ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)

DOI: 10.5958/2249-7137.2021.02086.3

CYBER SECURITY LESSONS FROM NUCLEAR WEAPONS

Dr. Ajay Rana*; Rohit Vats**

*Shobhit Institute of Engineering and Technology,
(Deemed to be University), Meerut, INDIA
Email id: ajay.rana@shobhituniversity.ac.in,

**School of Computer Science and Engineering,
Faculty of Engineering and Technology,
Shobhit Institute of Engineering and Technology,
(Deemed to be University), Meerut, INDIA
Email id: rohit.vats@shobhituniversity.ac.in

ABSTRACT

The term "revolutions in military affairs" is arbitrary, but some inflection points in technological change are larger than others: for example, the gunpowder revolution in early modern Europe, the nineteenth-century industrial revolution, the early twentieth-century second industrial revolution, and the nuclear revolution in the middle of the last century. We may also include the information revolution in this century, which has resulted in today's very fast development of cyberspace. Earlier information technology revolutions, such as Gutenberg's printing press, had significant political consequences, but the present revolution can be traced back to Moore's law and the thousand-fold reduction in computing power prices that happened in the final part of the twentieth century. Political leaders and experts are just now starting to understand the implications of this game-changing technology. Cyber security has mainly been the province of computer professionals and specialists until recently. This tiny group was like a virtual village of individuals who knew each other when the Internet was established 40 years ago, and they built an open system with no regard for security. While the Internet is not new, the commercial Web is just a few decades old, with a user base that has grown from a few million in the early 1990s to more than two billion now. This growing interconnectedness has generated both tremendous possibilities and significant weaknesses, which strategists are now grappling.

KEYWORDS: *Cyber War, Cyber Crime, Nuclear Reactor, Nuclear War, Space Technology.*

INTRODUCTION

The term "cyber" refers to computer and electromagnetic spectrum-related activity. The Internet of networked computers is part of the cyber domain, as are intranets, cellular technology, fiber-optic cables, and space-based communications. A physical infrastructure layer exists in cyberspace that adheres to the economic rules of competing resources as well as the political laws of sovereign authority and control[1]. This element of the Internet isn't a "commons" in the conventional sense. It also contains a virtual or informational layer, which is characterized by growing economic rewards on scale and political behaviors that make jurisdictional control difficult. Attacks may be launched from the informational domain, where costs are cheap, against the physical domain, where resources are limited and costly. Control of the physical layer, on the other hand, may have territorial and extraterritorial implications for the informational layer. Within cyberspace or in other areas outside of cyberspace, cyber power may generate desired results. Sea power, by analogy, refers to the capacity to utilize ocean resources to win naval battles on the seas, but it also relates to the ability to use the waters to influence wars, trade, and public opinion on land. The similar analogy may be used to describe airpower[2].A complicated man-made environment is the cyber realm. Human enemies, unlike atoms, are sentient and deliberate.

Mountains and seas are difficult to shift, but cyberspace can be switched on and off with the flick of a switch. Moving electrons around the globe is less expensive and faster than moving big ships over vast distances via salt ocean friction[3]. The expenses of building multiple carrier task forces and submarine fleets create huge obstacles to entry, allowing the United States to claim naval supremacy. Nonstate actors and tiny nations, on the other hand, may play major roles in the cyber realm since the entrance hurdles are so low. One of the major power changes of this century, according to The Future of Power, is the dispersion of power away from governments. This larger tendency is shown by cyberspace. The biggest nations are unlikely to be able to exert as much control over this area as they have over others such as the sea, air, or space[4]. They have more resources, but they also have more weaknesses, and at this point in the technology's evolution, attack outnumbers defense in cyberspace. Although the United States, Russia, the United Kingdom, France, and China have more capability than other state and nonstate entities, it is difficult to talk about cyberspace supremacy. In fact, relying on sophisticated cyber systems to support military and commercial operations exposes big nations to new vulnerabilities that may be exploited by nonstate actors. The Pentagon invented the Internet four decades ago, and by most measures, the United States is still the top nation in both military and civilian usage. At the same time, the United States is more susceptible to assault than many other nations due to its higher reliance on networked computers and communication, and the cyber domain has become a significant source of insecurity. The phrase "cyber-attack" refers to a broad range of activities, including basic probes, website defacing, denial of service, espionage, and destruction[5].

Similarly, the phrase "cyber war" is loosely used to a broad variety of activities. It follows dictionary definitions of war, which vary from military combat to any antagonistic dispute (for example, "war between the sexes" or "war on poverty"). On the other hand, some people define cyber war as a "bloodless war" between nations that solely involves fighting in the virtual realm of cyberspace[6]. However, this sidesteps key problems like the interconnectedness of cyberspace's physical and virtual levels, which we addressed before. Hostile acts in cyberspace that have consequences that magnify or are comparable to significant kinetic violence are a more appropriate definition of cyber war. Governments having a near monopoly on large-scale use of force in the physical world, the defense has a thorough understanding of the terrain, and assaults terminate due to attrition or fatigue. Resources and movement are both expensive. Actors in the virtual world are varied, sometimes nameless, physical distance is irrelevant, and offense is often inexpensive. The attack presently has the upper hand over the defense since the Internet was built for ease of use rather than security. This may not be the case in the long run as technology advances, including attempts to "reengineer" certain systems for increased security, but it is at this time[7].

The bigger party's capacity to disarm or kill the adversary, occupy territory, or employ counterforce tactics successfully is restricted. The most spectacular of the possible dangers is cyber war, which is still in its early stages. Cyber assaults on military and civilian targets may theoretically cause enormous disruption as well as physical damage if carried out by major nations with extensive technological and human resources. Interstate deterrence (but not traditional nuclear deterrence), offensive capabilities, and plans for network and infrastructure resilience if deterrence fails are among the responses to cyber war. It may be feasible to strengthen these processes with some basic standards in the future, but the world is still in the early stages of such a process[8]. If hacktivism is seen as mostly a nuisance at this point, there are four primary types of cyber risks to national security, each with a distinct time horizon and (in theory) various solutions: States are primarily linked with cyber war and economic espionage, whereas nonstate actors are usually associated with cybercrime and cyber terrorism. For the United States, the greatest expenses are now incurred via espionage and crime, but war and terrorism may become bigger risks in the next decade or two. Furthermore, as various players' affiliations and strategies develop, the categories may become increasingly entwined. “Sooner or later, terror organizations will acquire cyber-sophistication,” says ADM Mike McConnell. It's similar to nuclear proliferation, but far less difficult.” We're just now seeing glimpses of cyber war, such as an add-on to certain conventional assaults, such as the denial-of-service attacks that followed the conventional war in Georgia. Can we learn anything about the present cyber change from the nuclear revolution in military operations seven decades ago? The answer seems to be no at first sight[9]. The disparities in technology are just too big. Differences in the threshold for action and attribution are cited by the National Research Council—nuclear explosions are unmistakable, whereas cyber intrusions that plant logic bombs in the infrastructure may go unnoticed for long periods of time before being used, and even then, can be difficult to trace. The sheer destructiveness of nuclear technology is much more striking.

Cyber does not represent an existential danger, unlike nuclear weapons. As points out, the destruction or disconnection of cyber networks may return us to the 1990s economy, resulting in a massive loss of GDP, while a catastrophic nuclear conflict could send us back to the Stone Age. 10 Comparisons of cyber with biological and chemical weapons may be more appropriate in this and other aspects. Furthermore, cyber devastation may be disaggregated, allowing for the delivery of tiny doses of damage over time. While there are various degrees of nuclear devastation, they are always above a critical point or firebreak. Furthermore, although civilian and military nuclear technology overlap, nuclear technology was developed for use in war, and the distinctions in its use are more obvious than in cyber, where the Web has grown in popularity in the civilian sector[10]. The “dot mil” domain name, for example, is just a tiny portion of the

Internet, and 90 percent of military phone and Internet connections are routed via civilian networks.

Finally, nonstate actors have much reduced obstacles to entrance into cyberspace due to economic dominance and cheap costs. While nuclear terrorism is a significant threat, the hurdles to non-state actors getting access to nuclear materials remain high; hiring a botnet to cause havoc on the Internet is simple and inexpensive.However, ignoring the past would be a mistake, as long as we realize that metaphors and analogies are never flawless.“History never repeats itself, but it rhymes sometimes,” as Mark Twain famously said. There are some important nuclear-cyber strategic rhymes, such as the superiority of offense over defense, the potential use of weapons for both tactical and strategic purposes, the possibility of first-and second-use scenarios, the ability to create automated responses when time is limited, the likelihood of unintended consequences and cascading effects when a technology is new and poorly understood, and the likelihood of unintended consequences and cascading effects when a technology is new and poorly understood. Even more significant than these technological and political parallels is the learning process that governments and corporate players go through as they attempt to comprehend disruptive technology and develop strategies to deal with it. Although official studies on computer and Internet vulnerabilities date back to 1991, and the Pentagon just published a new plan, few experts believe the country has established an effective national cyber security strategy.

DISCUSSION ON THE CYBER WAR

The uneven and slow history of nuclear learning should serve as a warning to some of the dangers and possibilities that lie ahead in the cyber realm. In the first half-decade after World War II, Ernest May characterized US military policy and the development of nuclear strategy as chaotic. He'd probably use the same phrase to describe the current state of cyberspace. Nuclear energy was first harnessed for military reasons, but it soon became apparent that it had significant civilian applications as well. During the early stages of nuclear energy research, it was predicted that electricity would become ubiquitous. Too inexpensive to meter” and an atomic reactor would provide a year's worth of fuel for vehicles The size of a vitamin pill pellet. The engineers' enthusiasm for their new invention is contagious. A political goal to encourage civilian applications of technology bolstered technology of nuclear power Fearful of anti-war and anti-nuclear protests. The government of Dwight D. Eisenhower sponsored an Atoms for Peace initiative. Volunteered to help promote nuclear energy throughout the globe. Other several nations took part. As a result, a strong local and international presence was established.

A global campaign for nuclear energy promotion that aided in the provision of materials required for India's nuclear explosion in 1974, France justified the sale of a reprocessing facility to Pakistan and the sale of a reprocessing plant to Germany. Enrichment technique was first introduced to Brazil in the mid-1970s. The Atomic Energy Commission and the Joint Atomic Energy Committee were established to provide civilian control of nuclear technology, but both became instances of regulatory capture over time. Strong economic interests, who are more concerned with marketing than with the truth security and regulation Late in Ford's presidency. The group was dissolved. However, after the 1974 oil crisis, it became an article. Nuclear power would be the energy of the future; that uranium would be the fuel of choice. It would be required to build reactors. Following the Carter administration, the non-governmental Ford-Mitre Report's suggestions, which were attempted in 1977, it hit a roadblock in its efforts to halt the growth of the plutonium economy. Not just from outside, but also from the nuclear sector, there has been a whirlwind of response. Its domestic supporters in Congress. As previously said, the civilian sector plays an even greater role in the conflict. The issue of creating a national security policy is further complicated by the cyber realm. The Internet has evolved into a far more powerful tool. Nuclear energy has never been a major contribution to GDP. The personal than a policy restriction, the sector is at the core of the activity. That policy is intended to safeguard. Risk is unavoidable, and redundancy and backup plans are essential.

A plan must include resilience after an assault. The private sector owns and operates the infrastructure, while the government owns and operates the land. There are just a few little levers to operate. Proposals to establish a central agency in the executive branch as well as a joint committee on cyber security in Congress may be considered. It's important to be aware of the risks of regulatory capture and the formation of a cyber "iron triangle" including the executive branch, Congress, and business. In the cyber realm, there is a mismatch of economic incentives from a security standpoint. Up to a degree, businesses have a motivation to provide for their own security, but product price competition restricts that point. Furthermore, businesses have a financial interest to keep incursions that might undermine public trust in their goods and stock prices hidden. “The public (and, in many cases, the industry) awareness of this major national security danger is essentially negligible owing to the extremely small number of voluntary disclosures by victims of intrusion activity,” according to a McAfee white paper. As a consequence, there is a scarcity of accurate data and a lack of national security investment. Furthermore, antitrust rules limit private-sector collaboration, and the complexity of determining responsibility in sophisticated software restricts the involvement of the insurance market. Different views and distrust hinder public-private cooperation. Something terrible will have to happen before markets begin to reprice security, as one attendee at a recent cyber security conference observed. Without collaboration, learning may lead to belief convergence. Governments operate in the best interests of their countries, but they may also act in the best interests of their citizens. How they define their passions, both in terms of how they describe their passions and how they define their passions.

It was unrealistic to believe that exports would stay entirely quiet. The instability of the weapons race, as well as the costs and dangers it involved, was a fourth area of general knowledge. These points of view evolved separately and in tandem, and it took more than two decades for them to come together in a formal way. Harmony would result from perfect agreement of views, which is very uncommon in global politics. Cooperation in the nuclear field arose from certain shared ideas as well as real and expected conflict. The linked cyber realm necessitates a degree of collaboration and governments being aware of the issue by its very nature. Some commentators compare internet to the wild west, however unlike the early days of nuclear power, cyberspace includes a variety of private and public governance sectors. Certain technical Internet protocol standards are established (or not) by agreement among engineers in the nonprofit Internet Engineering Task Force. Despite the existence of certain cooperative frameworks, such as the European Convention on Cyber Crime, they are still weak, and governments continue to concentrate on the zero-sum rather than positive-sum aspects of these games.

Simultaneously, some of these problems may be undergoing some autonomous learning. For example, Russia and China have refused to join the Cybercrime Convention and have sheltered behind plausible deniability by encouraging “patriotic hackers” to get into their systems. However, if the costs outweigh the advantages, their views may shift. “Russian cyber-criminals no longer obey hands-off regulations when it comes to homeland targets, and Russian authorities are starting to abandon the laissez-faire attitude, and China is suffering increasing cyber-crime expenses on its own,” for example. Independent learning, as in the nuclear realm, may lay the basis for subsequent active collaboration. Crises aren't the only way to learn, of course. Players may learn the importance of collaboration in maximizing their payoffs over time by playing iterated games of prisoner's dilemma in circumstances with a long shadow of the future. Early steps in nuclear cooperation paved the way for subsequent steps without necessitating a shift in the overall relationship's competitive character. Informal "Track Two" discussions, such as the Pugwash Conferences, bolstered these government actions. There have been no significant cyber-crises to far, but denial-of-service assaults on Estonia and Georgia, as well as the Stuxnet strike on Iran, hint to what is to come. As previously said, some experts believe that markets will not adequately price security in the private sector unless there is a visible catastrophe. Other types of learning, however, are possible. In the case of industrial espionage, for example, China has little incentives to limit its conduct since the advantages greatly outweigh the risks. Spying has been practiced since the dawn of time and does not contravene any specific rules of international law. Nonetheless, governments have created rules of the road to restrict espionage and participated in tit-for-tat retribution patterns to provide an incentive for collaboration. While binding treaties prohibiting governments from engaging in espionage are impossible to conceive, a process of iterations (tit for tat) that establishes rules of the road that minimize harm in practice is feasible.

To prevent "defection lock-in," which may lead to unintended escalation, it's helpful to participate in conversations that might lead to shared views of redlines, if not completely accepted standards, as happened during the Cuban missile crisis. Discussion helps to put particular distinctions into a larger perspective a shadow of the future.Concerns about crisis management and accidents prompted the establishment of the hotline, as well as the early 1970s Accidents Measures and Incidents at Sea seminars. Similarly, the two sides found a shared interest and started cooperating on nonproliferation problems in the mid-1960s, long before bilateral arms control agreements on matters of arms race stability in the 1970s. Nuclear learning and agreements progressed at various speeds in different sectors, contrary to the popular belief that nothing is resolved in a contract until everything is settled. It's probable that the cyber domain will be similar. As we've seen, there are already certain agreements and organizations in place that deal with the fundamentals of Internet operation, such as technical standards and names and addresses, as well as the beginnings of a normative framework for cybercrime.

However, it is probable that agreement on difficult topics like as cyber incursions for espionage and war preparation would take longer. Nonetheless, the inability to envision a broad consensus does not have to stymie progress on specific problems. Indeed, breaking down word assaults into individual acts that may be handled independently may provide the greatest chance of success. As previously stated, the military may be under civilian authority while maintaining its own operational culture. It is tasked with entertaining worst-case scenarios due to its nature and purpose. It does not necessarily learn the same lessons as its civilian counterparts at the same pace. Early in the SALT negotiations, Soviet military officials protested about the Americans' practice of sharing classified military material in front of the Soviet delegation's civilian members. The exercise resulted in increased communication on the Soviet side. At the same time, Soviet military commanders lacked a basic grasp of American institutions and the function of Congress in relation to nuclear matters. Their participation in armament negotiations aided in the development of a more sophisticated generation of younger leaders. “It's difficult to address the topic with the military,” Foreign Minister Andrei Gromyko said, “but the more interaction they have with the Americans, the simpler it will be to transform our troops into something more than martinets.”

CONCLUSION AND IMPLICATION

If taken too literally, historical parallels may be hazardous, because the distinctions between nuclear and cyber technology are vast. Cyberspace is fresh and dynamic; much as nuclear technology was when it was first developed. When we consider how lengthy and difficult it was to create a nuclear strategy, much alone worldwide nuclear cooperation, it may assist to put the challenges of creating a cyber-security strategy into perspective, especially the element of state collaboration. Nuclear education was sluggish, halting, and insufficient. The intellectual and political rivalry between the United States and the Soviet Union was much more intense than it is now between the United States and Russia or the United States and China. The partnership has much fewer positive threads of dependency. Despite the intensity of the zero-sum game, rules of the road and cooperative agreements were developed to assist maintain the parallel positive-sum game. The good news is that this is the case. The bad news is that cyber technology provides nonstate actors much more power than nuclear technology, and the dangers they represent are certain to grow. The cyber domain's transnational, multifactor games raise a new set of issues about what national security means. National and unilateral security responses, focusing on cleanliness, redundancy, and resilience, are some of the most significant security responses. However, it is probable that major countries will eventually realize that cooperation against nonstate actors' insecurity would need a higher priority in attention. At this point in cyber technological development, the globe is a long way from such a reaction. However, such reactions did not emerge until the third decade of the nuclear age. The World Wide Web has only been around for two decades.

REFERENCES

1. T. Rid, “Cyber War Will Not Take Place,” *J. Strateg. Stud.*, 2012, doi: 10.1080/01402390.2011.608939.

2. T. J. Junio, “How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate,” *J. Strateg. Stud.*, 2013, doi: 10.1080/01402390.2012.739561.

3. M. Sleat, “Just cyber war?: Casus belli, information ethics, and the human perspective,” *Rev. Int. Stud.*, 2018, doi: 10.1017/S026021051700047X.

4. M. Durante, “Violence, Just Cyber War and Information,” *Philos. Technol.*, 2015, doi: 10.1007/s13347-014-0176-5.

5. M. Robinson, K. Jones, and H. Janicke, “Cyber warfare: Issues and challenges,” *Comput. Secur.*, 2015, doi: 10.1016/j.cose.2014.11.007.

6. N. Kshetri, “Pattern of global cyber war and crime: A conceptual framework,” *J. Int. Manag.*, 2005, doi: 10.1016/j.intman.2005.09.009.

7. P. Dombrowski and C. Demchak, “Cyber War, Cybered Conflict, and the Maritime Domain,” *Nav. War Coll. Rev.*, 2014.

8. B. K. Mishra and A. Prajapati, “Modelling and Simulation: Cyber War,” *Procedia Technol.*, 2013, doi: 10.1016/j.protcy.2013.12.447.

9. J. Andress and S. Winterfeld, “Chapter 16 - The Future of Cyber War,” *Cyber Warf. (Second Ed.*, 2014.

10. A. Sharma, “Cyber wars: A paradigm shift from means to ends,” 2009, doi: 10.3233/978-1-60750-060-5-3.