such as Giulio Douhet during the inter-war period of the 20th century.[82] At its heart, the Revolutionary School of Thought is a manoeuvrist approach to warfare: agents avoid striking at the concentration of power found in a state's military, and attack the source of that power by collapsing critical infrastructure. It is thought that collapsing critical

---

[79] Gray, *Strategy for Chaos: Revolutions in Military Affairs…*, 280.

[80] Arthur C. Clarke, "Dial 'F' for Frankenstein," *Playboy* (1965).

[81] The US National Research Council report *Computers at Risk*, published in October of 1990, introduced the idea, since widely cited that "the modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb." - Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 1st ed. (New York; Emeryville, CA: Thunder's Mouth Press; Distributed by Publishers Group West, 1994), 13.

[82] Giulio Douhet, *The Command of the Air* (University of Alabama Press, 2009).

infrastructure results in either social chaos in the forms of riots, runs on the bank, and famine like domestic conditions, or it creates a more limited form of political paralysis. In either case, the state is prevented from pursuing military action as a result of the loss of internal cohesion.

As one would expect there is considerable overlap between those who subscribe to the concept of an RMA and cyber warfare revolutionaries. As Arquilla and Ronfeldt point out:

> … history is filled with examples in which weapon, propulsion, communication and transportation technology provide a basis for advantageous innovations in doctrine, organisation, and strategy that enable the innovator to avoid exhausting attritional battles and pursue a form of decisive warfare.[83]

However, cyberspace is regarded by the Revolutionary School as the "new high ground" much as earlier forms of technological innovation in aircraft and space technologies were thought to confer strategic advantages. For the Revolutionary, there is no ambiguity about the reality of the threat posed by cyber capabilities. It is instantaneous and global in nature, skips the battlefield and is already happening. As USAF Lieutenant General Robert Elder, Commander USAF Cyber Operations Task Force 2006-2009, stated:

> …if you are defending in cyberspace, you're already too late. If you do not dominate in cyberspace, you cannot dominate in other domains. If you are a developed country [and you are attacked in cyberspace], your life comes to a screeching halt.[84]

The possibilities offered by contemporary technology are sure to expand in the future: "What we have seen is far from indicative of what can be done."[85] The possibility of a society leveling

---

[83] Arquilla and D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Vol. MR-880 (Santa Monica, Calif.: Rand, 1997), 1.

[84] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and what to do about It*, 1st ed. (New York: Ecco, 2010), 36.

[85] Clarke et al, *Cyber War: The Next Threat to National Security and what to do about It …,* 30.

event, often referred to as either an "Electronic Pearl Harbor" (EPH)[86] or a "Digital 9/11"[87] are frequently alluded to. EPH's are alleged to be a likely consequence of cyber warfare given the interdependencies of industry, finance, transportation, power, and communication for the generation of wealth and power in modern developed economies. As Winn Schwartau argues in *Information warfare: Chaos on the electronic superhighway*, "[g]overnment and commercial systems are so poorly protected today that they can be essentially be considered defenseless…." [88]

Futuristic scenarios figure prominently in the Revolutionary literature. Scenarios enable the analyst to transcend history by describing hypothetical events and concepts.[89] Schwartau asks us to imagine a world in which knowledge and information usurp military might; where whomever controls information can control the people; where privacy no longer exists; in short a world where bombs and bullets have been replaced by bits and bytes.[90] Rattray describes large scale offensive assaults on information assets supporting the critical infrastructure of modern society such as EPH's and Cyber 9/11's.[91] Thus, air traffic control systems and other transportation networks, stock markets, credit card and banking transactions, communication networks including telephone exchanges, publishing, newspapers, and manufacturing, all of which are heavily dependent on computerised systems, can be destructively targeted by cyber

[86] John Schwartz, "Preparing for a Digital Pearl Harbor," *New York Times* (2007).
[87] Karen J. Greenberg, "Preparing for a Digital 9/11," *TomDispatch*, last modified 21 October 2012. http://www.tomdispatch.com/blog/175607/.
[88] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 13.
[89] Mikkel Vedby Rasmussen, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century* (Cambridge University Press, 2006), 43-90.
[90] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 14-15.
[91] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and their Use," In *Proceedings of a Workshop on Deterring Cyberattacks, Informing Strategies and Developing Options for US Policy* (2010): 8.

capabilities.[92] Carr describes a scenario in which nuclear power plants are targeted by a combination of distributed denial of service attacks initiated by a Conficker-type botnet[93] to distract the plants' control room operators. Meanwhile, Trojan horses infiltrate the plants' firewalls by means of socially engineered attacks, enabling external agents to take control of the control processes. In the ensuing attack, these agents crash the safety systems of 70% of America's nuclear plants, causing core meltdowns at scores of sites around the country.[94] Some scenarios describe combinations of cyber and kinetic attacks, car bombs as well as information attacks, coordinated to cause waves of terror.[95] These scenarios are not simply ahistorical, they are also apolitical. As Hall points out, "we are in a '100 Years' War' against formidable and creative opponents. The struggle involves a zero-sum triumph of will – there will be no compromise from either side until one side wins or the other loses."[96] However, *who* one is in a war against, and *what* are their objectives is left for the reader to imagine, surely as strange a war as ever has been. Such generic descriptions focus exclusively on the technical capabilities offered by cyber tools, failing to explain the political circumstances which might lead to their use.

As mentioned previously, technologically influenced scenarios and visions of this School are often articulated in the writings of futurists or manifested in popular culture and fantasy comic

---

[92] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001), 12.

[93] "The Conficker worm first appeared in October 2008 and quickly earned as much notoriety as Code Red, Blaster, Sasser and SQL Slammer. The infection is found in both home and business networks, including large multi-national enterprise networks.[….] Conficker is called a worm because the first discovered variant attached to a program (executable), was self-replicating, and (importantly) used a network as the delivery mechanism. This combination of characteristics distinguishes worms from viruses. Conficker is actually a blended threat8 because it can be delivered via network file shares, mapped drives and removable media as well. The Conficker infection is a type of software called a Dynamic Link Library (DLL)." - David Piscitello, "Conficker Summary and Review," *ICANN, May 7* (2010).

[94] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media Inc., 2011), 9-11.

[95] Wayne M. Hall, *Stray Voltage: War in the Information Age* (Annapolis Md; Naval Institute Press, 2003), vii – x.

[96] Hall, *Stray Voltage: War in the Information Age* …, x..

books, television dramas or feature films well before their main-stream acceptance. Arthur C. Clarke's story *Dial 'F' for Frankenstein* outlines a tale of a global communication network becoming self-aware and eventually waging war on humanity.[97] Interestingly enough, Clarke's vision of a communication network from 1964 is eerily similar to the modern day cyber environment. Members of the Revolutionary School look to visionaries like Clarke to convince others of the potential dangers of a highly technologic agency world.

Interestingly in 2009, Schwartau asked us to imagine a world in which information warfare, the control of information and the generation of fear in those concerned about information privacy. Citing the linkages between information warfare and the coercive elements of money, fear and power, Schwartau states:

> Information warfare is about money. It's about the acquisition of wealth, and the denial of wealth to competitors. It breeds Information Warriors who battle across the Global Network in a game of cyberrisk. Information warfare is about power. He who controls the information controls the money. Information Warfare is about fear. He who controls the information can instill fear in those who want to keep their secrets a secret.[98]

The themes of information warfare and the fear of controlling secret information were also employed in the 2011 CBS television network program *Person of Interest*,[99] a techno-drama centered on self-aware computer systems, *Northern Lights* and *Samaritan*, built for the US government to record individuals' activities and predict potential acts of terrorism. Part of the allure of such entertainment relates to the engendered fear relating to the loss of individual privacy and the misuse of information that defines our very being. A Revolutionist could even argue that the loss of control over an individual's information represents a potential loss of

---

[97] Arthur C. Clarke, "Dial 'F' for Frankenstein," *Playboy* (1965).
[98] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 15.
[99] CBS, "Person of Interest," last accessed 14 April 2015, http://www.cbs.com/shows/person_of_interest/.

control over the very notion of one's existence. With the leak of classified information in 2013 by the IT specialist Edward Snowden, the fears of state surveillance imagined by Schwartau and portrayed in *Person of Interest* were validated as details of the NSA clandestine surveillance program PRISM were made public.[100] It is alleged that the PRISM program began in 2008 to collect "relevant" internet communications in order to protect US citizens. Despite attempts by the US government to characterize PRISM as a required tool for domestic security, the potential for abuse of individual liberties is considerable not to mention the significance of such a capability in the greater context of international information warfare.

[100] Jennifer Stisa Granick and Christopher Jon Sprigman, "The Criminal NSA," *International Herald Tribune* (2013): 29-30.

Impacts of Big Data

Viktor Mayer-Schönberger is a member of the Revolutionary School who writes about "Big Data" and the ontological impacts on society living in the information age. Mayer-Schönberger characterizes "Big Data" as:

> …things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments and more.[101]

Mayer-Schönberger argues that at the core of "Big Data" lies the power to generate better predictions. Some may confuse "Big Data" with Artificial Intelligence (A.I.) and the pursuit to have computers reason similar to humans. Instead, the concept of big data involves computers applying mathematical models to large amounts of data to arrive at effective predictions.[102] In addition, the predictions improve with time by analysing patterns and outcomes. Mayer-Schönberger predicts that in the future many tasks that require explicit human judgement will be augmented or replaced with big data systems.[103] The Mayer-Schönberger vision of the big data and mass surveillance is very similar to the ones expressed by Revolutionaries Schwartau and *Person of Interest* creator Jonathan Nolan about artificial intelligence capabilities that will be able to not only drive cars and play chess but predict illness, identify probabilities of violent acts or decide who threats to society are. Liberal Materialist understand the challenge of "data-driven thinking"[104] and look to ways of regulating the technology to avoid the "dark side" of big data

[101] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform how we Live, Work, and Think* (Houghton Mifflin Harcourt, 2013), 18.
[102] Mayer-Schönberger et al, *Big Data: A Revolution* …, 23.
[103] Mayer-Schönberger et al, *Big Data: A Revolution* …, 24.
[104] Economist Intelligence Unit, "Big Data-Lessons from the Leaders," *Londres: The Economist* (2012): 19.

and the removal of human intervention from the advice used for key decisions. [105] Predictions made from big data may precipitate pre-emptive commercial and state decisions (including lethal force) against individuals or groups based on math and "probabilistic cause."[106] Mayer-Schönberger expresses concern about the "dark side" of big data and the potential for the misuse and abuse: "It leads to an ethical consideration of the role of free will versus the dictatorship of data… the age of big data will require new rules to safeguard the sanctity of the individual."[107] The information revolution has produced an environment in which "the amount of data in the world is growing fast, outstripping not just our machines but our imaginations." [108] The concern of being inundated by information is encapsulated in a quote by Joel Kurtzman:

> "Cyberspace, like the earth itself, is becoming polluted. Too much information is filling it. And our brains are just too tiny to sort through it all. Information overload threatens to bring further catastrophe, no matter how well the trading rooms are designed."[109]

[105] Mayer-Schönberger et al, *Big Data: A Revolution* …, 28.
[106] Mayer-Schönberger et al, *Big Data: A Revolution* …, 28.
[107] Mayer-Schönberger et al, *Big Data: A Revolution* …, 28.
[108] Mayer-Schönberger et al, *Big Data: A Revolution* …, 20.
[109] Joel Kurtzman quoted in Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 78.

Fear of Computers and Artificial Intelligence

According to Schwartau one has an inherent mistrust for computers.[110] This mistrust stems from a computer's processing ability which is significantly faster than the human brain. Since human mental processing is dwarfed by the computational power of modern computers people perceive them as uncontrollable. Furthermore, despite being dependent on computers to sustain civilization, human angst about computer superiority is augmented by a complete lack of knowledge by most as to their internal processing.

A good Revolutionist scenario that portrays the devastating outcome when code is allowed to replace human judgment occurs in the *Terminator* franchise. In *Terminator 3: Rise of the Machines,* the self-aware code Skynet outwits its USAF masters with an intelligent virus and initiates global nuclear war known as Judgement Day. Skynet's intelligent virus was able to exploit cyber vulnerabilities in key strategic defence systems to leave the US defenseless. Skynet was then given full automated control of the US military systems to eradicate the virus which was beyond the capacity of USAF personnel to resolve. The Revolutionist visionary scenarios within the *Terminator* franchise are cautionary tales of out of control artificial intelligence and automated integration that play on the fears of human inferiority within a technological society. Removing human judgment from prosecuting the complex problem in the *Terminator* scenario allowed the artificial intelligence to take over the world with lethal force. Such fearful Revolutionary scenarios parallel the growing debate over the implications of employing artificial intelligence for military purposes including Lethal Autonomous Weapons Systems (LAWS).[111] Revolutionaries can see that if militarized artificial intelligence and automated weapon systems

[110] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway …*, 22.

[111] Kathleen Harris, " 'Killer robots' pose risks and advantages for military use," *CBC News,* last modified 09 April 2015, http://www.cbc.ca/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963.

replace human decision making in the application of lethal force, the nature of warfare will shift from high human agency to a higher technologic agency.[112]

Neural Interfaces and Cyborgs

Another member of the Revolutionary School is the Canadian philosopher Herbert Marshall McLuhan. Best known for his catch phrase "the medium is the message," McLuhan in several works conveyed his thoughts about communication technology and how it influences human activity and interaction.[113] McLuhan's revolutionary conceptions of technological phenomenon clearly place him in the Revolutionary School. His revolutionary thoughts on changes to the human ontology give way to ideas of humanity becoming integrated nodes on a network. McLuhan states:

> During the mechanical ages we had extended our bodies in space. Today, after more than a century of electric technology, we have extended our central nervous system itself in a global embrace, abolishing both space and time as far as our planet is concerned. Rapidly, we approach the final phase of the extensions of man - the technological simulation of consciousness, when the creative process will be collectively and corporately extended to the whole of human society, much as we have already extended our senses and our nerves by the various media.[114]

In his book *Understanding Media: The Extensions of Man*, McLuhan makes the distinction between the physical extensions of the body and the extensions of cerebral functions such as sense, consciousness and the central nervous system.[115] One scenario that encapsulates McLuhan's futuristic perspectives relating to the physical extension of the body through an

---

[112] Owen Bowcott, "UN urged to ban 'killer robots' before they can be developed," *The Guardian*, last modified 09 April 2015, http://www.theguardian.com/science/2015/apr/09/un-urged-to-ban-killer-robots-before-they-can-be-developed.

[113] Herbert Marshall McLuhan, *Understanding Media: The Extensions of Man*, 1st ed. (New York: McGraw-Hill, 1964).

[114] McLuhan, *Understanding Media: The Extensions of Man* …, 3.

[115] McLuhan, *Understanding Media: The Extensions of Man* …, 43.

interface occurs in Craig Thomas' 1977 techno-thriller novel *Firefox*.[116] Thomas's novel envisions a scenario in which the Soviet Union develops a next-generation fighter prototype MIG-31 equipped with a thought control weapons system. The revolutionary idea of having the pilot control a planes weapon system through a neural interface raises the possibility of being able to aim and fire weapons more rapidly while in combat. In doing so, the pilot in essence becomes an extension of the aircrafts weapon systems. This scenario is consistent with the theme of McLuhan's revolutionary writings in which "…all technologies are extensions of our physical and nervous system to increase power and speed."[117]

Researchers at the University of Pittsburgh are investigating the concepts of thought control and neural interfaces by controlling a robotic limb through cerebral implants.[118] Employing implants to connect a human directly to technology parallels McLuhan's revolutionary concept of extending cerebral functions through technology. Members of the Revolutionary School look at such research developments as the foundation to further envision potential military implications of integrating the human nervous system with a cybernetic-interface. One such visionary scenario that deals with the extensions of a pilot's cerebral functions and central nervous system occur in Dale Bown's 1989 novel *Day of the Cheetah*.[119] Brown's novel envisions a fighter aircraft equipped with a thought control interface that controls all aspects of combat flight. Brown's concept of full pilot mental integration provided the pilot with an integrated consciousness of all aircraft flight and combat systems. Brown's fictitious XF-34 aircraft transformed the pilot and plane into a singular cybernetic killing machine. Brown's

[116] Craig Thomas, Firefox (London: Joseph, 1977), 288.
[117] McLuhan, *Understanding Media: The Extensions of Man* …, 90.
[118] Institute of Physics, "Thumbs-up for mind-controlled robotic arm," last modified 17 December 2014, http://www.iop.org/news/14/dec/page_64708.html.
[119] Dale Brown, *Day of the Cheetah* (New York: Berkley, 1989).

Revolutionary scenario may appear to some as complete flights of fancy with no basis in reality. Interestingly enough, the cybernetic research conducted by the University of Pittsburgh has been expanded with the assistance of the US Defense Advanced Research Projects Agency (DARPA) to demonstrate that an F-35 aircraft simulator can be operated through cybernetic implants.[120] One particular experiment proved that a quadriplegic woman could control an F-35 flight simulator using only neural implants.[121] The use of cybernetic implants and neural integration to enhance one's abilities is commonly referred to in science-fiction as a Cyborg.[122]

To Revolutionaries, the concept of cyborgs and cybernetic implants to improve man's ability to wage war is nothing new. In main stream popular culture cybernetic beings have appeared in television shows from *Doctor Who* to *Star Trek*. In *Star Trek: The Next Generation* a cybernetic and emotionally absent race of humanoids known as *Borg* employ cybernetic implants to better their race in a pursuit of perfection of being. The Borg's implants allow them to intercommunicate and fight as a more effective collective. The collective "hive mind" gives the Borg superior ability to fight with a unity of effort and purpose. In addition, the rapid passage of information allows Borg forces to rapidly adapt tactics against adversarial initiatives. In the information age, the Borg represent an ideal military force that is able to have perfect synchronization of command intent with the ability of passing all force knowledge to each individual soldier. "Our conceptualization of the Borg centers on the collective ontological and cybernetic formation that result from being connected to other brains and bodies through

---

[120] Abby Phillip, "A paralyzed woman flew an F-35 fighter jet in a simulator — using only her mind," *Washington Post*, last modified 3 March 2015, http://www.washingtonpost.com/news/speaking-of-science/wp/2015/03/03/a-paralyzed-woman-flew-a-f-35-fighter-jet-in-a-simulator-using-only-her-mind/.

[121] Nick Stockton, "WOMAN CONTROLS A FIGHTER JET SIM USING ONLY HER MIND," *WIRED*, last modified 5 March 2015, http://www.wired.com/2015/03/woman-controls-fighter-jet-sim-using-mind/.

[122] "a person whose body contains mechanical or electrical devices and whose abilities are greater than the abilities of normal humans." - Merriam-Webster, "cyborg," last accessed 01 May 2015, http://www.merriam-webster.com/dictionary/cyborg.

embodied technology."[123] In a Borg society all humanoids are fully integrated into the collective cyber environment similar to any network appliance and the Borg "collective" represents a singularity of consciousness and being. DARPA's well-intentioned pursuit to "to use brain implants to read, and then control, the emotions of mentally ill people"[124] may be the initial stages of creating highly integrated and emotionally absent soldiers. DARPA's work with cybernetic implants and neural interfaces potentially represent the first step for humanity toward a Borg-like culture.[125] Some may also argue that humanity has already taken the first step toward a Borg-like society with the creation of a highly interconnected cellular culture through the proliferation of smart phone and wireless devices.[126] Oddly enough, it was the *Star Trek* communicator from the 1964 series that served as the inspiration behind the revolution in mobile personal communications.[127]

A New Era of Warfare

In order to emphasise the revolutionary nature of an era, Revolutionaries tend to propose new categories of emerging warfare and associated conceptual language. Hall discusses "Knowledge War", which he describes as "an intense competition for valuable information and knowledge that both sides need for making better decisions faster than the adversary."[128] In this, there is an obvious linkage between this concept and the thinking of Col. John Boyd and his

---

[123] Ronnie D. Lipschutz and R. Hester, "We are the Borg! Human assimilation into cellular society," *academia.edu*, last accessed 01 May 2015, https://www.academia.edu/6169698/We_are_the_Borg_Human_assimilation_into_cellular_society.

[124] Antonio Regalado, "Military Funds Brain-Computer Interfaces to Control Feelings," *MIT Technology Review*, last modified 29 May 2014, http://www.technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/.

[125] Regalado, "Military Funds Brain-Computer Interfaces to Control Feelings," ..., http://www.technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/.

[126] Lipschutz et al, "We are the Borg! Human assimilation into cellular society,"…, https://www.academia.edu/6169698/We_are_the_Borg_Human_assimilation_into_cellular_society.

[127] Paul Hsieh, "8 Star Trek Technologies Moving From Science Fiction To Science Fact," *Forbes*, last modified 24 June 2014, http://www.forbes.com/sites/paulhsieh/2014/06/24/8-star-trek-technologies/.

[128] Hall, *Stray Voltage: War in the Information Age* …, 2.

Observe, Orient, Decide and Act (OODA) Loop.[129] The goal of knowledge warfare is to find and "sustain decision dominance, which leads to an overall advantage in decision making and results in a triumph of will by one side or the other."[130] Hall argues that technology produces three specific features which enable the generation of knowledge warfare. First, the inter-relations between social, economic, and political systems create a "world tapestry of systems."[131] This tapestry enables second and third order effects to be created by pulling on the threads of this tapestry, even from a distance. Second, "truth" has increasingly become a relative variable, rather than an absolute one. As such, this opens up many paths to consider what constitutes the "proper" course of action. While this certainly raises the spectre of anarchy and relativism, it also frees individual decision makers from "dogmatic thinking", opening up new paths for creative problem solving. Finally, technology unites these two aspects together and reflexively speeds up the process as it advances in capability. "Victory in future conflicts will go to the side whose leaders make the best use of knowledge to make the most effective and, in some cases, quickest decisions."[132] Thus, knowledge leads to better decisions, resulting in rapid actions generating political effects, which in turn influence the will of the enemy to continue engaging in conflict.[133]

Irrespective of whether they discuss novel forms of warfare that will emerge in this new era, Revolutionaries tend to emphasise the opportunities for manoeuvre that emerge with cyber warfare. Schwartau argues that cyber offers "subtlety" in achieving strategic goals, a better way to reach them without the chaos and bloodshed of kinetic operations.[134] The goals of

---

[129] John R. Boyd, "The Essence of Winning and Losing," *Unpublished Lecture Notes* (1996).
[130] Hall, *Stray Voltage: War in the Information Age* …, 2.
[131] Hall, *Stray Voltage: War in the Information Age* …, 9.
[132] Hall, *Stray Voltage: War in the Information Age* …, 3.
[133] Hall, *Stray Voltage: War in the Information Age* …, 3-4; 9-10.
[134] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 82.

"information warriors" is to steal information in order to turn it against their opponents, modify information in order to instill fear or embarrass them, the outright destruction of information to deny its use, and only finally, to destroy information infrastructure so as to put the method for transmitting information out of commission.[135] Hall echoes this emphasis on manoeuvre in his writings as well. Information warfare is linked to "asymmetric warfare" in its emphasis on affecting and influencing behaviour as opposed to movement and control of terrain and the destruction of objects on that terrain.[136] Hall cites Sun Tzu, a theorist of revolutionary concepts, arguing that the real terrain of battle lies in the minds of humans and manoeuvre involves the manipulation of knowledge and the psyches of human beings as central to this modality of warfare.[137] Influenced by Sun Tzu's writings on offensive strategy, "those skilled in war subdue the enemy's army without battle."[138]; Carr offers a definition for cyber warfare that captures its indirect nature along with the sophistication of Sun Tzu inspired strategy: "Cyber Warfare is the art and science of fighting without fighting, of defeating an opponent without spilling their blood."[139]

Arquilla and Ronfeldt are two of the most prominent Revolutionary writers in the canon. Since their seminal piece *"Cyberwar is Coming!"*[140] they have published numerous works examining the impact of modern information technology on contemporary conflict.[141] Both were among the first to use the term "Cyberwar" as a conceptual tool as well as developing a civil

---

[135] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 82-85.
[136] Hall, *Stray Voltage: War in the Information Age* …, 4.
[137] Hall, *Stray Voltage: War in the Information Age* …, 5.
[138] Griffith et al, *The Art of War by Sun Tzu* …, 79.
[139] Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* …, 2.
[140] John Arquilla and David F. Ronfeldt, *Cyberwar is Coming!*, Vol. P-7791 (Santa Monica, Calif.: Rand Corporation, 1992).
[141] Other works by John Arquilla and David F. Ronfeldt: *Advent of Netwar* (1996); *In Athena's Camp: Preparing for Conflict in the Information Age* (1997); *Networks and Netwars: The Future of Terror, Crime and Militancy* (2001); and *Netwar Revisited: The Fight for the Future Continues* (2002).

oriented term, "Netwar" to describe non-military use of information weaponry. Both concepts attempt to create similar conditions: interference in "what a target population knows or thinks it knows about itself and the world around it."[142] Netwar is aimed at elite and public opinions and works through the use of propaganda, subversion, deception, and interference with the media. Cyberwar, on the other hand, while similar in nature, focuses solely on military use of these vectors to alter "the balance of information and knowledge in one's favour, especially if the balance of forces is not." Both concepts seek to take advantages of the technological affordances of IT to lower the entry costs of these activities: as less capital and labour is necessary to initiate this type of activity, smaller, less well-resourced, decentralized and agile groups are able to take on larger, centralized, and static institutions.[143] Arquilla and Ronfeldt share similar ideas to Hall's "Knowledge War" in that they argue that actors involved in Netwar aim to "confound people's fundamental beliefs about the nature of their culture, society, and government, partly to foment fear, but mainly to disorient people and unhinge their perceptions." Thus, "Epistemological War" structurally challenges an organisation by raising fundamental questions as to whose responsibility it is to respond and what missions are necessary to undertake: "When roles and missions of defenders are not easily defined, both deterrence and defence become problematic."[144]

Following from their Netwar concept, Arquilla and Ronfeldt discuss the spread of social conflict onto the internet and how Cyberwar manoeuvre also takes place in terms of the actors who are introduced to this new battlespace. Small communities of interest now have not only the

[142] Arquilla et al, *Cyberwar is Coming!* …, 28.
[143] John Arquilla and D. Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: National Defense Research Institute, RAND, 1996), 5-6.
[144] Arquilla et al, *The Advent of Netwar* …, 14.

ability to confront states more aggressively.[145] Netwar enables non-state actors, NGOs and other militant social activists, and even states pursuing limited objectives with limited means to attack policy problems.[146] The recent activities of "Anonymous,"[147] which has targeted states, corporations, and other interest groups, provides an obvious example of this effect, however, so do the Tea Party and Occupy Wall Street movements in the US, as well as certain aspects of the Arab Spring.[148] However, illegitimate actors may also participate and may ultimately form the principal drivers for this form of activity. Carr notes that "cyber-crime is the lab where malicious payloads and exploits used in cyber warfare are developed, tested and refined."[149] All this points to a more fluid operational environment where the lowered entry costs to strategic competition between social groups lends agency to groups that have traditionally had more limited opportunities to participate. In effect, the growth of strategic capability on the part of these new actors has increased the manoeuvre space available to these groups, and further complicated the military operating environment for more traditional strategic actors.

Arquilla and Ronfeldt are firmly in the Revolutionary camp with these concepts. They argue that both Cyberwar and Netwar are waypoints towards a new post-industrial era, arguing

---

[145] Arquilla et al, *The Advent of Netwar* …, 5. Arquilla and Ronfeldt define Netwar as an "emergent form of conflict (and crime) at societal levels, short of war in which the protagonists use network forms of organization and related doctrines, strategies and technologies attuned to the information age."

[146] Arquilla et al, *The Advent of Netwar* …, vii.

[147] "Some vigilantes are affiliated with loosely knit hacking organizations like Anonymous, known more for infiltrating computer networks of governments and corporations to make political statements or for the "lulz" — the hacker term for laughs" – Rick Gladstone, "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State," *New York Times*, last modified 24 March 2015, http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?ref=topics.

[148] John Pollock, "Streetbook: How Tunisian and Egyptian Hackers and Soccer Fans Created the Arab Spring," *MIT Technology Review*, last modified 23 August 2011, http://www.technologyreview.com/featuredstory/425137/streetbook/.

[149] Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* …, 5.

that the age of attrition is coming to an end and that military forces may not even need to be engaged in order to achieve victory.[150] Arquilla and Ronfeldt state:

> The emergence of Netwar [and Cyberwar for that matter] implies a need to rethink strategy and doctrine, since traditional notions of war as a sequential process based on massing, maneuvering and fighting will likely prove inadequate to cope with a non-linear landscape of conflict in which societal and military elements are closely intermingled.[151]

Greg Rattray introduces the concept of "Strategic Information Warfare", which "describes efforts to defeat opponents through attacks on centres of gravity without fighting fielded military forces."[152] Similar to Arquilla and Ronfeldt's Netwar, Strategic Information Warfare targets the opponent's will to fight, his ability to carry on normal economic routines, and command fielded forces.[153]

The Revolutionary perspective on this emerging cyber environment is also of a particular character. Revolutionaries tend to be deterministic in their outlook on the impact of technology on the strategic environment.[154] For Schwartau, the technological environment of IT is the source of Cyberwar. Networks' ability to defy borders, their utility in the spread of information enabling all to weigh their local circumstances against conditions elsewhere, the clean and bloodless nature of Cyberwar and the low risks of action versus the high payoffs for success, all motivate consideration of it as a strategic vector for influencing others. Because in general high technology is poorly understood, yet still highly relied upon, fear of the unknown means that cyber-events will generate a significant amount of fear. Last, Schwartau concludes that

---

[150] Arquilla et al, *Cyberwar is Coming!* …, 44.
[151] Arquilla et al, *The Advent of Netwar* …, vii.
[152] Rattray, *Strategic Warfare in Cyberspace* …, 22.
[153] Rattray, *Strategic Warfare in Cyberspace* …, 99-100.
[154] For a discussion on Technological Determinism, see Joelien Pretorius, "The Technological Culture of War," *Bulletin of Science, Technology & Society* (2008).

Cyberwar will take place simply because it can. In other words, technology is an anarchic free force that will sweep all before it.[155]

Clarke focuses on the actual design of the internet as a causative factor in the appearance of Cyberwar. Noting that the Internet was designed to share information, not for security, Clarke notes that features such as the Domain Name Service, the internet's addressing system, is easily spoofed as is the routing system, the Border Gateway Protocol. Internet reliance on open and unencrypted software allows any with the will to reprogram and interfere with the system; indeed its decentralised design with a lack of centralised control measures are often the excuse for facilitating systematic anarchy which facilitates bad behaviour.[156] The same technological features also create a first strike incentive for those considering Cyberwar attacks. A Cyberwar attack to an offensively minded group offers several advantages: speed of attack, anonymity, the difficulty to deter such attacks, and the continued secrecy with which cyber events are treated by governments and corporations. Given such overwhelmingly positive incentives to conduct a Cyberwar strikes, Cyber capable groups are left without any need to reflect on the possible repercussions of such an act.[157]

Arquilla and Ronfeldt also discuss technology in a deterministic fashion. Information technology disrupts and erodes hierarchies, by diffusing and redistributing power, crossing borders, expanding spatial and temporal horizons, and opening closed systems. Arquilla and Ronfeldt state:

> The information revolution favours the growth of such networks by making it possible for diverse, dispersed actors to communicate, consult, coordinate and

[155] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway …*, 20-22.
[156] Clarke et al, *Cyber War: The Next Threat to National Security and what to do about It …,* 74-82.
[157] Clarke et al, *Cyber War: The Next Threat to National Security and what to do about It …,* xi.

> operate together across greater distances and on the basis of more and better information than ever before.[158]

These conditions allow "swarming" actions to occur, when dispersed nodes converge on a target or issue area from multiple directions in a sustained pulse of activity. Nodes coalesce rapidly and stealthily; once the task is completed, they disengage and re-disperse, and then ready themselves for the next pulse. This is viewed as being considerably different from typical mass and manoeuvre of conventional military operations.[159] As they put it:

> […] the information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. The rise of network forms of organization … is one of the single most important effects of the information revolution for all realms: political, economic, social, and military. It means that power is migrating to small, nonstate actors who can organize into sprawling networks more readily than can traditionally hierarchical nation-state actors. It means that conflicts will increasingly be waged by "networks," rather than by "hierarchies." It means that whoever masters the network form stands to gain major advantages in the new epoch.[160]

Along with opening up strategic agency at the organisational and operational levels, technology also blurs conventional concepts for structuring cognitive understanding of the battlespace. Thus, offence and defence are blurred to the extent where it becomes "difficult to distinguish between attacking and defending actions."[161] Similar sorts of problems can be seen in the difficulty of determining who is undertaking the action and what their motivations for it are. Thus simple "hacking"[162] becomes conflated with cyber-crime and ultimately with Cyberwar itself as the only thing that distinguishes these activities from one another is the motivation

---

[158] Arquilla et al, *Cyberwar is Coming!* …, 27.
[159] Arquilla et al, *The Advent of Netwar* …, 13.
[160] Arquilla et al, *In Athena's Camp: Preparing for Conflict in the Information Age* …, 5.
[161] Arquilla et al, *The Advent of Netwar* …, 13.
[162] And here, we mean hacking in the sense that the term was originally used by programmers, as "an expert or enthusiast" that understands how a system works and how it can be manipulated to perform tasks. See Pekka Himanen, *The Hacker Ethic: A Radical Approach to the Philosophy of Business* (New York: Random House, 2009).

which lies behind it. This in turn complicates the ability of the state to respond to these actions. Arquilla and Ronfeldt argue:

> (nation state) sovereignty and authority are usually exercised through bureaucracies in which issues and problems can be sliced up and specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear. A protagonist is likely to operate in the cracks and gray areas of a society, striking where lines of authority crisscross and the operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash.[163]

Cyber Vulnerabilities with Integrated Military Hardware

Science-fiction writers and Revolutionaries are fascinated with the vulnerabilities that come with a society that is completely dependent on the information and services that support their basic existence. Less advanced adversaries need not look to direct military confrontation but indirect approaches that negate the technological advantages of superior military capabilities dependent on technology to be effective at war.[164] Furthermore, globalization of electronics manufacturing has opened the door to foreign interests to embed covert code or leave the hardware open to external commands/influence by adversarial groups or nations.[165] The majority of the electronic component fabrication occurs outside continental North America leaving the US [and Canadian] defence industry significantly vulnerable to cyber-attacks.[166]

Revolutionaries draw on visionary scenarios to articulate the impact of cyber vulnerabilities by considering futuristic "most dangerous" courses of action that lead to defeat of a force. One science-fiction scenario that captures the essence of potential cyber vulnerabilities

---

[163] J. Arquilla and D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime* (Rand Corporation, 2001), 14.

[164] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* …, 53.

[165] Sally Adee, "The Hunt for the Kill Switch," Spectrum, IEEE 45, no. 5 (2008): 34-39.

[166] Shalal, "Nearly every U.S. arms program found vulnerable to cyber attacks," …, http://www.reuters.com/article/2015/01/21/us-cybersecurity-pentagon-idUSKBN0KU02920150121.

involves the Borg from the television series *Star Trek: The Next Generation*. Despite the advantages posed by the interconnected nature of the Borg society, their highly integrated being becomes their greatest point of vulnerability. In the episode *The Best of Both Worlds: Part 2*, the crew of the Enterprise were able to defeat the more powerful Borg adversary by hacking into an unprotected portion of the Borg network and injecting a command that put all the Borg personnel to sleep. The Revolutionary lesson from this scenario is that legitimate system commands may be leveraged by hackers to neutralize a highly sophisticated weapon platform.

As mentioned in the introduction, the potential cyber vulnerability specific to the F-35 fighter aircraft lies in the Autonomic Logistics Information System (ALIS) and its control over aircraft functions.[167] The concerns/fears of defence officials relates to the potential that adversaries will find a way to compromise/exploit the F-35's ALIS and ground the plane or take control away from the pilot to operate the fighter aircraft. A Revolutionist scenario that envisioned similar cyber vulnerabilities in fighter aircraft occurred during the first episode of the 2003 *Battlestar Galactica* mini-series. In the episode, Cylon forces leverage an electronic jamming exploit during their assault to completely neutralize all the computer systems aboard their adversary's 7th generation Viper fighter spacecraft. In this scenario, the antiquated and lower tech military platforms operating with closed computer systems such as the Mark 2 Viper were immune from the cyber "kill switch"[168] vulnerability. Such Revolutionist scenarios highlight the potential for concern when employing sophisticated military hardware such as the 5th generation F-35.

[167] CyberWarZone, "New F-35 Fighter Jet is vulnerable to cyber-attacks," …, http://cyberwarzone.com/new-f-35-fighter-jet-vulnerable-cyber-attacks/.
[168] Adee, "The Hunt for the Kill Switch,"…,.

To the members of the Conservative School, referencing science-fiction to highlight the concept of a military cyber "kill switch" does not instill confidence that the concept has any merit. On the other hand, Revolutionaries are able to contemplate possible future outcomes in military affairs without mental restrictions. Conservatives may have doubted the possibility of a military cyber "kill switch" until the details of the 2007 Israeli Operation Orchard were made public.[169][170] During Operation Orchard, the Israeli Air Force performed airstrikes on a suspected nuclear reactor in Syria without alerting the Syrians to their location or triggering any air defence capabilities. The cyber significance of this operation relates to the Israeli Defence Forces' ability to completely suppress the Syrian air defences through cyber and not kinetic techniques. The Israeli Defence Forces employed airborne network attack technology to take control of the Syrian defence network and subsequently activate a secret "kill switch" that neutralized the system. The existence of a cyber "kill switch" for networked military capabilities is no longer the domain of Revolutionary visionaries but a cold hard threat for Conservatives to consider and Liberal Materialists to manage. The cyber "kill switch" is yet another example of a technological concept that was forecasted by revolutionary science-fiction several years before becoming reality in the public domain.

Conclusions

This chapter considered Revolutionary Materialist perspectives within the Cyber Warfare Schools of Thought schema. Revolutionary Materialists are forward looking visionaries that consider possible future outcomes to better understand the implications of

[169] Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," last modified 2 November 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

[170] John Leyden, "Israel suspected of 'hacking' Syrian air defences," last modified 4 October 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

technological changes on society. The Revolutionary approach considers the "most dangerous" trend of technological changes to better develop strategies and responses. While this approach raises the spectre of anarchy and relativism, it also frees individual decision makers from "dogmatic thinking", opening up new paths for creative problem solving. It is the basic belief of Revolutionaries that cyber technology has profoundly altered the praxis if not the nature of warfare. Influenced by luminary writers such as Author C. Clarke and Marshall McLuhan, Revolutionaries employ technologically influenced scenarios to articulate the complex concepts in relatable terms. Revolutionaries "prepare people to accept the future without pain and to encourage a flexibility of mind."[171]

The most materialists of the Schools of Thought schema, Revolutionaries focus on the affordances offered by cyber capabilities and the impact of technology on humanity. In terms of cyber warfare, Revolutionaries are maneuverist warfare advocates emphasizing the advantages of adopting irregular approaches to attacking adversaries' critical vulnerabilities. To Revolutionaries, cyberspace is the "new high ground" from which to exert strategic power. This new high ground also erodes classical hierarchies of control and offers strategic power to non-traditional non-state ideologically inspired groups with cyber exploitation skills. The most dangerous outcomes facing society are cyber skilled state and non-state actors launching paralyzing EPH's or "kill switch" exploitations on key capabilities.

With implications of humanity becoming fully integrated with technology to enhance humankind, the highly technologic agency of the Revolutionary School

[171] Jerome Agel, *The Making of Kubrick's 2001* (New American Library, 1970), 300.

professes profound changes to the conduct of warfare. Current discussions of cybernetic implants and lethal autonomous weapons offer a certain degree of credibility to the visionary epistemological approach to understanding the implications on humanity. Interestingly, bold Revolutionary visions eventually turn out to be humorously "conservative" as the products of invention and discovery become common place in society.

In the next chapter this paper will explore the fundamental characteristics of the Liberal Materialist School of Thought. Liberal Materialists represent the middle ground perspective on the School of Thought spectrum. Liberal Materialists also focus on materialism, but counterbalances that focus with a Conservative framework of human agency to control the effects of cyber warfare through the power of social institutions. This paper will explore how Liberal Materialists leverage pragmatic thought to balance historical and futuristic perspectives to more effectively deal with managing humanity's technologically based social issues and the implications on the praxis of warfare.

Liberalism is trust of the people tempered by prudence. Conservatism is distrust of the people tempered by fear.

- William E. Gladstone

CHAPTER 4 – THE LIBERAL MATERIALIST SCHOOL OF THOUGHT

In many ways, the Liberal Materialist School of Thought has been the least visible of the major divisions of reflection on cyber warfare. Liberals have published few manifestos on the issue of cyber warfare and generally have not attracted similar levels of attention.[172] This is because this School of Thought is the most expansive of the three, in that it devotes itself to the question of how information technology is shaping our society, as opposed to strictly confining itself to the issue of cyber warfare.[173] As such, the Liberal School is hidden within broader studies of internet governance, privacy, and the exploration of the social impact of computing technologies. Nevertheless, within these areas, specific consideration of cyber warfare is often present within these studies given the overlap of issue areas.

Like the Revolutionaries, Liberals share a thread of materialism in their thinking in that their writings emphasise how the technological context is opening up both opportunities and new dangers for individuals, organisations, and states. However, Liberal writing lacks the sensationalism and scenarios found in the revolutionary literature. As their name suggests,

---

[172] One exception to this rule has been the explorations of Ron Deibert and his CitizenLab at the University of Toronto. They have published several studies concerning internet censorship, privacy, and hacking that have been well publicized within the international media. While studies such as Ghostnet have not been explicitly about cyberwarfare, the implications of that study raise many important issues of computer security, the role of cyber-espionage, and the breach of privacy that resonate strongly within the area of cyberwarfare. See Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: Signal, 2013).

[173] Lawrence Lessig, "The Law of the Horse: What Cyberlaw might Teach," *Harvard Law Review* (1999): 501-549. See also Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press, 2006). See also Manuel Castells, *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*, Vol. 1 (John Wiley & Sons, 2011). See also Jonathan Zittrain, *The Future of the Internet--and how to Stop It* (Yale University Press, 2008). See also Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Toronto: Knopf, 2011).

Liberals emphasise the agency that accompanies the growth of information technology. This agency accrues to everything that IT touches, and so while individuals can take advantage of this, so too can states, non-governmental organisations, and even other forms of technology. However, Liberals have little faith that this evolution in technology necessarily points towards classic "liberal"[174] ends or results. Indeed, many argue that without effective state intervention, the results might be decidedly poor for society. Others, point to new forms of policy engagement between the state and other actors in mediating these new opportunities. As such, Liberals share with the Revolutionaries that technology is changing society; however, their approach is more evolutionary than revolutionary. There is still space for the state to act in this novel environment, and not all institutions are to be swept away.

Liberal Issues

The Liberal School shares a heavy materialist focus, like the Revolutionary School. This materialism, however, is tempered by very typical liberal emphasis on issues of freedom, individuality, and institutional development. Amongst Liberals, however, there is little confidence that IT's effect on society will be anything but liberal. As such, there is an equally liberal emphasis on activism and engagement in order to shape technological developments in open-minded and humane directions.

Technology has a critical role in shaping society, according to the Liberal School. Significant changes in how society in general, and international society in specific, is organised stem from the global nature of contemporary digital communication technology. Because these

[174] Liberal as a derivative of liberalism - The belief in the value of social and political change in order to achieve progress. - Merriam-Webster, "liberalism," last accessed 01 May 2015, http://www.merriam-webster.com/dictionary/liberalism.

technologies and the companies that provide communication services cross international jurisdiction, efforts to impose controls on them are inherently costly and complex. This is magnified by the growing scale of the communication facilitated by this rapidly evolving technology and the distribution of decision making beyond that of political units. All of this has required new institutions such as ICANN (Internet Corporation for Assigned Names and Numbers) and the IETF (Internet Engineering Task Force) in order to manage the constellations of technologies, service providers, civic society groups, and states.[175]

As many writers point out, in function, many of these developments are nothing new.[176] What may be new in these developments is the reflexive change they cause in the interactions between technological advance and human affairs. Digital communications are eminently flexible in their tendency to be repurposed and re-appropriated by communities of interest outside the original design parameters. These successes build upon one another in a manner which ultimately directs the technology into areas not originally anticipated by the designer. As Dan Kuehl remarks:

> It is the inseparable linkage of the technology, the human users, and the impact of the interconnectivity in the modern world that differentiates these kinds of information networks from earlier ones—such as the Pony Express of the 1860s—and that hints at cyberspace's future impact.[177]

This interaction has produced clashes between the new capabilities offered by technology and the interests of states in particular. Mueller breaks these conflicts into four areas: intellectual

---

[175] Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Mit Press, 2010), 5. See also Milton Mueller and Brenden Kuerbis, "Towards Global Internet Governance: How to End US Control of ICANN without Sacrificing Stability, Freedom Or Accountability," In *2014 TPRC Conference Paper*. (2014).

[176] Mosco, "The Digital Sublime,"…: 1. See also Wu, *The Master Switch: The Rise and Fall of Information Empires…*, 37. See also James Gleick, "Cyber-Neologoliferation," *The New York Times Magazine 5* (2006): 6.

[177] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security* (2009): 31.

property protection, cyber security, content regulation (concerning pornography, especially that related to pedophilia), and critical internet resources (the technical security of those resources). These issues raise clear questions of cross border jurisdiction and governance capacity. As Mueller remarks:

> There is a family resemblance across each of these domains observable in the acute conflict between the capabilities of open global networking and the problem of maintaining boundaries and control. This conflict can only be resolved through changes in the existing institutions governing communication and information.[178]

Many of the challenges posed by digital communications technology, however, have little to do with conflict between states and emerging non-state institutions. Some of the most creative vectors within cyberspace arise from criminal activity, which Diebert and Rohozinski remind us is also a form of liberation, often seeking to transcend local limitations stemming from poverty or political inequality.[179] In both cases, however, the interest of the Liberal School of Thought is to "uphold the Internet as a forum of free expression and access to information…."[180] The objectives of this project is a "shared agenda of communications security and privacy, freedom of expression, equal access, the protection of an open public domain of knowledge, and the preservation of cultural diversity."[181]

Materialism in the Liberal School

---

[178] Mueller, *Networks and States: The Global Politics of Internet Governance* …, 6.

[179] Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy* 21, no. 4 (2010): 48.

[180] Ronald J. Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," *Access Denied: The Practice and Policy of Global Internet Filtering*, Ed.Ronald J.Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008) (2008): 127.

[181] Deibert et al, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet,"…: 127-128.

While the goals of the Liberal School are essentially humane in nature, human activity is not necessarily the only or even the most important influence on the behaviour of this medium. As Deibert and Rohozinski note, the physical structure of cyberspace "shape and limit notions of security and risk… the technical character of cyberspace itself are restrictive factors that shape the realm of the possible in ways that discourse alone cannot explain."[182] The spread of computers into most aspects of contemporary life has a technological basis which Manuel Castells refers to as "informationalism."[183] Castells argues that informationalism forms the technological basis on which all of the possibilities of the information age are built, composed of the effects of the falling cost and rising power of microprocessors (Moore's Law), the combinatorial effect of networking (Metcalfe's Law), and the essential mutability of digital information which allows it to be effortlessly combined in new ways to produce new applications, services, and information.[184] Dorothy Denning observes that the consequence of computers in every aspect of our lives is the increasing accessibility of information. The significance of this access cannot be accurately determined given the mutability of that information. However, Denning argues that these increased opportunities to access and manipulate information cannot lead to anything other than an equally increasing opportunity to conduct information warfare.[185] Kuehl argues that the technological basis of cyberspace is changing how one creates information content, how one shares that content, and ultimately, how

[182] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 18. See also Martin C. Libicki, "Global Networks and Security: How Dark is the Dark Side?" *The Global Century: Globalization and National Security* (2001): 816. See also See Chapter 1"Code is Law." - Lawrence Lessig, Code (Lawrence Lessig, 2006), 1-8.

[183] Manuel Castells, *The Network Society: A Cross-cultural Perspective* (Northampton, MA: Edward Elgar Publishing, Inc., 1996), 7.

[184] Castells, *The Network Society: A Cross-cultural Perspective*…, 7.

[185] Denning, *Information Warfare and Security*…, 15.

humans will interact with one another in the future.[186] Finally, Deibert and Rohozinski point out that the technological basis of cyberspace will shape the character of conflict that takes place within that domain.[187] Thus, there is a clear prerogative to control the physical infrastructure in order to effectively control the information that flows over its sinews; there will be considerable importance at both the strategic and tactical levels for denying information to opponents; the distributed nature of the medium will incite both outsourcing or "privateering" as well as globalising any conflict; finally the complex nature of the medium will both create and magnify unanticipated outcomes stemming from cyber conflict.[188]

Given the cross cutting nature of issues arising from the governance of the internet, it will not only be a resource for those in conflict, but also a contested space itself.[189] Mueller's four issue areas listed above (intellectual property protection, cyber security, content regulation and critical internet resources) are all ones over the scope of freedom versus the need to regulate content, behaviour, and access. However, Deibert and Rohozinski caution against simplifying all conflict over the internet to a simple binary of liberation versus control. As they note, both "liberation" and "control" are socially constructed ideas the meaning of which varies considerably depending on the political and social context in which they are discussed. Furthermore, not only are the social forces very dynamic, the technological context in which they are deployed is itself constantly changing from moment to moment, making "any portrayal of

[186] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem,"…: 32-33.
[187] Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 4.
[188] Deibert et al, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War,"…: 5-6
[189] Mueller, *Networks and States: The Global Politics of Internet Governance* …, 12.

technology that highlights a single overarching characteristic biases towards either liberation or control seem fanciful."[190]

As such, while the Liberal School points to the critical role of technology in shaping this medium, it is equally insistent that there are no technical fixes to be had in resolving these problems. There are technical problems inherent in the distributed nature of digital technologies and those who deploy and control them, and its inherent mutable and multifunctional nature makes it innately creative to the whims of those who use it. On top of these fundamental issues, there is the equally intrinsic problem of human conflict in general. Just as the problem of crime has historically resisted "solution" irrespective of the nature of political organisation, one should not expect that the extension of traditional human conflict to cyberspace will be any more resolvable than it has been in physical space.[191] At its heart, cyberspace and its security is a multifaceted social problem built on a strong technological foundation.

Agency, Human or Otherwise, in Cyberspace

The limitations of a strict materialist approach to cyberspace is evident when one considers that conflict within cyberspace is not about the technology itself, but how it is used by political actors. Kuehl links cyber warfare to earlier forms of conflict by contrasting naval and air warfare with it. Kuehl states:

> A materially based view is clearly inappropriate because the issue is not controlling electrons or electromagnetic forces, but rather influencing the use of cyberspace in the same way that air or naval superiority is not about controlling molecules of air or water but rather controlling how the physical domain is used. It is a measure of effect of impact on human affairs and processes.[192]

[190] Deibert et al, "Liberation vs. Control: The Future of Cyberspace,"…: 44.
[191] Mueller, *Networks and States: The Global Politics of Internet Governance* …, 162-163.
[192] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem,"…: 37.

Deibert and Rohozinski also compare cyberspace to other military domains, but add that while the technological context constrains human use of it, unlike sea, air, land, and space, cyberspace is dependent upon human intervention in order to keep it functioning. As such, the actions of human agency affect its very constitution.[193] However, elsewhere they argue that "communication technologies are neither empty vessels to be filled with products of human intent, nor forces unto themselves imbued with some kind of irresistible agency." Rather, they are the manifestation of dynamic and evolving social forces, which when introduced, reflexively shape and direct the manner in which they will be used, but are also subject to the forces of contingency, innovation, and repurposing.[194] In sum, human society, individual creativity, commercial interests, and technological affordances all combine together in a complex mix of influences and social dynamics to produce cyberspace. As Carl H. Builder puts it, "[n]ot all may seek or elect to exploit the emerging abundance of information, but it is there for the taking, and the power it conveys depends only on the creativity, imagination, and boldness of the individual."[195] Thus power is there to those who are able to create and use it but it is "a tangled web of rival public and private authorities, civic associations, criminal networks and underground economies,"[196] as well as contingencies arising from repurposed technologies and commercial decisions that become political.[197]

Distribution of Power

[193] Deibert et al, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War,"…: 2.
[194] Deibert et al, "Liberation vs. Control: The Future of Cyberspace,"…: 44.
[195] Arquilla et al, *In Athena's Camp: Preparing for Conflict in the Information Age* …, 95.
[196] Deibert et al, "Liberation vs. Control: The Future of Cyberspace,"…: 46.
[197] Deibert et al, "Liberation vs. Control: The Future of Cyberspace,"…: 45.

Notably then, the Liberal School places particular emphasis on the distribution of power that is being caused by digital technologies. This distributive feature is located in a variety of sources. The very nature of the contemporary communication sector facilitates much of this distributive element. For Mueller, it is located in the increasingly privatised nature of internet governance, which is a structural response to the limitations of governments to provide for it. Four aspects dominate this march of privatisation. The scale of the internet means that no one person or body can possess complete knowledge of the overall system. Thus, local network operators are best positioned to manage the volume of activity. The rapid advance of technology makes it difficult for the rationalised bureaucracies of modern states to keep pace in terms of both human and capital resources. Again, those with specialised technological know-how are best positioned to provide advice on the implementation of technologies and management policies. Further, the same rationalised jurisdictions of government bureaucracies makes them poor actors in a policy arena where the issues cross all manner of jurisdictional and policy boundaries. Finally, governments are bound by codes of conduct which private actors are not, thus making them perfect proxies to accomplish what governments otherwise cannot.[198]

Another effect of the increasing computerisation of contemporary society is the growth in pure data that is being stored by all manner of applications. This is easily seen in the commonality of gigabyte sized storage devices and the arrival of terabyte sized ones in increasing numbers. This challenge demands increasing sophistication in information processing.[199] Studies conducted Martin Hilbert at the University of Southern California's Annenberg School for Communications and Journalism calculated in 2007 there existed over 300

[198] Mueller, *Networks and States: The Global Politics of Internet Governance* …, 211. See also Deibert et al, "Risking Security: Policies and Paradoxes of Cyberspace Security," …: 16.

[199] Robert Latham and Saskia Sassen, *Digital Formations: IT and New Architectures in the Global Realm* (Princeton University Press, 2009), 13.

exabytes[200] of stored data, of which 7% of the data was non-digitized book, etc.[201] Hilbert further estimates that stored information worldwide in 2013 to be approximately 1200 exabytes with less than 2% of that figure to be non-digital. "The amount of stored information grows four times faster than the world economy, while the processing power of computers grows nine times faster."[202]

Military organizations are also not adverse to the challenges presented by "big data" and the sheer volume of data and information that must be effectively filtered and analysed in the conduct modern day operations. In 2008, the CAF *Concept of Fusion* paper remarked:

> In order to conduct effective military operations, commanders and respective staffs continually need to understand and accurately predict changes in their battle-space. This means military decision makers need to be able to perceive their environment or battle-space, comprehend their environment, and make projections about the changes that will take place in their environment in order to achieve Situation Awareness (SA). The fundamental challenge facing military decision makers is the selective absorption of pertinent information from numerous and complex sources to efficiently achieve comprehensive SA. [203]

The CAF concept of "fusion" proposed the creation of an automated service by which volumes of "various sources and types of information can be combined to enable commanders and staffs to generate a more informed, coherent "view" of operational activities that supports their decision-making process."[204] The sought algorithm/service to enable information fusion would employ big data predictive techniques to propose which sources of information where pertinent for commanders and staffs to develop more profound knowledge and understanding of a particular situation as it unfolds. The "dark side" of such a service relates to the human

---

[200] One Exabyte is $1x10^{18}$ bytes or 1 billion Gigabytes.
[201] Mayer-Schönberger et al, *Big Data: A Revolution* …, 20.
[202] Mayer-Schönberger et al, *Big Data: A Revolution* …, 20.
[203] Paul Martin, Jim Hutton and Loren Klimchuck, *CF Concept of Fusion* (Department of National Defence/Canadian Forces, 07 Aug 08), 1.
[204] Martin et al, *CF Concept of Fusion* …, 1.

confidence placed in the sophisticated automated/artificial "intelligence" to determine what information is pertinent to military operations. The dark tendency would be for commanders and staffs to not develop a profound knowledge of the situation but rather rely explicitly on computer based advice to make potentially lethal decisions. Liberal Materialists must concern themselves with the regulation of automated influence in the development of military advice to ensure that lethal force is not applied solely on the basis of automated mathematical "probabilistic cause."[205]

Scott Knight is another member of the Liberal Materialist School that advises on cyber issues as they relate to military activities. In one of his works, *War by Computer: Canadian Cyber Forces in 2025*, Knight acknowledges the need for policy and capabilities in the rapidly evolving cyber domain to protect citizens and military forces from their dependence on information technologies.[206] Knight argues that managing and protecting against cyber threats from an institutional perspective requires more capability than just purchasing the latest commercial security solution. Cyber defences will require a targeted strategy of defence that includes a militarized cadre of skilled cyber forces.[207] Knight admits that commercial intrusion detection systems and anti-virus software is adequate for defending against adversaries employing broad based attack techniques (indiscriminately attacking everyone) but does little against those adversaries that are specifically targeting the institution. Knight states:

> The most dangerous kinds of adversaries are those who are targeting us specifically. By definition these adversaries are willing to expend the resources, and take the risks, involved in gaining access to our information systems. These are foreign intelligence services, military adversaries, and others, and are our most dangerous opponents.[208]

---

[205] Mayer-Schönberger et al, *Big Data: A Revolution* …, 28.
[206] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 74
[207] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 75.
[208] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 75.

A solid member of the Liberal Materialist camp, Knight is concerned about institutionally defending against dangerous cyber adversaries that possess the funding, the manpower and the access to commercial products to develop techniques and capabilities that will defeat standard commercial off-the-shelf perimeter defences.[209] In addition to developing exploits to counter institutional "server-side" perimeter defences that protect against external attacks, adversaries are also investigating alternate attack vectors suck as "client-side" exploits. The "client-side" approach attempts to exploit more vulnerable software resident inside the institutional protective perimeter by introducing malicious code at a client computer. Previously, it was felt that if classified computers or command networks were "air-gapped" and isolated from other networks or the Internet it was safe from attack. "Client-side" attack vectors employ various forms of exploits that can be introduced with removable media across "air-gapped" systems. Knight introduces the concept of "information flows" as the transfer of information [bidirectional or uni-directional] from one system to another by way of removable media, data diodes, etc.[210] Once an adversary can identify an "information flow" it can be exploited as a system vulnerability. "Air-gapped" classified computers and command networks are no longer safe from malicious codes exploiting an "information flow" and defeating the protection of stand-alone isolation.[211]

In terms of a "client-side" attack of a network connected to the Internet, the malicious code can introduced through some benign method such as USB stick, mail attachment, or a compromised web page. Once the code has been deployed on the unsuspecting system it will attempt to covertly communicate back to an adversarial individual or group through by way of an

[209] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 76.
[210] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 77.
[211] Geoffrey Ingersoll, "US NAVY: Hackers 'Jumping The Air Gap' Would 'Disrupt The World Balance Of Power'," *Business Insider*, last modified 19 November 2013, http://www.businessinsider.com/navy-acoustic-hackers-could-halt-fleets-2013-11.

"information flow." The malicious communication or "covert channel"[212] will attempt to hide within the regular activity of the system or network to avoid detection by system security capabilities. Knight explains that covert channels can establish a back-door communication path with an attacker that can defeat traditional outward facing firewall and perimeter defences.[213]

Knight also highlights that critical mission systems onboard warships, aircraft and air defence systems are just as vulnerable to cyber-attack.[214] The "credential stealing" virus infection of US Predator and Reaper drone fleets is but one example of a weapon system falling victim to an adversarial cyber-attack.[215] There are growing concerns as to the increased vulnerability of sophisticated US weapons systems in light of the known losses of advanced systems designs to Chinese sponsored espionage.[216] Publicly, the Pentagon remains confident in their warfighting capabilities despite the compromises of key weapons programs such as the Patriot missile system as well as the F-22 and F-35 fighter aircraft. "Suggestions that cyber intrusions have somehow led to the erosion of our capabilities or technological edge are incorrect."[217] Nevertheless, "highly connected" warfare strategies that increase the cyber

---

[212] "Covert channels are unexpected and hidden communication paths embedded within a communication system that violates the system security policy. Covert communication occurs when a user or application deliberately manipulates and embeds information into some property of a communication system in such a way that the embedded information is not apparent to the legitimate users of the communication system. Internet based covert channels with low bit rates are enough to convey critical information such as network encryption keys or system access codes." - Paul E.C. Martin, "Covert Channels In Secure Wireless Networks" (master's thesis, Royal Military College of Canada, 2007, v.

[213] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 77.

[214] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 79.

[215] Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet," ..., http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/. See also Shachtman, "Military 'Not Quite Sure' How Drone Cockpits Got Infected,"..., http://www.wired.com/2011/10/military-not-quite-sure-how-drone-cockpits-got-infected/. See also Alex Knapp, "America's Drones Have Been Infected by a Virus," *Forbes*, last modified 10 August 2011, http://www.forbes.com/sites/alexknapp/2011/10/08/americas-drones-have-been-infected-by-a-virus/.

[216] Sky News, "China Cyberattack: US Weapons Systems Breached," last modified 29 May 2013, http://news.sky.com/story/1096826/china-cyberattack-us-weapons-systems-breached.

[217] Pentagon Press Secretary George Little quoted in Sky News, "China Cyberattack: US Weapons Systems Breached," …, http://news.sky.com/story/1096826/china-cyberattack-us-weapons-systems-breached.

integration of military capabilities also increase the exposure of these capabilities to cyber-attack and exploitation.[218]

In addition to state sponsored cyber warfare, many Liberal writers share similar concerns with the Revolutionaries Arquilla and Ronfeldt with respect to non-state actors. Like their concept of Netwar, Liberals discuss how non-state actors, both civil and otherwise, are emerging based on the distributive properties of digital technology. Civic networks were the earliest of adopters for social technologies, in terms of both producing communities of interest and practice, as well as in generating financial support. These civic networks are complemented by so called "Dark nets" made up of militant groups, extremists, criminal organisations, and terrorists. Deibert and Rohozinski divide these up into "armed social movements" (Al Qaeda, Hezbollah, Chechen guerrilla organisations) and transnational criminal organisations.[219] The new organisational arrangements prompted by these developments themselves raise novel political issues and governance problems that generate institutional change at the transnational level. The challenges arising from cyberspace involve highly scalable and difficult to trace actions and distributed actors that exceed the ability of the state to control them. This has prompted new organisational arrangements that are beginning to reconstitute relationships between business, government, and civil society. However, these new arrangements are themselves problematic in terms of governance and politics. Mueller argues that society is not seeing a reassertion of the state, but rather its gradual adaptation to these new circumstances.[220] Yet new forms of organisation will only enable new forms of collaboration, not provide actual answers to the questions raised by this new distribution of power: who decides, how power to be authoritatively

[218] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 79.
[219] Deibert et al, "Risking Security: Policies and Paradoxes of Cyberspace Security," …: 21-24. See also Deibert et al, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet,"…: 130.
[220] Mueller, *Networks and States: The Global Politics of Internet Governance* …, 182-183.

distributed is, what rights accrue to which actors, and how is conflict to be resolved. While the state's power has been eroded by digital technology, its role in settling these issues remains paramount.

The Role of the State

The Liberal Materialist School of Thought views the role of the state as the foundation for managing and controlling cyber capabilities in order to protect society from ongoing cyber threats. Liberal Materialists recognize the paradox created by the permeation of cyber technology into the functioning and sustainment of society. On one hand, cyber capabilities offer society effective and efficient opportunities for goods and services as well as opportunities for the sharing of ideas and information. While on the other hand, cyber capabilities offer governments, militaries, state-based and non-state actors a powerful new means to exert strategic force that is challenging to defend against if not impossible to deter.[221] US National Security Strategy also acknowledges the paradoxical situation stating: "The very technologies that empower us to lead and create also empower those who would disrupt and destroy."[222] In the eyes of the Liberal School, the state is responsible to formulate a national cyber strategy and exert cyber-power "to support the attainment of larger objectives … across the elements of national power – political, diplomatic, informational, military and economic."[223] The development of a

[221] David Betz, Tim Stevens and International Institute for Strategic Studies, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (New York: Routledge, for the International Institute for Strategic Studies, 2011), 10.

[222] United States. Executive Office of the President of the United States, *National Security Strategy of the United States, May 2010* (Washington, DC: U.S. Government Printing Office, 2010), 27.

[223] Betz et al, *Cyberspace and the State: Toward a Strategy for Cyber-Power*…, 44.

national cyber strategy requires the state to effectively balance its ends, ways and means to adequately address national cyber-defence and cyber-security threats.[224]

In terms of balancing the ends, ways, and means of national strategy the state must consider national goals that impact domestic as well as international perceptions with respect to the contribution to cyber peace and security.[225] For example, Canadian cyber strategy is comprised of three primary objectives: "Securing Government Systems, Partnering to secure vital cyber systems outside the federal Government, [and] Helping Canadians to be secure online."[226] The role of DND and CAF as a derivative of the national cyber strategy is to protect defence infrastructure, identify threats and possible responses and maintain cyber defence relationships with allied militaries.[227] Ron Deibert views Canada's cyber strategy to be rather "thin" in terms of national commitment and overall detail.[228] Deibert argues that governments need to be more aware and active in countering the social forces currently undermining the openness of cyberspace with "assertions of state power, interstate competition, espionage, crime and warfare."[229] As a means to combat the forces that threaten cyberspace (cyber warfare), governments may leverage capabilities and services to conduct state sponsored surveillance, censorship and information warfare.[230]

---

[224] Daniel Ventre, *Cyber Conflict: Competing National Perspectives* (John Wiley & Sons, 2013), 297.

[225] Ventre, *Cyber Conflict: Competing National Perspectives*…, 298.

[226] Department of Public Safety, *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (Ottawa: Canada Communication Group, 2015), 1.

[227] Department of Public Safety, *Canada's Cyber Security Strategy* (Ottawa: Canada Communication Group, 2010), 10.

[228] Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," *Journal of Military and Strategic Studies* 14, no. 2 (2012): 2.

[229] Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," ...: 23..

[230] Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," ...: 23.

Some Liberal Materialists argue national cyber strategy should include both elements of preemption and deterrence. [231] In an article published in The *Washington Post*, Mike McConnell makes the case that depending on the threat facing the US; it should be able to employ both preemption and deterrence to defend its interests.[232] Following in McConnell's train of thought, other Liberal Materialists believe that "the laws of armed conflict can be widened to embrace Cyber Warfare in order to allow the US to respond with the use of force against aggressive assaults on its computer and IT infrastructure."[233] Classifying a cyber-attack as an act of war allows the state to use both cyber and kinetic response capabilities as coercive means of deterrence. The 2015 US National Security leaves the door open to all available state response capabilities stating:

> On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government.[234]

The Liberal Materialist School being the middle ground between Conservatives and Revolutionaries employ elements of both Schools to manage cyber warfare issues. In the case of military responses to cyber-attacks, Liberal Materialists acknowledge cyber activities have political and ontological significance and look to established Conservative frameworks of control to manage behavior and deter inappropriate activity. In the case of national cyber-defence strategy, strategic thinking Liberal Materialists are investigating

---

[231] Mike McConnell. "Mike McConnell on how to Win the Cyber-War We're Losing," *Washington Post*, 28 February 2010, last accessed 02 May 2015, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[232] McConnell. "Mike McConnell on how to Win the Cyber-War We're Losing," ..., http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[233] Ed Pilkington, "Washington moves to classify cyber-attacks as acts of war," *TheGuardian*, last modified 31 May 2011, http://www.theguardian.com/world/2011/may/31/washington-moves-to-classify-cyber-attacks.

[234] Executive Office of the President of the United States, *National Security Strategy 2015* (Washington, DC: U.S. Government Printing Office, 2015), 24.

aspects of *jus ad bellum* or "the rules that regulate the use of armed force by states in their international relations."[235] Article 51 of Chapter VII to the United Nations Charter dealing with Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression states:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[236]

But invoking *jus ad bellum* in response to malicious cyber activity is problematic due to well-known challenges of action attribution and actor identification.[237] There exists a legal obligation to identify the perpetrator of a cyber-incident as well as verify it did not occur accidentally.[238] Therefore the major issue with justifying action based on cyber-attack self-defence is the proof linking aggressor with action.[239]

In response to Liberal Materialists concerns about the unmanageable characteristics and architecture of the Internet, some senior US government officials have proposed constructing a more secure and protected enclave within the "supposed lawless

---

[235] Marco Roscini, "World Wide Warfare-'Jus Ad Bellum' and the use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 88.

[236] United Nations, "CHAPTER VII: ACTION WITH RESPECT TO THREATS TO THE PEACE, BREACHES OF THE PEACE, AND ACTS OF AGGRESSION," last accessed 01 May 2015 , http://www.un.org/en/documents/charter/chapter7.shtml.

[237] Roscini, "World Wide Warfare-'Jus Ad Bellum' and the use of Cyber Force,"…: 88.

[238] Roscini, "World Wide Warfare-'Jus Ad Bellum' and the use of Cyber Force,"…: 119..

[239] Roscini, "World Wide Warfare-'Jus Ad Bellum' and the use of Cyber Force,"…: 119.

Wild West of the Internet."[240] While others suggest the Internet should be reengineered to ensure geolocation and attribution are inherent in the Internet's architecture as a means of deterrence.[241] Unfortunately, the idea of redesigning the Internet and starting afresh is an extremely costly proposal that does not guarantee success in achieving specific security goals.[242] Furthermore, there are mounting concerns with the political leadership militarizing cyberspace and seeking to create their own "cyber Manhattan Project to build weapons" instead of pursuing collaborative security through alliances and partnerships to resolve international and interrelated cyber issues.[243]

One collaborative step toward security and civility would entail the creation of an international Cyberspace Treaty as an extension of the Laws of Armed Conflict. The likelihood of misinterpreted actions potentially leading to conflict is increased in the absence of any international agreements establishing the standards of cyber conduct and what constitutes armed attack in cyberspace.[244] Such a treaty would also pave the way for a universal application of constabulary functions by police forces to control nefarious activity.[245]

Alison Lawlor Russell in her book *Cyber Blockades* extends the traditional Laws of Armed Conflict relating to physical blockades to a state sponsored activity in

---

[240] P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 167.

[241] McConnell. "Mike McConnell on how to Win the Cyber-War We're Losing," ..., http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[242] Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* …, 175.

[243] Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* …, 175.

[244] Benjamin Mueller, "The Laws of War and Cyberspace on the Need for a Treaty Concerning Cyber Conflict," (2014): 16.

[245] Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* …, 185-193.

cyberspace. Based on the alleged Russian cyber-attacks on Estonia in 2007[246] and on Georgia in 2008 [247], Russell explores the implications of state sponsored applications of cyber force as a means of national power to "shut down, close off, or otherwise render cyberspace useless for an entire country."[248] Traditionally regarded as acts of war, blockades in cyberspace represent an expedient, low cost method to punish an adversary through denial of services connected to the Internet. In addition, depending on the context of application, cyber blockades may not always represent an act of war due to the passive nature of the act.[249] Interfering with state sovereignty and the freedom of action within its own territory, cyber blockades represent a potentially strong coercive measure short of war. Nevertheless, Cyber blockades at present are a significant challenge for Liberal Materialists to manage in the absence of an international cyber-treaty or codification into international law.

Finally, the role of the state from the perspective of Liberal Materialists involves commitment and resources to respond to growing cyber-defence and cyber-security issues. Governments need to invest in not only technology but human capital.[250] Misha Glenny argues a similar point in her book *DarkMarket: How Hackers Became the New Mafia*: "Computers and networks will never be safe if they are not protected by advanced hackers."[251] Knight makes the same case for the CAF of the future by calling for the creation and development of highly educated cadre of skilled cyber forces to complement

---

[246] Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 75-78.
[247] Russell, *Cyber Blockades* …, 103.
[248] Russell, *Cyber Blockades* …, 5.
[249] Russell, *Cyber Blockades* …, 145.
[250] William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (2010): 5.
[251] Misha Glenny, *DarkMarket: How Hackers Became the New Mafia*Random House, 2012)., 271.

existing automated defences.[252] Investment in developing human cyber expertise is also a tenant of the US military's cyber strategy to establish the organizational and training framework to generate and employ cyber forces in an active and layered capacity.[253] Unfortunately, Liberal Materialists must contend with the challenges of competing national imperatives in order to secure the required resources for an effective cyber-defence strategy.

Conclusions

This chapter considered Liberal Materialist perspectives within the Cyber Warfare Schools of Thought schema. The most expansive of the three Schools of Thought, Liberal Materialists are devoted to managing and controlling how information technology is shaping our society. The issues relating to cyber warfare are just a derivative of the broader social scope concerning the Liberal Materialist School. Liberals fully accept that technology is changing society, but view technological changes as more evolutionary than revolutionary in nature. Liberals have little faith in IT's impact on society and believe that technology must be governed if humanity is to positively evolve with technologic discoveries and advances. In terms of cyber, Liberals attempt to balance the desire for net neutrality with required controls to ensure appropriate use and conduct. Liberals approach the impact of cyber activities on society with guarded prudence instead of succumbing to the Conservative fears of the unknown.

To shape the character of conflict in cyberspace, Liberals must control not only the physical infrastructure supporting cyber but consider potential actions that could deny

[252] Knight, "War by Computer: Canadian Cyber Forces in 2025," …: 74.
[253] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," ...: 6.

an adversary access to information or deny freedom of action with the domain. Cyber Warfare represents a wicked problem for Liberals to solve as the globalizing nature of cyber invites a host of additional non-traditional actors to aggravate and amplify unanticipated strategic outcomes. Technology is a critical factor in shaping cyberspace, but the resolution to the problem of protection, control and governance is a social challenge. Governments and states are bound by international law while non-state or private actors act with little worry of prosecution. With issues of attribution and identification plaguing cyberspace, private actors make perfect proxies for state sanctioned cyber warfare.

Warfare strategies that increase the cyber integration of military capabilities also increase the exposure of these capabilities to cyber-attack and exploitation. Liberals must be prudent and practical in their approach to ensuring traditional warfare means enhanced with highly integrated cyber capabilities are not compromised in time of need. Knowing that “air-gapped” classified and command and control systems are vulnerable to client side attacks despite commercial security products, Liberal strategies must include the investment of human capital to develop and leverage the necessary skills to ensure governments can adequately protect its citizens and their interests in time of conflict.

Liberal Materialists view the state as the foundational element in protecting society from cyberspace threats. Liberals must contend with the paradoxical nature of cyber capabilities on society. Cyber capabilities are powerful tools that can also be abused to disrupt or potentially destroy. Governments need to adopt a Liberal Materialist approach in order to more effectively balance the ends, ways and means of national power to adequately address cyber security threats on behalf of its citizens. Given the

effects of globalization and the interconnected nature of cyber on international relations, Liberal Materialists must influence states and governments to collaborate internationally to enhance the existing framework of international law, including the Law of Armed Conflict, to include cyber activities. Cyber warfare need not be conducted in the shadows but be officially recognized as a means of national power that can be managed and controlled.

In the next and final chapter, this paper will explore the key points extracted from the application of the Cyber Warfare Schools of Thought schema on the survey of available literature and consider how an institution may approach bridging the epistemological/ontological divide. In addition, the Conclusion chapter will articulate some thoughts and recommendations for CAF leadership facing the challenges of operating forces integrated with the cyber environment in the execution of defence activities and the need for epistemological normalization to effectively bridge the divide.

CHAPTER 5 – CONCLUSION

At the close of this discussion of the different Cyber Warfare Schools of Thought, the essential questions that began this inquiry remain unanswered: What is to be done? What course of action should militaries and governments follow? Has the proposed schema of "Cyber Warfare Schools of Thought" bridged the epistemological/ontological divide? Completing a survey of cyber literature and subsequently categorizing the different points of view, it becomes obvious that there is a basic lack of agreement on the nature of the threat posed by information technology to the security of states, organisations, or individuals. Each School has its own tensions and contradictions in addressing the social problem of technologic influence. Approaching the social problem with dissimilar cognitive lenses, the different Schools interpret the social problem uniquely and subsequently derive distinctive social explanations to each of the unique problems. In essence, there is an epistemological divide which prevents a fundamental assessment on the ontological meaning of cyber events for the consideration of long term security issues.

Revolutionaries often pose the "most dangerous" apocalyptic scenarios or herald occurrences of technology-led RMAs that easily catch the attention of politicians, journalists, and worry warts of every description. However, the absence of an EPH as yet, the failure of extant information attacks to pose any sort of wider threat aside from nuisance value, and the difficulty in measuring the effect of compromised information due to subversion, espionage, and sabotage all suggest the problematic nature of some of this School's predictions. In his book *Strategy for Chaos*, Colin S. Gary also takes a dim view of agents professing such revolutionary promotion remarking, "… RMA advocacy literature can be linked to monkeys making chess

moves and parrots repeating clever phrases. The monkeys and parrots may well perform accurately, but they will not understand the meaning of what they are doing."[254] Furthermore, the assumption of widespread social chaos seems ahistorical in nature and may be reflective of broader philosophical assumptions and biases unrelated to the issue of warfare. In the experience of the Second World War, the use of air power failed to achieve the results that were predicted of it by earlier air power theorists such as Giulio Douhet. In the case of both Britain and Germany, the populations did not protest, riot or demand a cessation of hostilities in the face of aerial bombardment. While the use of nuclear weapons seems to have confirmed the predictions of air power theorists, there was considerable debate within the Japanese leadership on whether to surrender based on imperial strategic considerations and not due to the atomic bomb's influence on Japanese society. The recent events in Japan following the tsunami and nuclear meltdowns at Fukushima in 2011 did not result in widespread panic. Furthermore, the power outages associated with the ice storm in 1998 and the North American blackout during the summer of 2003 did not lead to widespread chaos, despite the length of time both events took to be resolved. Nor do Revolutionaries provide any psychological or social theory to justify their assumption that the effects of an EPH or Digital 9/11 would lead to the widespread social chaos that their scenarios describe. All of these suggest problems with the "most dangerous" assumptions made by Revolutionaries.

The Liberal School of Thought seems more pragmatic and eminently more reasonable. It describes conditions which are clearly visible in everyday life in terms of its assessment of technological change. The disruptive effects of compromised cyber capabilities on industries

---

[254] Gray, *Strategy for Chaos: Revolutions in Military Affairs …*, 280.

such as SONY Studios in 2014 are easily visible even to those not familiar with academic debates. Nevertheless, Liberals must contend with several securitization actors that play on society's fears of the unknown and attempt to prejudice the pragmatic threat assessments of the Liberal School. Special interest groups such as lobbyists and corporations are often accused of leveraging their influence for commercial gain. Lobbyists and corporations that promote unnecessary defence spending and place corporate gains ahead of public welfares are commonly referred to as a "military-industrial complex." Touting the advantages of offensive over defensive cyber warfare capabilities, special interests advancing cyber warfare agendas now represent a new cyber military-industrial complex. Feasting on a climate of fear and insecurity of the unknown cyber threat, the cyber military-industrial complex has been increasingly successful at proliferating tools and services and creating the conditions for a new arms race. Cyber-weapon escalation in the form of a cyber-arms race self-generates additional threats that primarily serve the financial interests of the cyber military-industrial complex. Still, the Liberal School lacks precision in addressing cyber threats as well as the special interests of the cyber military-industrial complex. Furthermore, the fundamental debate over its core imperative (liberal freedom vs. state control) limits the Liberal School's utility in terms of understanding the changes affecting warfare and the reassessment of traditional military praxis.

While many of the objections raised against the Materialist Schools of Thought would seem to imply the relative correctness of the Conservative position, it may under-estimate the threat posed by cyber warfare. Consistent with the dangers of Black Swan Theory and Hume's Induction Problem, by focussing on the constancy of warfare, it may miss the outlier changes that might ultimately lead to a shift or fundamental revolution in military affairs. An intellectual born out of the Romantic era, Clausewitz viewed war and human affairs as entities apart from

scientific rules and principles. He sought to explain the impact of morale and military genius, such as Napoleon, on the practice of warfare. Clausewitz was writing against earlier military based Enlightenment theory which was attempting to provide a scientific basis for the conduct of warfare and characterise the praxis of 18th century warfare through the tools of geometry. Thus, while Clausewitzian thought provides the benchmark for analysing the presence of change in warfare, Clausewitz himself was writing of fundamentally revolutionary events and how they had changed the nature of warfare from what it had been prior to Napoleon. If society is in fact going through social shifts as momentous as those created by the conditions of Industrialism and the Enlightenment, then the Conservative School of Thought, with its emphasis on the incremental/evolutionary rather than revolutionary value of information technology, may miss the changes that are all around us.

It is important to note that the ontological issues concerning the crisis of modernity are far broader than simply the changes in the military cyber warfare environment or even of information technology itself within the social conditions of "post-industrial" society. As far back as the 1960s, authors such as Marshall McLuhan were noting that important technological social shifts were underway that were likely to cause significant shifts in how society functions. One needs to understand the nature of information technology and its broader social dimensions. This will permit the discussion to escape the cage in which it has been placed by the parameters of the technology-led RMA debate. Instead, one must consider the implications and social consequences given the ontological changes to the very being of society. In doing so, one calls upon the value of the "out of the box" perspectives of the Revolutionary School to extrapolate clear guideposts and cautionary tales of a technologically determinist society. C ellular telephone culture derived from the revolution in mobile personal communications is but one example of

society's technological determinism. The growing impatience to move information more quickly and always be connected with society is the foundation of the addiction which abhors the separation of an individual from personal communications.

A consideration of the epistemological issues confronting those who wish to use cyberspace as a new vector for state action must be dealt with before one can be secure in moving forward with this capability. The essential mutability of information technology poses concrete challenges to the use of this technology to achieve political ends in the manner warfare has traditionally functioned. Strategic advantages derived from the exploitation of cyberspace have been difficult to identify. The nature of the epistemological challenges may pose as many opportunities as barriers for those who can take advantage of them. For governments and militaries such as the CAF to resolve the epistemological dilemma, they must first embrace the technologic influences and changes on society's ontology. Institutions must be honest in their assessment of the social dimensions influenced by technology. For command chains this entails an introspective look at what cyber technology means for the being of people and organizations and the ontological significance on the existing praxis of warfare. This also means accepting the military operating environment has increased in complexity with the introduction of cyber capabilities and exploits. The debate of whether cyberspace is its unique warfighting domain or harmonized with the traditional warfighting domains remains outside the scope of this paper. Nevertheless, the acceptance that a warfighter's ontology involves interacting and employing cyber capabilities is a significant step toward bridging the epistemological/ontological divide.

The proposed schema of the" Cyber Warfare Schools of Thought" can in fact bridge the epistemological/ontological divide. Having accepted that society's ontology has changed, militaries such as the CAF must develop a pragmatic and comprehensive cyber warfare strategy

that not only complements traditional warfighting capabilities but address the threat realities of the current modern world with responses up to and including military force. From the Schools of Thought schema this would entail the CAF adopting a Liberal Materialist perspective in drafting such a strategy. For a traditionally "conservative" organization, such a shift in perspective may be difficult and require a shift in institutional culture. In educational terms, this may entail a better balance/mix of leadership backgrounds ranging from conservative defence studies (social sciences) to liberal rooted scientific and engineering studies (applied sciences). This does not mean that all the traditional values in the Conservative School will be lost, but rather enhanced with Liberal and potentially some Revolutionary Materialist inspired insights. A consolidated and well-rounded perspective of cyber warfare derived from the School of Thought schema will empower the CAF to be more versatile and responsive to known and unknown cyber threats. The use of the "Cyber Warfare Schools of Thought" schema should not be approached from a purely quantum perspective labeling people and organizations by discrete Schools that never change. The "Cyber Warfare Schools of Thought" schema is a spectrum that can be leveraged and employed as the situation demands. Nevertheless, the anchor of the CAF strategy needs to be unified and clearly solidified on Liberal Materialists values if it is ever going to effectively bridge the epistemological/ontological divide.

Leveraging the proposed typology one can conclude that cyberspace is a working space that traverses the divide between a purely technologic base of knowledge and the state of society's being. For society to effectively resolve its own social epistemological dilemma, it must find resolution in the questions relating to the meaning and significance of cyberspace. The social nature of knowledge must be tempered by the understanding of what society has become. No longer the exclusive territory of science fiction, cyberspace is a reality from which society's

existence is supported. In order to dispel its fears of cyber technology, society in general must demand that its government be more transparent about the threats and the ends, ways and means of national strategy that are being used to protect everyone against misuse, abuse and anarchy.

BIBLIOGRAPHY

60 Minutes Overtime. "Can the U.S. military's new jet fighter be hacked?." Last modified 01 June 2014. http://www.cbsnews.com/news/can-the-f-35-be-hacked/.

Adee, Sally. "The Hunt for the Kill Switch." *Spectrum, IEEE* 45 no. 5 (2008): 34-39.

Agel, Jerome. *The Making of Kubrick's 2001*. New American Library, 1970.

Alexander, Keith B. *Warfighting in cyberspace*. National Defense Univ Washington DC Inst for National Strategic Studies, 2007.

Arquilla, John, and D. Ronfeldt. *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation, 2001.

Arquilla, John, and D. Ronfeldt. "Cyberwar is coming!." *Comparative Strategy* 12, no. 2 (1993): 141-165.

Arquilla, John, and D. Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Vol. MR-880. Santa Monica, Calif.:Rand corporation, 1997.

Arquilla, John, and D. Ronfeldt. *The Advent of Netwar*. Santa Monica, CA: National Defense Research Institute, RAND, 1996.

Barton, Rosemary. "Chinese cyberattack hits Canada's National Research Council." *CBC News*, last modified 29 July 2014. http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.

BBC News. “Iran nuclear deal: Key points.” Last modified 20 January 2014. http://www.bbc.com/news/world-middle-east-25080217.

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* Yale University Press, 2006.

Betz, David J., and T. Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. New York: Routledge, for the International Institute for Strategic Studies, 2011.

BibleHub. “2942. Kubernétés.” Last accessed 28 April 2015. http://biblehub.com/greek/2942.htm.

Bowcott, Owen. "UN urged to ban 'killer robots' before they can be developed." *The Guardian*, last modified 09 April 2015. http://www.theguardian.com/science/2015/apr/09/un-urged-to-ban-killer-robots-before-they-can-be-developed.

Boyd, John R. "The Essence of Winning and Losing." *Unpublished Lecture Notes* (1996).

Brown, Dale. *Day of the Cheetah.* New York: Berkley Books, 1989.

Builder, Carl H. *The masks of war: American military styles in strategy and analysis: A RAND Corporation research study*. Baltimore, Md.: Johns Hopkins University Press, 1989.

Burns, R. Nicholas, Jonathon Price, Joseph S. Nye, Brent Scowcroft, Aspen Institute, and Aspen Strategy Group. *Securing Cyberspace: A New Domain for National Security*. Washington, D.C.: Aspen Institute, 2012.

Canada. Department of Public Safety. *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. Ottawa: Canada Communication Group, 2015.

Canada. Department of Public Safety, *Canada's Cyber Security Strategy*. Ottawa: Canada Communication Group, 2010.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media Inc., 2011.

Castells, Manuel. *The Network Society: A Cross-cultural Perspective*. Northampton, MA: Edward Elgar Publishing, Inc., 1996.

Castells, Manuel. *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Vol. 1. John Wiley & Sons, 2011.

CBS. "Person of Interest." Last accessed 14 April 2015. http://www.cbs.com/shows/person_of_interest/.

Clarke, Arthur C. "Dial 'F' for Frankenstein." *Playboy* (1965).

Clarke, Richard A. and R. K. Knake. *Cyber War: The Next Threat to National Security and what to do about It*. New York: HarperCollins, 2010.

Clausewitz, Carl von, Michael Eliot Howard, Peter Paret, and Beatrice Heuser. *On War*. Oxford World's Classics. [Vom Kriege.]. Oxford: Oxford University Press, 2007.

CyberWarZone. "New F-35 Fighter Jet is vulnerable to cyber-attacks." Last modified 31 May 2014. http://cyberwarzone.com/new-f-35-fighter-jet-vulnerable-cyber-attacks/.

Deibert, Ron. "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." *Journal of Military and Strategic Studies* 14, no. 2 (2012).

Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal, 2013.

Deibert, Ronald J., and R. Rohozinski. "Good for liberty, bad for security? Global civil society and the securitization of the Internet." *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008) (2008): 123-149.

Deibert, Ronald J., and R. Rohozinski. "Risking security: Policies and paradoxes of cyberspace security." *International Political Sociology* 4, no. 1 (2010): 15-32.

Deibert, Ronald, and R. Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010): 43-57.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war." *Security Dialogue* 43, no. 1 (2012): 3-24.

Denning, Dorothy Elizabeth Robling. *Information warfare and security*. Vol. 4. Reading, MA: Addison-Wesley, 1999.

Douhet, Giulio. *The Command of the Air*. University of Alabama Press, 2009.

Espenschied, Jon. "A Discussion of Threat Behavior: Attackers & Patterns." *Microsoft Corporation and NATO CyCon*, June (2012).

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." *White paper, Symantec Corp., Security Response* 5 (2011).

Feldman, Noah. *Cool War: The Future of Global Competition*. Random House Incorporated, 2013.

Follath, Erich, and H. Stark. "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor." Last modified 2 November 2009. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Gash, Jim. "Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits." *Canadian Military Journal* 12, no. 3 (Summer 2012): 28-34.

Gladstone, Rick. "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State." *New York Times*, last modified 24 March 2015. http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?ref=topics.

Gleick, James. "Cyber-neologoliferation." *The New York Times Magazine* 5 (2006).

Glenny, Misha. *DarkMarket: How Hackers Became the New Mafia*. Random House, 2012.

Granick, Jennifer Stisa and C. J. Sprigman. "The Criminal NSA." *International Herald Tribune* (2013): 29-30.

Gray, Colin S. *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*. Vol. 2. Portland, OR: Frank Cass, 2003.

Greenberg, Karen J.. "Preparing for a Digital 9/11." *TomDispatch*, Last modified 21 October 2012. http://www.tomdispatch.com/blog/175607/.

Greenert, Admiral Jonathan W. and US Navy. "Imminent Domain." U.S. Naval Institute Proceedings Magazine 138, no. 12 (1) (2012): 318. Last accessed 02 May 2015. http://www.usni.org/magazines/proceedings/2012-12/imminent-domain.

Griffith, Samuel B. and B. Liddell Hart. *The Art of War by Sun Tzu*. New York: Oxford University Press, 1963.

Hall, Wayne M. *Stray Voltage: War in the Information Age*. Annapolis, Md.: Naval Institute Press, 2003.

Harris, Kathleen. "'Killer robots' pose risks and advantages for military use." *CBC News*, last modified 09 April 2015. http://www.cbc.ca/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963.

Headrick, Daniel R. *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*. New York: Oxford University Press, 1991.

Himanen, Pekka. *The Hacker Ethic: A Radical Approach to the Philosophy of Business*. New York: Random House, 2009.

Hsieh, Paul. "8 Star Trek Technologies Moving From Science Fiction To Science Fact." *Forbes*, last modified 24 June 2014. http://www.forbes.com/sites/paulhsieh/2014/06/24/8-star-trek-technologies/.

Ingersoll, Geoffrey. "US NAVY: Hackers 'Jumping The Air Gap' Would 'Disrupt The World Balance Of Power'." *Business Insider*, last modified 19 November 2013. http://www.businessinsider.com/navy-acoustic-hackers-could-halt-fleets-2013-11.

Institute of Physics. "Thumbs-up for mind-controlled robotic arm." Last modified 17 December 2014. http://www.iop.org/news/14/dec/page_64708.html.

Knight, Scott. "War by Computer: Canadian Cyber Forces in 2025." *In The Canadian Forces in 2025 Prospects and Problems*, edited by J. L. Granatstein. First ed., 74-88. Victoria, B.C., Canada: FriesenPress, 2013.

Knox, MacGregor and W. Murray. *The Dynamics of Military Revolution, 1300-2050*. New York: Cambridge University Press, 2001.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." *Cyberpower and National Security* (2009): 26-28.

Langner, Ralph. "To Kill a Centrifuge: A Technical Analysis of what Stuxnet's Creators Tried to Achieve." (2013). Last accessed 02 May 2015. Http://Www.Langner.Com/En/Wp-Content/Uploads/2013/11/to-Kill-a-Centrifuge.Pdf.

Latham, Robert and S. Sassen. *Digital Formations: IT and New Architectures in the Global Realm.* Princeton University Press, 2009.

Lessig, Lawrence. *Code.* Lawrence Lessig, 2006.

Lessig, Lawrence. "The Law of the Horse: What Cyberlaw might Teach." *Harvard Law Review* (1999): 501-549.

Leyden, John. "Israel suspected of 'hacking' Syrian air defences." Last modified 4 October 2007. http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

Libicki, Martin C. "Global Networks and Security: How Dark is the Dark Side?." *The Global Century: Globalization and National Security* (2001): 809-824.

Lipschutz, Ronnie D., and R. Hester. "We are the Borg! Human assimilation into cellular society." *academia.edu*, last accessed 01 May 2015. https://www.academia.edu/6169698/We_are_the_Borg_Human_assimilation_into_cellular_society.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. Vol. 9 Psychology Press, 2004.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, (2010): 97-108.

Martin, Paul E.C. "Covert Channels In Secure Wireless Networks," Master's thesis, Royal Military College of Canada, 2007.

Martin, Paul, Jim Hutton and Loren Klimchuck. *CF Concept of Fusion.* Department of National Defence/Canadian Forces, 07 Aug 08.

Mayer-Schönberger, Viktor and K. Cukier. *Big Data: A Revolution that Will Transform how we Live, Work, and Think.* New York: Houghton Mifflin Harcourt, 2013.

McConnell, Mike. "Mike McConnell on how to Win the Cyber-War We're Losing." *Washington Post*, 28 February 2010. Last accessed 02 May 2015. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

McGuffin, Chris and P. Mitchell. "On Domains: Cyber and the Practice of Warfare." *International Journal: Canada's Journal of Global Policy Analysis* (2014): 0020702014540618.

McLuhan, Herbert Marshall. *Understanding Media: The Extensions of Man*. 1st ed. New York: McGraw-Hill, 1964.

Merriam-Webster. "cyborg." Last accessed 01 May 2015. http://www.merriam-webster.com/dictionary/cyborg.

Merriam-Webster. "liberalism." Last accessed 01 May 2015. http://www.merriam-webster.com/dictionary/liberalism.

Merriam-Webster. "praxis." last accessed 28 April 2015. http://www.merriam-webster.com/dictionary/praxis.

Morningstar, Chip and F. Randall Farmer. "The Lessons of Lucasfilm's Habitat." *Journal for Virtual Worlds Research* 1, no. 1 (2008).

Mosco, Vincent. "The Digital Sublime." *Myth, Power, and Cyberspace* (2004).

Mueller, Benjamin. "The Laws of War and Cyberspace on the Need for a Treaty Concerning Cyber Conflict." (2014).

Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. Mit Press, 2010.

Mueller, Milton, and B. Kuerbis. "Towards Global Internet Governance: How to End US Control of ICANN Without Sacrificing Stability, Freedom or Accountability." In *2014 TPRC Conference Paper*. 2014.

Munslow, Alun. *The Routledge Companion to Historical Studies*. New York: Routledge, 2000.

Paddon, David. "Cyber attacks have hit 36 per cent of Canadian businesses, study says." *The Globe and Mail*, last modified 18 August 2014. http://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/.

Paganini, Pierluigi. "China vs US, cyber superpowers compared." *INFOSEC Institute*, last accessed 29 Apr 15. http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/.

Phillip, Abby. “A paralyzed woman flew an F-35 fighter jet in a simulator — using only her mind.” *Washington Post*, last modified 3 March 2015. http://www.washingtonpost.com/news/speaking-of-science/wp/2015/03/03/a-paralyzed-woman-flew-a-f-35-fighter-jet-in-a-simulator-using-only-her-mind/.

Piscitello, David. "Conficker Summary and Review." *ICANN*, May 7 (2010).

Public Safety Canada. “Cyber Security in the Canadian Federal Government.” *Government of Canada*, last modified 04 March 2014. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-eng.aspx.

Pollock, John. “Streetbook: How Tunisian and Egyptian Hackers and Soccer Fans Created the Arab Spring.” *MIT Technology Review*, last modified 23 August 2011. http://www.technologyreview.com/featuredstory/425137/streetbook/.

Pretorius, Joelien. "The Technological Culture of War." *Bulletin of Science, Technology & Society* (2008).

Rasmussen, Mikkel Vedby. *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge University Press, 2006.

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

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, Mass.: MIT Press, 2001.

Regalado, Antonio. “Military Funds Brain-Computer Interfaces to Control Feelings.” *MIT Technology Review*, last modified 29 May 2014. http://www.technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press, 2013.

Roscini, Marco. "World Wide Warfare-'Jus Ad Bellum' and the use of Cyber Force." *Max Planck Yearbook of United Nations Law* 14 (2010): 85-130.

Russell, Alison Lawlor. *Cyber Blockades*. Washington, DC: Georgetown University Press, 2014.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. 1st ed. New York; Emeryville, CA: Thunder's Mouth Press; Distributed by Publishers Group West, 1994.

Schwartz, John. "Preparing for a Digital Pearl Harbor." New York Times (2007).

Shachtman, Noah. “Exclusive: Computer Virus Hits U.S. Drone Fleet.” *WIRED*, last modified 07 October 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/.

Shachtman, Noah. “Military ‘Not Quite Sure’ How Drone Cockpits Got Infected.” WIRED, last modified 19 October 2011. http://www.wired.com/2011/10/military-not-quite-sure-how-drone-cockpits-got-infected/.

Shalal-Esa, Andrea. "Pentagon downplays comment on F-35 fighter jet cyber threat." *Reuters,* last modified 25 April 2013. http://www.reuters.com/article/2013/04/25/us-lockheed-fighter-cyber-idUSBRE93O1HK20130425.

Shalal, Andrea. "Nearly every U.S. arms program found vulnerable to cyber attacks." *Reuters,* last modified 20 January 2015. http://www.reuters.com/article/2015/01/21/us-cybersecurity-pentagon-idUSKBN0KU02920150121.

Sherwell, Philip. "Canadian killer was recent convert to Islam identified as terror risk." *The Telegraph*, last modified 23 October 2014. http://www.telegraph.co.uk/news/worldnews/northamerica/canada/11181394/Soldier-killed-as-gunman-brings-terror-to-Canadian-Parliament.html.

Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Sky News. “China Cyberattack: US Weapons Systems Breached.” Last modified 29 May 2013. http://news.sky.com/story/1096826/china-cyberattack-us-weapons-systems-breached.

Stockton, Nick. “WOMAN CONTROLS A FIGHTER JET SIM USING ONLY HER MIND.” *WIRED*, last modified 5 March 2015. http://www.wired.com/2015/03/woman-controls-fighter-jet-sim-using-mind/.

Taleb, Nassim Nicholas. "The Roots of Unfairness: The Black Swan in Arts and Literature." *Literary Research/Recherche Litteraire* 21, no. 41-42 (2005): 241-254.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. Random House, 2010.

Thomas, Craig. *Firefox.* London: Michael Joseph Ltd, 1977.

Unit, Economist Intelligence. "Big data-Lessons from the leaders." *Londres: The Economist* (2012).

United Nations. “CHAPTER VII: ACTION WITH RESPECT TO THREATS TO THE PEACE, BREACHES OF THE PEACE, AND ACTS OF AGGRESSION.” Last accessed 01 May 2015. http://www.un.org/en/documents/charter/chapter7.shtml.

United States. Executive Office of the President of the United States. *National Security Strategy of the United States, May 2010.* Washington, DC: U.S. Government Printing Office, 2010.

United States. Executive Office of the President of the United States The White House. “Summary of Technical Understandings Related to the Implementation of the Joint Plan of Action on the Islamic Republic of Iran’s Nuclear Program.” Last modified 16 January 2014. https://www.whitehouse.gov/the-press-office/2014/01/16/summary-technical-understandings-related-implementation-joint-plan-actio

United States. Executive Office of the President of the United States. *National Security Strategy of the United States, February 2015.* Washington, DC: U.S. Government Printing Office, 2015.

Ventre, Daniel. *Cyber Conflict: Competing National Perspectives.* John Wiley & Sons, 2013.

Wiener, Norbert. *Cybernetics* Paris: Hermann, 1948.

Wu, Tim. *The Master Switch: The Rise and Fall of Information Empires.* Toronto: Knopf, 2011.

Yasar, Nurgul, Fatih M. Yasar, and Yucel Topcu. "Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield." In *SPIE Defense, Security, and Sensing*, pp. 84080G-84080G. International Society for Optics and Photonics, 2012.

Zetter, Kim. “A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER.” *WIRED*, last modified 01 January 2015. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

Zittrain, Jonathan. *The Future of the Internet--and how to Stop It*. Yale University Press, 2008.