IPRI Journal XV, no. 2 (Summer 2015): 95-112

Strategizing Cyber Revolution within the Domain of Security Studies

Dr. Zafar Khan*

Abstract

Cyber technology is now part of international security apparatus and its study in this realm has assumed a key place. Cyber studies require a sound theoretical formulation and execution within the literature of strategic and security studies. Currently, this literature is extremely limited. Most of the recent works on cyber revolution refer to the unending debate on cyber pessimism and optimism and the challenges and prospects of war resulting from conflicting cyber episodes. Not much work has been done on the importance of strategizing cyber studies within the domain of security studies. This article goes beyond the existing literature and attempts to evaluate cyber related issues in order to find if cyber studies can form part of the broader domain of strategic studies. It suggests that a sound and comprehensive theoretical foundation is required to be laid if cyber studies' claim for a place in security studies is to be accepted.

Keywords: Cyber Revolution; Strategizing Cyber Studies; Security Studies; The Evolution of Cyber World

Introduction

The phenomenon of cyber weapons originated with the emergence of the computer and the internet. The cyber weaponry includes computer viruses which are created and designed to corrupt, infect, harm and destroy the normal life of a computer.[1]These computers handle a state's political, economic, military and strategic activities. Thus, states which are vulnerable to cyber invasion would always develop a perception with regard

* The Author is Assistant Professor, Department of Strategic Studies, Faculty of Contemporary Studies, National Defence University, Islamabad.

1 Kevin G. Coleman, "Aggression in Cyberspace," in Scott Jasper ed. "*Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*," (Washington: Georgetown University Press, 2012), 105-122.

to computers and computer related materials. They are likely to be suspicious of introducing computers in the major domain of the state's architecture and would question the origin of computers and its related ingredients and whether their usage in running the state's mechanism, is safe, secure and reliable? Any possible harm and infection via cyber invasion may not only slow down the state's affairs, but also undermine the safety and security of the national economic, political and strategic assets. A cyber invasion on the state's computer system can also facilitate one state's military intervention into another state by paralyzing its central line of command, control and communication. Although a cyber attack may not cause large scale collateral damage like conventional and strategic weapons, the protection and combat against these unknown cyber-related viruses becomes a routine duty and responsibility of the state. Geographical distances between states become irrelevant in this warfare. Therefore, there is greater possibility of cyber invasion from powerful states against weaker states, from weaker against powerful states, and from non-state actors against the state actors, though the nature and degree of such invasion may vary from country to country depending on the level of expertise and the nature of the goal to be accomplished. With technological advancement, the mechanics of the sophisticated machines is getting complex and hard to comprehend. For instance, cyber-related viruses may have a stealthy capability together with speed that the central domain of a computer under attack may have no knowledge about. The increasing number of cyber incidents show the threat exists. Even the most developed countries like the US face the cyber threat. The US official pronouncements raise concerns about cyber-related threats of a quick and rapid invasion that could be determined in "nanoseconds."[2]The RAND 1993 report by John Aquila and David Ronfeldt declared that the "cyber war is coming".[3] Very recently, the US Secretary of Defence Leon Panetta warned the US administration of a "cyber-Pearl Harbor"[4] stating, "the next Pearl Harbor could very well be a

[2] Dan Kuehl, quoted by Grace Chng, "Cyber War: One Strike, and You're Out," *Sunday Times* (Singapore), July 18, 2010.

[3] John Arquilla & David Ronfeldt, "*Cyber War is Coming*," Rand, 1993, 1-38: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf (accessed March 17, 2015).

[4] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyber-Attack," *New York Times*, October 11, 2012.

cyber-attack".[5] In this sense, cyber pessimism continues amongst major defence circles in the US William Lynn, the US Pentagon Deputy Secretary of Defence stated, "Although cyberspace is a man-made domain", it has become "just as critical to military operation as land, sea, and space."[6]And Richard Clarke considered the tsar of cyber revolution urges the US to take concrete measures to avert the threats emanating from cyber weaponry.[7]

Nevertheless, it is difficult to understand the strategic aspects of the innovative technology that is behind the cyber revolution. Simply, it would take time for a strategist to craft a framework to understand well what cyber revolution would mean; and it would not be easy for the technical side to master the major ingredients of strategic studies in order to help emplace cyber studies within this broader domain. For example, despite the rising cyber threats, the US administration gets entangled with regard to cyber revolution and its interaction with the conceptual strategic aspects.[8] Intellectual development and policy relevance demand the integration of cyber revolution within the domain of strategic studies; it requires the avoidance of the existing dichotomy between the technical and conceptual strategic aspects to better understand cyber revolution and its implications; and more importantly, this could require strategic scholars to open their strategic toolkits to craft a better theoretical framework that underpins cyber related issues and their closer examination both from a technical and theoretical point of view.

This article attempts to find out whether or not there is a room for cyber revolution to get strategized and emplaced as one of the essential pillars of strategic and security studies. While most studies focus on the technical, legal, and military aspects of the cyber studies, some of them examine the prospects of cyber revolution bringing states to war.[9] Other

---

[5] Lisa Daniel, "Panetta: Intelligence Community Needs to Predict Uprisings," *American Force Press Service*, February 11, 2011.

[6] William J. Lynn, "Defending a New Domain," *Foreign Affairs*, 89 (5), 2010, 101.

[7] Richard A. Clarke and Robert K. Knake, "*Cyber War*" (New York: Ecco, 2010)

[8] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft" *International Security*, 38(2), fall, 2013, 7-40.

[9] Cyber pessimism holds a perception that cyber war is coming and it will take place; Arquilla and Ronfeldt, "Cyber War is Coming," *Rand*, 1993, 1-38: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf (accessed 17 March, 2015); John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies*, vol. 36, no.1 (2013), 101-108; David C. Gompert

works represent cyber optimism on the strength of empirical evidence that a cyber war would not take place.[10] Yet, most recent studies tend towards cyber pessimism. There is a little or nothing written on the strategic aspects of cyber revolution becoming one of the important pillars of international security. This article is an attempt to deal with issues relating to strategic aspects of the cyber revolution. It provides a theoretical discussion of the many issues that cyber studies face and encourages more scholarship to conceptualize the practical understanding of cyber technology as a tool of strategic and security studies.

Understanding Cyber Studies

Cyber revolution is an innovative and emerging domain in the field of social sciences. It has rapidly occupied a unique place in the international politics especially with regard to security and strategic issues. The rich domain of strategic and security studies accepts the emerging trends of cyber revolution in terms of observing, reflecting, formulating and executing the theoretical framework of this embryonic field of research. Although much is being written on this, however, scholars, policy maker, and practitioners have yet to comprehend both the conceptual and operational ingredients of cyber studies. There is no substantial understanding of how cyber studies can have a theoretical framework? Or whether that is needed or not. How would security and strategic studies scholars strategize cyber studies? The chief of US Cyber Command,

---

and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival*, vol. 56, no. 4 (August-September 2014), 7-22; Andrew F. Krepinevich, *Cyber Warfare: a nuclear option*? US: Centre for Strategic and Budgetary Assessment, 2012, 1-84; David E. Sanger, 'Obama Order Sped up Wave of Cyber attacks against Iran', *Washington Post*, June 1, 2012; Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), ch. 8.

[10] Cyber optimism holds a perception that cyber war is not coming and this will not take place. See Thomas G. Mahnken, "Cyber War and Cyber Warfare," in Kristin M. Lord and Travis Sharp eds. *America's Cyber Future: Security and Prosperity in the Information Age* Washington D.C.: Center for a New American Security, 2011; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, 35 (1) February 2012, 5-32; For a brief version of Thomas Rid account on cyber warfare, see Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal*, 157(1), 6-13.

General Keith Alexander, stated that there exists confusion and no common agreement "on how to characterize the strategic stability" of cyber interactions "or on what to do about it".[11]The good news is that the states have started to think about cyber revolution with the rapid pace of technological advancement and to relate it with strategic and security issues. Though in its early stages concern about cyber studies is surfacing among states, especially the major powers which are showing interest in understanding and formulating polices with regard to cyber related issues. The dilemma still exists between the theoretical and operational domains. That said, it is imperative to note that those who understand the strategic part of research, may not fully comprehend the operational and technical aspects of cyber studies, while those trained and having the technical know-how may lack the intellectual and conceptual understanding required to strategize cyber studies. The dilemma, perhaps, would continue within the domain of international politics until cyber studies are comprehensively absorbed within the discourse of strategic and security studies. In the meantime, the fictional and intellectual endeavors would flourish and dominate the field of cyber studies each attempting to sort out a better theoretical framework to provide a sound base for future scholarship.

Theorizing Cyber Studies

Cyber studies are still in an embryonic stage and attempts are being made to popularize and theorize the cyber revolution, yet the concreteness of theoretical explanation is still required. Initially, the world did not know what to do with the advanced military weapons since the dawn of the industrial revolution. Nation-states later came to know how to manipulate and strategize these new weapons to achieve their political and military goals. Similarly there was no theoretical explanation of deterrence when the nuclear weapons came on the scene.[12] States' leadership, policy makers and scholars lacked proper understanding of the nuclear weapons and their deterrent aspect: can they be used as *regular weapons* within the military domain? After several decades, the world realized the rationale of the

---

[11] Keith B. Alexander to the US Senate Committee on Armed Services (Washington DC: US Government Printing Office, April 15, 2010), 219.

[12] For a wonderful work on this aspect, see William Walker, "International Affairs and 'the nuclear age', 1946-2013," *International Affairs*, 90 (1), (2014), 107-123.

nuclear weapons that they could only be used for political purposes as a way to deter the adversary given the fear associated with these weapons. The strategy of nuclear weapons was later crafted and conceptualized into various aspects of deterrence (i.e., mutual assured destruction, rational deterrence, virtual deterrence, limited deterrence, minimum deterrence, and recessed deterrence). Nuclear policies were initiated in terms of deterrence, force structure, command, control and communication, targeting options, concealment, dispersal, protection, and arms control and disarmament.[13] Despite the danger and fear linked with these deterrent forces, the world started to live with the nuclear weapons. Like the conventional and strategic deterrent forces, cyber weaponry needs a sound theoretical foundation to better understand cyber revolution within the parameters of international politics, although cyber weaponry is different from strategic and conventional forces. When theorizing cyber studies, scholars need to keep in mind the reasons, significance, and theoretical aspects of this particular issue. Also, there are some theory-based issues that need further understanding and scholarship to overcome the gaps.

First, it is considered that there are many cyber related intrusions taking place and their number is increasing each year. The incidents on routine bases are getting so profuse that it is difficult, if not impossible, to analyze these technical and often codified data. It is reported that only in the US nearly 50,000 cyber related attacks of varying characteristics took place between 2011 and 2012.[14] The lack of refined theoretical cyber framework and poor techniques in understanding the incoming hundreds and thousands of cyber intrusions discourage the prospects of scholarship to theorize and strategize cyber studies within the domain of security studies. Part of the issue lies with the state's strict secrecy on cyber related matters. Stephen Walt, a security expert in international politics, states "the whole issue is highly esoteric – you really need to know a great deal about computer networks, software, encryption, etc. to know how serious the danger might

[13] For interesting analysis on this, see Rajesh Basrur, *Minimum Deterrence and India's Nuclear Security*, California: Stanford University Press, 2006; Also, see Zafar Khan, *Pakistan's Nuclear Policy: a Minimum Credible Deterrence*, (London: Routledge, 2015).

[14] Michael S. Schmidt, "New Interest in Hacking as Threat to Security," *New York Times*, March 13, 2012.

be."[15] In most of the states, cyber related attacks are shrouded in deep secrecy. Very often the private firms who run the critical cyber infrastructure keep the cyber related intrusions ambiguous for obvious reasons of avoiding the reputational and financial cost. This creates suspicion between scholarship and practice.

Second, the ambiguity also lies with the sound understanding whether or not cyber-attacks could be termed as a declaration of war upon states. To know whether cyber-attacks of varying degree could be considered as an act of war against the victim states, it is imperative to go back to the essential ingredients of war and relate them to the cyber warfare. One, it is important to understand how much the strategic approach with regard to war fits the domain of the emerging cyber warfare discourse. Two, the essential ingredients of war could be compared and contrasted with cyber warfare for chalking out a better theoretical and comparative analysis for future scholarship of cyber studies. To do this, strategists need not to go beyond the literature produced by Carl von Clausewitz whose definition of war and its essential determinants still provide a sound understanding of warfare even in the 21st century. The Clausewitzian literature on warfare remains classic: First, the war always remains "violent" and "lethal". It is "an act of force to compel the enemy to do our will."[16] Without the physical violence, the notion of war remains a hodgepodge.[17] That said, war brings violence and violence escalates to extreme causing killing and destruction. Second, war is instrumental in character. It means war theorizes the *means* (physical force) and the *end* (to force the enemy to accept the attacker's will). More broadly, the instrument of war includes tactical, operational, strategic and political aspects. Last but not least, war is political in nature. War does not remain one sided. The nature of war is political in a sense that there is purpose behind waging a war against another state. Along with the military goal where force is enacted, the political means remain the backbone of

---

[15] Stephen M. Walt, "Is the Cyber Threat Overblown?" Stephen M. Walt blog, *Foreign Policy*, March 30, 2010. Also, see Walt, "What Does Stuxnet Tell Us about the Future of Cyber-Warfare?" Stephen M. Walt blog, *Foreign Policy*, October 7, 2010.

[16] Carl von Clausewitz, *Vom Kriege*, Berlin: Ullstein 1832, 1980, 27.

[17] Jack P. Gibbs, "Deterrence Theory and Research," in Gary Melton, Laura Nader and Richard A. Dienstbier eds. *Law as behavioral instrument*, Lincoln: University of Nebraska Press, 1987, 87.

war. Clausewitzian often quoted phrase with regard to political aspect of war: "War is a mere continuation of politics by other means".[18] Moreover, the actual war must be violent, political, and instrumental in nature. These essentials are rudimentary associated with the act of war. Modern strategists and theorists need to determine cyber-attacks and cyber-warfare through the lens of Clausewitzian fundamentals of war. If cyber warfare includes these basic instruments, then it could become easier for security studies scholars to determine whether or not cyber-attacks are violent, political, and instrumental in nature. For now, cyber warfare has failed to absorb these essentials of actual warfare. Unlike cyber pessimists, cyber-optimists claim that cyber warfare does not alter the actual characteristics of war which is not so violent and does not create collateral damage and therefore, cyber danger is overstated. It is difficult to determine whether or not any cyber-attack could be declared as an act of war against the victim state.

Third, for a sound theoretical setting with regard to cyber revolution and cyber warfare, the debate between the cyber pessimism and cyber optimism is very useful. Like the debate between the nuclear pessimism and nuclear optimism, the cyber warfare debate is expected to expand and enrich the theory side of cyber studies and gradually help make a room for it in security studies. The caveat at present with regard to cyber revolution is that it lacks the expected level of intellectual conceit like the security and strategic studies. It is yet to reveal what the cyber world looks like. Cyber studies with technological wordings can go nowhere, but secure merger with the rich literature of international security studies. The enriched conceptual theoretical understanding of security studies and its core intellect can be teased down and unpacked by the emerging cyber studies to avoid the dangers of cyber theoretical stagnation. However, the security studies scholars have not yet made serious efforts to acknowledge cyber studies. Lucas Kello states, "The security studies scholars have barely begun to apply their theoretical toolkits to explain, model, or predict competition in the cyber arena; in a realm of study that should be theirs, they have provided no school."[19]This widening gap between the cyber and

[18] Clausewitz, no. 12, 44.
[19] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraftm," 13.

security studies remains a sheer obstacle for crafting a cyber-school of strategy –one that should be based on flawless policy orientation.

Last but not least, cyber studies require security policy in relation to cyber revolution and need to be based on the flawless assumption. A policy based on flawed assumption is likely to fail if it is not carefully and intellectually crafted. Bad theories with regard to newer technology could bring more chaos and danger to international security in general and the state's strategic architecture in particular. The overall strategy in relation to the cyber revolution and its framework could vary from one state to another in terms of the nature of attack, predictability, threat perception, and the motives behind the cyber intrusions. A sound understanding, formulation, and execution of any cyber related strategy should be based on the concreteness of better and effective theoretical grounds which in turn could help the policy makers to understand and predict the cyber related warfare and its possible intrusions in a state's machinery. This would help the scholars and policy makers to assume correctly the state's strategic architecture through the lens of cyber revolution.

To construct a framework on related issues and the close examination of various important cases bolstered with empirical analysis becomes the first step forward. Effective theorization of cyber studies require more reliable cases, the technicality and coded ingredients in relation to cyber warfare, cyber threat, and cyber revolution need a careful analysis. Although few cases are often quoted in the existing literature for understanding cyber revolution and its implications on strategic studies, scholars require more cases that are classified by the states vulnerable to cyber-attacks. Scholars need to understand why cyber studies, if it can be theorized and strategized within the state's strategic architecture, can bring war to the state. This is discussed in the following sections by examining few relevant cyber-related episodes in the cyber world and find out if cases like these would suffice to provide a broader understanding of the cyber studies, its strategy, and future implications on state's security.

Cyber Incidents and their Implications on the State's Strategic Architecture

Cyber incidents have been on the rise over the past dozen years. The damaging aspects of cyber incidents such as the Siberian pipeline explosion (1982)[20], Stuxnet Cyber Worm (2009/2010),[21] Estonian Cyber Episode (2007)[22] and Georgian Cyber-related Incident (2008)[23]and their objectives can vary from case to case depending on their nature. The existing empirical evidences show that security breaches against the governmental institutions and private firms are occurring frequently. Although these cyber related cases have not yet caused much collateral damage, the debate between the cyber-pessimism and cyber optimism is getting enlarged. However, it is important to understand how these incidents could impact the state's security in the absence of sound cyber framework and how these and many other unknown cyber related incidents could help the construction of cyber studies within the broader domain of strategic studies.

In addition to the above mentioned cyber incidents, there are many other cyber-attacks against the computerized systems of states that are vulnerable to cyber related attacks like the "*Moonlight Maze*", "*Operation Orchard*", "*Titan Rain*", "*Aurora", "Night Dragon"* and *"Shady Rat".* These cases are few amongst many discussed in cyber studies, but may have little or no major strategic implications for the state's security

---

[20] Thomas C. Reed, *At the Abyss* (New York: Random House, 2004); Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Ecco, 2010); National Transportation Safety Board, "Pipeline Rupture and Subsequent Fire in Bellingham," *Washington*, June 10, 1999; Pipeline Accident Report, NTSB/PAR-02/02 Washington DC, 2002; Anatoly Medetsky, "KGB Veteran Denies CIA Caused 82 Blast", *Moscow Times*, March 18, 2004.

[21] Sanger, "Obama Order Sped up Wave of Cyber-attacks against Iran;" Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, ch. 8; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, 53 (1), March 2011, 23-40; Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 108.

[22] On the Estonian cyber related episode, Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents*, Tallinn: CCDCOE 2010, 2; Josef Menn, *Fatal System Error: the hunt for the new crime lords who are bringing down the internet*, (New York: Public Affairs, 2010); Tim Espine, "Estonia's cyber-attacks: lessons learned, a year on," *ZDNet UK*, May 1, 2008.

[23] Tikk, Kaska and Vihul, *International Cyber Incidents*, 1-132; Krepinevich, *Cyber Warfare: a nuclear option*?, 20-25.

infrastructure. Although it does not mean that states vulnerable to cyber incidents may not plan to counter these incidents given the rise of cyber-attacks around the world. Thomas Rid, in his seminal piece "cyber war will not take place" is widely optimistic that these cyber-attacks have no greater strategic implications. These types of attacks only damage the machines not the men. Therefore, no major collateral damage has occurred due to cyber-attacks. If cyber related incidents have ever occurred with concrete galley of proof, then these events do not meet the essential ingredients of Clausewitzian understanding of war. They are non-violent, minimally instrumental and non-political and one may not be able to find out who the attackers are. They have got nothing to do with the cyber warfare and more importantly Rid relates these famous cyber related incidents with the cases of sabotage, espionage, and subversion which are minor to a bigger conceptual understanding of warfare in the real world.[24] In contrast to Rid, as a cyber-optimist, the 1993 RAND report by Arquilla and Ronfeldt presents a pessimistic view on this and argues in their nearly 40-page report that "cyber war is coming".[25]

The emerging debate between these two streams will persist until we reach to a logical conclusion and until we craft and develop a robust theoretical framework to understand, analyze, and predict the cyber cases within the expected domain of international security. For this to happen, both policy makers and scholars need to dig out more cyber related issues and decide whether or not these cases be theorized either in light of strategic and security studies or else could only be tackled through the technical lens. The technical and strategic lenses become two broader beams of cyber revolution which, if tightly knit together, can produce a better understanding of cyber revolution and its theorization within the domain of security studies. Yet, cyber studies would confront issues within the cyber revolution in terms of theorizing and strategizing as long as certain issues with regard to the conceptual understanding of cyber warfare remain on board. These issues, if not carefully, conceptually, and practically tackled, theorizing and emplacing cyber studies within the domain of security and strategic studies may confront both technical and strategic complications. Both policy makers and scholars interested in cyber revolution and its related studies need to analyze the emerging challenging

[24] Ibid., 5-32.
[25] John Arquilla & David Ronfeldt, 1-38. note. 3.

questions: can cyber theoretical framework predict correctly the cyber warfare between two or more states? Could cyber-attacks, however minor they may be cause military escalation perhaps to the nuclear level between two nuclear weapon states? Which aspects of warfare strategy, that is, offensive or defensive may be prioritized when it comes to cyber-attacks? Can the cyber theoretical understanding resolve the emerging attribution difficulties, technological vitality and the cyber ambiguity as the cyber studies groom further? Given these issues in relation to cyber studies, cyber revolution faces difficulties under security studies without a robust and comprehensive theoretical framework. The following section analyses some of these related issues in light of cyber studies and its possible mobility within the domain of security studies.

The Issue of Attribution

The attribution difficulty remains an important issue when it comes to cyber-attacks on a state's political, economic and military infrastructure. It becomes then difficult to untangle the attribution with regard to cyber incidents.[26] Various factors are in play to untangle the attribution issue. Robert Knake, a senior international affairs fellow at the Council on Foreign Relations, presented a report in 2010 to the subcommittee on technology and innovation within the United States House of Representative on attribution issue into three ways: 1) the attacks are difficult to deter because of the individuals living in a non-cooperative country, different architecture of internet, and the lack of security on many hosts; 2) the attribution issue persists in cyber-attacks when it is not carried out merely on internet rather these attacks involve other delivery mechanisms such as the use of microwave radio transmissions, thumb drives and other portable media like CDs and DVDs; and 3) the attribution issue continues to stay with regard to the introduction of malicious code in the supply chain for both hardware and software which is the main concern

[26] Robert K. Knake, "Untangling Attribution: moving to accountability in cyberspace," July 15, 2010. http://www.cfr.org/united-states/untangling-attribution-moving-accountability-cyberspace/p22630 (accessed June 3, 2014); David D. Clarke and Susan Landau, "Untangling Attribution," March 16, 2011, http://harvardnsj.org/2011/03/untangling-attribution-2/ (accessed June 3, 2014).

for state's security in the contemporary world.[27] This indicates the complexity and difficulty in terms of understanding cyber related intrusions which could further lay down issues for cyber strategists to concretely devise a cyber-theoretical framework, although the creation of cyber theory is extremely important to predict timely the cyber-attacks and help resolve the issues of attribution. The practical ground reality is of a different characteristic when it comes to real world politics. The attribution issue with regard to cyber intrusion exists and becomes hard to disentangle. For instance, the attack carried out from within state "A" against state "B" may turn out to be, what Adam Liff stated as a "plausible deniability".[28] In this context, the actor A would deny the attack against the actor B even if the attack in reality was carried out by actor A. The actor B assessment is based on mere suspicion and/or intelligent guess; therefore, based on absence of concrete evidence, actor B cannot initiate the counterattack against actor A. This could have happened in the case of Siberian pipeline explosion, Estonian and even Stuxnet cyber related intrusions. None of the cases truly led states to wage war against each other causing greater instability and collateral damage. The issue of attribution could probably become more problematic with the introduction of several proxies within the states in relation to cyber intrusions. With this cyber-attack related impunity, states are discouraged to undertake counter measures against each other.

The Offense-defence Dilemma

Cyber revolution and its related substances are treated similar to the nuclear and conventional forces. The offence-defence dilemma exists both with regard to nuclear and conventional force deterrence as well as cyber deterrence. Cyber-attack increases the security dilemma; that is, the increase in security of state "A" decreases the security and/or defence of state "B". As the cyber warfare emerges as a new domain of security studies, scholars have already begun commenting in favour of the offensive mode rather than the defensive. Like the nuclear strategists, the cyber strategists consider that there is no defence against attacks and defensive mode, therefore, remains more expensive and over-ambitious. States with

---

[27] Ibid., 3.

[28] Adam P. Liff, "Cyberwar: a New 'Absolute Weapons?' the Proliferation of Cyber Warfare Capability and Interstate War," *Strategic Studies*, 412-413.

defensive prospects with regard to cyber warfare remain vulnerable.[29] Liff states that, "the difficulty of defending against a surprise attack launched against military-affiliated logistic networks or a decapitation attack launched against the command and control systems…suggest that cyber warfare capabilities may significantly favour the offensive advantage".[30] Furthermore, "In a crisis situation in which defence is difficult or impossible, leaders on both sides may feel pressure to attack before being attacked".[31] In addition to this, the cyber offensive mode may favour cyber-strike for three reasons. 1) given the irrelevance of geography in the cyber revolution, the cyber strike attack could be quick, fast and damaging against the defender; 2) the cyber offensive facilitates the conventional strike by disrupting and dismantling the defender's military forces especially when these forces are connected with the computerized mechanism; and 3) it is considered that cyber offensive is not more expensive than the defence. Also hypothetically, those countries that have developed and advanced cyber technology would opt for offensive prospects of cyber strikes. However, the seminal work by Stephen Van Evera indicates the contrasting aspects of the offensive prospects, that is, the offensive mode of attacks could bring repercussion on the overall affairs of the state. The consequences could include aggressive foreign policy; increased risk of pre-emptive war; competitive style of diplomacy; and tighter military and political secrecy.[32] But, states with certain reasons could opt for an offensive mode of cyber-attacks: First, the cyber offensive is considered less expensive compared to defensive force posture when it comes to cyber revolution; 2) it becomes difficult for the states to get little or no time whether or not cyber-attacks are imminent given the speedy characteristics of cyber intrusions; 3) cyber-attack may help facilitate the conventional invasion against the adversary to cause maximum damage by crippling the cyber supported conventional forces; and 4) unlike the conventional and nuclear domain in which geography is considered and known factor, in the cyber world geography becomes irrelevant given the speed of cyber

[29] Clarke and Kanke, "Cyber War"; Andrew Krepinevich, "The Pentagon's wasting assets" *Foreign Affairs*, August, 2009.
[30] Adam Liff, 415. note. 36.
[31] Ibid., 415.
[32] Stephen Van Evera, "The Cult of the Offensive and the Origin of the First World War," *International Security*, 9(1), Summer 1984, 58-107.

intrusion against the adversary's state's infrastructure. Hence, the dilemma between the cyber offense and defence continues to linger.

The cyber strategists who conceptually analyze the cyber warfare need not only to closely observe the cases of the past, but also examine prospects of future cases before reaching to a reasonable conclusion whether or not the cyber offensive aspect is more convincing, worth contending, and preferable. In terms of the cost effectiveness, the cyber offensive aspect could also remain expensive for the states to carry out a successful and timely cyber intrusion. In other words, it is not the defensive aspect that the states would invest more, but the offensive cyber mode may also require states to incur heavy expenditure. However, it is not clear how much states spend on offensive and defensive modes of cyber-related strikes. In the existing literature, scholars have not particularly carried out the cost- benefit analysis of offense-defence of cyber strikes. For a sound theoretical understanding of the cyber studies, the future scholarship need to devise a concrete framework that could provide the scholarship a better picture of cost effective analysis on the offense-defence prospects of cyber revolution.

The Issue of Cyber and Nuclear Weapons Relationship

Very often scholars try to conceptually relate cyber warfare with nuclear weapon attack and they also link cyber intrusions such as espionage, subversion and sabotage cases with the nuclear forces without completely understanding the political and military aspects of nuclear weapons. The world knows the devastating effects of nuclear weapons since they were first used in Hiroshima and Nagasaki, although the lethality of those types of nuclear weapons is less lethal as compared to the advanced and modernized nuclear weapons of today. Nuclear weapons are not like cyber weapons. However, the absence of effective defence against both nuclear and cyber-attacks may urge states in possession of nuclear and cyber deterrent forces to prioritize the political and psychological aspects of these weapons. Even though the US spends billions on missile defence system and the defence shield may turn up to be a success story, but the defence shield may not prevent all the incoming missiles specially when the adversary develops sophisticated Multiple Independent Reentry Vehicles (MIRVs) and increases the number of nuclear forces. Similar may be the case against the cyber offensive attacks. One may defend some lines of intrusion successfully, but the complete cyber storm could become

extremely difficult to defend. Following are some of the differences between cyber and nuclear weapons to develop better understanding whether or not scholars regard cyber weapons as strategic weapons. First, given a few cases of cyber intrusions and nuclear attacks, one could safely argue that cyber-attacks are not lethal compared to nuclear attacks and until now cyber intrusions have not caused collateral damage. Second, nuclear weapons are considered as a political weapon used only for deterrence purposes given the fear associated with the nuclear weapons. Nuclear weapons are not military weapons. The term taboo is associated with the nuclear weapons in order to further promote the non-use of nuclear weapons. Cyber weapons may be used frequently both for political and military purposes. The offensive aspect in relation to cyber warfare is dominant. Third, there is no issue of attribution with regard to nuclear attacks. The attacker may quickly be known by the international community. The issue of attribution exists when it comes to cyber intrusions. The attacker could hide its identification even though the victim could figure out which country was used during the cyber-attacks. But that would be based on suspicion with no concrete evidence. Fourth, difference exists in number of strikes. For example, we may collect and analyze data from hundreds and thousands of cyber-attacks over just a few years, but the nuclear weapons are not used in such a way.

There are still certain other outstanding issues in relation to cyber related intrusions. For example, the cyber-attacks cannot easily be tackled down and/or managed like the conflicts between two states through establishing "hotline" and other useful tactics of confidence building measures. Kello states, "When dealing with a cyber-attack…signaling becomes murky; channels of communication break down or vanish; shared norms are rudimentary or unenforceable; and the identity, motives, or location of an attacker may not be known".[33] Also, given the speed via which the cyber-attacks are carried out remains phenomenal which in turn makes the strategic stance irrelevant. Cyber revolution appears to have seriously engaged the security, strategic and nuclear studies experts to examine these and the forthcoming cyber-related intrusions and work out a credible framework for cyber studies that is missing so that this particular emerging branch of studies finds a safe position within the existing domain of international security. In doing so, there is need for a balanced and more

[33] Lucas Kello, 35, note. 16.

academic approach towards the understanding of the evolving dynamics of cyber studies. At present, cyber studies are dominated by cyber pessimism that would result in one-sidedness if it continues to persist. The issue is not to stop the academic and intellectual endeavors for these invaluable inputs on cyber studies, but there is a need for holistic and fair treatment of the subject dynamics if and when the concreteness of theoretical framework is desired and the cyber studies become part of security studies.

Conclusion

Cyber revolution is becoming an emerging and an essential aspect of security studies. It requires a balanced and proper treatment to place it within the domain of international security. Cyber studies touch the core stream of strategic and security theoretical framework to build its own dynamic architecture. Examining only one side of the picture would not help grasp the quick emergence of this field. Both the industrial revolution and advent of nuclear weapons were covered by the technological shifts. The theoretical foundation for these sophisticated advancements within the cyber revolution is intellectually crafted, yet numerous puzzles with regard to these advancements still need a careful academic consideration. In a similar vein, cyber revolution requires contemporary scholarship to open their toolkits and go back to the security and strategic essential ingredients of various theories to frame a sound theoretical foundation. It requires teasing out those tangible and intangible variables with regards to cyber technology within the domain of security studies to provide a better and intellectually theoretical elucidation. Also, in terms of testing existing strategic theoretical foundation, it is to figure out which theory may best explain cyber related issues and which theory may not explain well. Our understanding on cyber revolution should not be based on murky, biased, and un-wielding approach rather a holistic cyber architecture is required to better understand and accept the arrival of cyber studies within the field of security studies.

Currently, this approach is limited, but with the expected arrival of more cyber episodes, opportunities can be created to promote cyber studies under a sound theoretical foundation. We could then possibly reach to reasonable conclusions whether or not cyber technology would really cause war between two states; how and why offensive is prioritized than defensive approach; if cyber related cases could become escalatory; and how to approach to resolve the attribution issue with regard to cyber related

attacks. At present, the cyber revolution confronts certain issues and is debated whether to embrace it as part of security and/or strategic studies or leave it in doldrums. The strategic/tech knowhow dilemma continues to exist when it comes to strategizing the cyber studies. The widening gap between the two may partially be resolved when the tech-side supply the conceptual and practical knowhow of the cyber revolution to those who are interested in strategizing cyber studies. The tech-side experts interested in cyber studies need to secure sound background knowledge of strategic studies. The two may tangle and help establish a balanced theoretical framework, not beyond the existing enriched strategic and security literature. The task is challenging and difficult, but not impossible. As part of strategic studies axiom: it is not you, but the cyber studies which is interested in you to strategize.■