IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, 2022

CYBER ATTACK AN INVISIBLE WAR AGAINST NATIONS: ISSUES & OPTIONS

Dr. S. P. Srivastava*

Professor, Department of Law and Governance, Central University of South Bihar, Gaya, India

Abstract

the Internet has provided a new delivery mechanism that can increase the speed, scale, and power of an attack on the national security and integrity of the nation. The threat is so potent that its impact is horrible than any act of terrorism. Cyber warfare attacker affect national critical infrastructures, including everything from elections to electricity. This paper intends to examine the intensity of threat relating to cyber attacks against the nation. It also evaluates the countries policy as well as the technological challenges in addressing threat. The researcher summed up that aalthough the government can play a key role in protecting such systems (e.g., through the development of policies, standards, and law enforcement), it can do little without support technological infrastructure and global cooperation.

Key Words: Cyber warfare, Reasons for cyber-attack, sabotage of data, Common Vulnerabilities and Exposures (CVE), and Lisbon and cyber security

I. BACKGROUND

A cyber-attack against the nation is known as cyber warfare and it is not an end in itself, but a powerful means to a wide variety of ends, from propaganda to espionage, from denial of service to the destruction of critical infrastructure. Due to these attacks the nature of a national security threat has not changed, but the Internet has provided a new delivery mechanism that can increase the speed, scale, impact and power of an attack.[1] In 1948, Hans Morgenthau wrote that national security depends on the integrity of a nation's borders and its institutions. Even, in 2011, military invasion and terrorist attack remain the most certain way to threaten the security of an adversary. However, entry of cyber warfare player has changed the border of protection it is no longer the outskirt of the geographical territory, the attacker target national critical infrastructures, including everything from elections to electricity, whatever is connected with computer system and network thereto. National security planners will also have to worry about invisible cyber-attacker who are unknown enemy to a country without any face targeting the country without human intervention with spider software, malware and trojan attacks on the infrastructure and facilities of the country.[2] Cyber-attacks may evolve from a corollary of real-world disputes to play a lead role in future conflicts.[3] Cyber-attacks raise issues of growing national as well international interest and concern. Cyber-attacks can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the

* Professor, Department of Law and Governance, Central University of South Bihar, Gaya, India. The author may be contacted at sanjayprakash@cusb.ac.in

[1] Kenneth Geers, *Strategic Cyber Security*, 2011, NATO Cooperative Cyber Defence Centre of Excellence, P. 9.

[2] *Id.* at 10.

[3] *Id.* at 9.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, 2022

same. Some major problems encountered with cyber attacks, in particular, are the difficulty in determining the origin and nature of the attack and in assessing the damage incurred. As the existing technology with the attacker have equipped them to use proxy server of the different destination and may initially mislead the whole preventive effort.

II. CYBER ATTACKS- CONCEPT

Cyber-attack, for the purposes of this discussion, is the deliberate disruption or corruption by one state of a system of interest to another state or it could be sponsored by one state without the knowledge of that state actual government. The former state will be referred to as the attacker; the latter state will be referred to as the target. Some potential cyber targets are government systems and some are private. Severe attacks on them are likely to get the public's attention.

The defence of private systems is largely in private hands. Although the government can play a key indirect role in protecting such systems (e.g., through the development of policies, standards, and law enforcement), it can do little directly. The government has no privileged insight into specific vulnerabilities of private systems, and there is little evidence that private system owners are interested in telling it.

The difficulty in a conflict between nation states where cyber attacks are used arises when the military methods are not used in kinetic terms, but the damage is achieved by cyber attacks. Although the consequences could be very serious, but attribution shall be very difficult. A long discussion has been going on how to solve the attribution issue in a cyber attack. So far we have no clear roadmap of how this problem could be tackled during a conflict. Although the forensics analysis will show the original sources, and lead to certain people in certain nationalities or equipment, during the conflict when you try to retaliate you will not have time to figure out the exact attack chain. Additionally, nation states or state sponsored actors could use the actors on territories without proper law enforcement, with weak government structures and non-existent national cyber monitoring systems. Lawless "cyber heavens" exist and this is a known fact for nation states as well as for organised crime and the terrorists.

Another category of vulnerability in cyberspace includes economic actors, industries or sectors that are attacked for political reasons. Although the majority of attacks at this level are carried out for economic gains and with criminal motivations, the trend to attack civilian infrastructure during political conflicts will grow and industries might find themselves at an extremely vulnerable position while attacked by state sponsored actors with considerable resources.

III. INTENTION BEHIND CYBER ATTACK

There are numerous reasons for targeted cyber attacks. It may be government operated or may be by non-state actors. If we refer the past experiences, it could be clubbed into following categories. The first type of attack targets the confidentiality of data. It encompasses any unauthorized acquisition of information, including via "traffic analysis," in which an attacker infers communication content merely by observing communication patterns. Because global network connectivity is currently well ahead of global and local network security, it can be easy for hackers to steal enormous amounts of sensitive information. For example, in 2009 a Canadian research group called Information Warfare Monitor revealed the existence of "GhostNet," a cyber espionage network of over 1,000

compromised computers in 103 countries that targeted diplomatic, political, economic, and military information.

The second type of attack targets the integrity of information. This includes the "sabotage" of data for criminal, political, or military purposes. Cyber criminals have been known to encrypt the data on a victim's hard drive and then demand a ransom payment in exchange for the decryption key. Some countries with poor human rights records have been accused of editing the email and blog entries of their citizens.

The third type of attack targets the availability of computers or information resources. The goal here is to prevent authorized users from gaining access to the systems or data they require to perform certain tasks. This is commonly referred to as a denial-of-service (DoS) and encompasses a wide range of malware, network traffic, or physical attacks on computers, databases, and the networks that connect them.

Fourth type of attack targets to deface websites, destroy data, interrupt functioning of information networks with a goal to damage military capabilities and economy.

Fifth type is intended to affect the economic competencies of the enemy nations when attacker targets infrastructural base including electricity, water supply and air services.

Lastly, it has been sometime used an intention to create confusion among by intrusion into the system of two friend nation attacking each other strategic location in a way that gives impression in primary investigation as if the attacker country is its friend.

IV. ISSUES UNDERLINED WITH CYBER ATTACKS

In cyber conflict, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbour in cyberspace. Hardware, software, and bandwidth form the landscape, not mountains, valleys, or waterways. The most powerful weapons are not based on strength, but logic and innovation.[4] Connectivity is currently well ahead of security, and this makes the Internet, and Internet users, vulnerable to attack. There are not only more devices connected to the Internet every day, but there are dozens of additions to the Common Vulnerabilities and Exposures (CVE) database each month. These combine to create what hackers call the expanding "attack surface." Hackers tend to be creative people, and they are able to exploit such complexity to find ways to read, delete, and/or modify information without proper authorization.

A couple of years ago, the Central Intelligence Agency (CIA) of USA were identifying Russia and China[5] specifically as possible cyber threats. Today, U.S. officials indicate that more than 20 countries have various kinds of information operations (IO).[6]

---

[4] *Ibid.*

[5] In 2007 and 2008, China was publicly accused of hacking into government facilities by officials in Australia, France,Germany, India, Japan, New Zealand, South Korea, and the UK. See, Indrajit Basu,."India Faces Cyber Challenge From China".
http://www.upiasiaonline.com/Security/2008/05/09/india_faces_cyber_challenge_from_china/5587/.

[6] General Alexander of US has warned Congress that policy directives and legal controls over digital combat are outdated and have failed to keep pace with the military's technical capabilities". He has also stressed that computer network warfare is evolving so rapidly that there is a gap between the military's technical capabilities and legal controls over digital combat and what he calls a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."

Cyberspace presents us with new vulnerabilities[7] that exhibit a risk unlike anything that we have experienced up until this point. This cyber attacks is not against the particular state by specific states.[8] Moreover, this cyberwar is not limited to government networks, computers, and computer systems.[9] A very unique aspect of cyberspace is that vulnerability is strictly connected to how well-developed and advanced a country is at information technology. Obviously this means that the most vulnerable countries are the ones that have grown to depend on IT in almost every aspect of their societies. Cyber attacks are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities.

"If I went and bombed a power station of any nation state that would be an act of war. If I went on to the net and took out a power station, is that an act of war? One could argue that it was.

"If someone bombed the electric grid in our country and we saw the bombers coming in it would clearly be an act of war. But If the same country uses sophisticated computers to knock out our electricity grid, whether it is an act of war or not, yet not decided. However, this becomes complicated when the identity of country and individual is not certain. Moreover till today majority of the communication in cyber space is done under packet switching technology. Where data is transferred through routers whatever way is free through IP/TCP mode. Further, feasibility of cloning of sim of data card also poses another level of danger that many a time act may be performed by an individual or group who is also declared criminal by that state from where the act was committed.

The problem with cyberspace is that attribution is extremely difficult. It's almost impossible to do it in terms of evidence that would be necessary in a court of law.

In 2011, an attacker's most important advantage remains a degree of anonymity. Smart hackers hide within the international, maze-like architecture of the Internet. They route attacks through countries with which a victim's government has poor diplomatic relations or no law enforcement cooperation. In theory, even a major cyber conflict could be fought against an unknown adversary.[10] According to Cyber Security Operations Centre (CSOC of UK), one of the problems hampering the prevention of cyber attacks is that an internationally agreed definition of cyber warfare remains elusive, with state actors making increasing use of hired criminals and 'hacktivists' to carry out deniable cyber attacks on their behalf. But it is important to remember that a digital attack against any country causing even minor damage would have a "catastrophic" effect on public confidence in the government.

---

[7] On a single day in 2008, the Pentagon was "attacked" electronically six million times by people seeking access. these attacks reportedly disrupted an internal e-mail system for two days. *See,* Lieutenant Colonel Patrick W. Franzese, "Sovereignty In Cyberspace: Can It Exist?", *The Air Force Law Review,* Vol. 64, 2009.

[8] In Britain, for example, e-mail across most, if not all, of the military was shut down in January 2009. In the summer of 2008, Canadian researchers discovered a large electronic spying operation that had infiltrated at least 1,295 computers in 103 countries—including many belonging to embassies, foreign ministries and other government offices—and stolen documents from hundreds of government and private offices. John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES.COM, Mar. 29, 2009 , quoted from Lieutenant Colonel Patrick W. Franzese, "Sovereignty In Cyberspace: Can It Exist?", *The Air Force Law Review,* Vol. 64, 2009, p. 3.

[9] Lieutenant Colonel Patrick W. Franzese, "Sovereignty In Cyberspace: Can It Exist?", *The Air Force Law Review,* Vol. 64, 2009, p. 2.

[10] Supra Note 1, p. 11.

Four things at this stage are important as initial premise with regard to cyber attacks. First, Cyber attacks are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Second, Policy directives and legal controls over digital combat are outdated. Third, every nation has to accept that currently there is a gap between the representative government technical capabilities and legal controls. Lastly, Individual nation step will not be sufficient step to minimize the imminent threat effect as today there are many non-state actors are working towards destabilising democratic setup without any state support and even working from many territories in concerted manner.

V. INDIA'S SECURITY AND CYBER ATTACK

Cyber attacks pose more than a theoretical challenge to the Indian government day-to-day national security agenda due to the intrusions and web defacements experienced after New Delhi's nuclear weapons test[11] and in the confrontation with Pakistan over Kashmir.[12] Recently a 'technical snag' had hit operations at the state-of-the-art T3 terminal at Indira Gandhi International Airport (IGIA). It now turns out it was caused by a "malicious code" sent from a remote location to breach the security at the airport. A hunt has been launched to nab the perpetrator with the CBI registering a case under the IT Act and IPC. Investigators say that the "malicious code" was in the form of "attack scripts", which means a programme was written by an expert to exploit the system's security weakness.[13]

According to a 2003 account in
The Hindu, for more than two years the hacker war between India and Pakistan has been intensifying, leading to the defacement of hundreds of websites on either side. "Earlier this year, newspaper reports had indicated that an unnamed virus launched by a secretive Indian hacker group had rendered 200 Pakistani websites inaccessible for several days and erased the hard disks of scores of computer [sic] in the Pakistani Government as well as the private sector in that country.[14]

Further it was reported that India's lone uranium enrichment facility at Rattehalli, near Mysore, may become the target of the gravest act of cyberwar against India to date, attacking no less than its strategic nuclear programme, sources in the Indian hacker/cyberwarfare community warned. The sources said computers at the Rattehalli facility, euphemistically called Rare Materials Plant (RMP), were possibly infected by the deadly Stuxnet, or a Stuxnet-derived malware, as a precursor to an attack to destroy thousands of centrifuges installed there.[15] One source in the rarefied cyberwarrior community said a hostile foreign

[11] On June 7, 1998, for example, an anti-nuclear group "Milw0rm" reportedly hacked into the Bhaba Atomic Research Center (BARC) network to protest India's nuclear tests.
[12] Charles G. Billo and Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States,* Institute For Security Technology Studies At Dartmouth College, 2004, p. 9.
[13] Rahul Tripathi, "Cyber attack led to IGI shutdown", Sunday 25, 2011.
www.indianexpress.com.
[14] G. Anand, "Indo-Pak Hacker War Comes Here Too," *The Hindu*, June 9, 2003.
[15] S. Raghotam, "Cyber attack on key N-facility in Mysore?", *The Asian Age*, 13 Dec. 2011.

intelligence agency or rogue agents within it had infected RMP's islanded computers — which run the plant's operations and are not connected to the Internet or any other network.[16] China has a staggering $55 million annual budget pumped into the devious science of strategic hacking and India is clearly its undisputed biggest enemy. Hacking is institutionalised in China. Virus-writing is taught in Chinese military schools. The art of hacking is very much a part of training imparted to a growing army of about 10,000 cyber soldiers. Chinese hackers are known to function as a covert arm of the Chinese navy. And like Pakistani jihadis, the Chinese government can always plausibly deny their existence.

The Red Hackers Alliance, the fifth largest hacker group in the world, is known to render services directly to the Chinese government. With the Alliance at its disposal, Beijing stays on the cutting edge of hacking techniques. Chinese hacking force uses malware, spyware, key loggers, trojans, bots and malicious code generators to break into Indian computers, copy documents, ex-filtrate sensitive material and bug classified correspondence. Without a dedicated Indian cyber-security organisation, this country will remain a sitting duck.

In India the Ministry of Technology and the Central Bureau for Investigation have developed a diverse national strategy to protect India's infrastructures. This strategy recommends "involving assistance from software industries" where ever it is urgent and necessary. In addition, the U.S. and India have set up a Cyber Security Forum to provide a conduit for an exchange of information on cyber threats. The forum fosters bilateral discussions on civilian and military infrastructure protection, legal cooperation and law enforcement, security standards, and research and development.[17] However, the initiatives taken so far are not sufficient to address the intensity of the threat as unless a cooperative ground zero monitoring mechanism as a preventive system shall not be developed all efforts shall be a veil of ignorance.

VI. INTERNATIONAL LAW AND CYBER ATTACKS

When does a cyberattack constitute "use of force" under Article 2(4) of the United Nations (UN) Charter? When does a cyberattack constitute an "armed attack" under Article 51 of the UN Charter? When can a state respond in self-defence with a cyberattack of its own? When can a state respond in self-defence with physical force to a cyberattack? And what is the appropriate, proportional response to a cyberattack?[18] Unfortunately, no consensus has developed in answering these questions. More troubling, various commentators still hold widely divergent views on basic, fundamental questions. For example, they cannot even agree on a framework when addressing the question of when a cyberattack constitutes an act of war, armed attack or use of force ("act of war"). Some believe that for a cyberattack to constitute an act of war, it must "accompany a military offensive in the real world.[19]

The only substantial international legal document developed to address issues related to cyberspace is the European Union's Convention on Cybercrime10(Cybercrime Convention).

---

[16] *Ibid.*

[17] "Hackers Take Kashmir Dispute to Cyberspace," *Jane's Intelligence Review*, October 1, 2002.

[18] *See*, *e.g.*, Walter Gary Sharp, Sr., Cyberspace And The Use Of Force (Aegis Res. Corp. 1999); Thomas C. Wingfield, The Law Of Information Conflict: National Security Law In Cyberspace (Aegis Res. Corp. 2000). These two books deliberate on such issues.

[19] "Marching Off to Cyberwar", Economist, Dec. 4, 2008, quoted from Lieutenant Colonel Patrick W. Franzese, "Sovereignty In Cyberspace: Can It Exist?", *The Air Force Law Review,* Vol. 64, 2009, p6.

While the Cybercrime Convention does not address cyberspace attacks as possible acts of war and instead focuses on criminal acts, it does help establish a framework for a new methodology of analyzing cyberspace attacks. Instead of focusing on the end result of a cyberspace event, the effects, and trying to determine whether such an act is a use of force or armed attack under international law, a criminal law methodology places increased emphasis on the genesis of a cyberspace event.[20]

At the 2010 NATO Summit in Lisbon, twenty-eight world leaders declared that cyber attacks now threaten international prosperity, security, and stability. In the future the consequences of a cyber attack may rise because the threat will affect national critical infrastructures of every kind. Goals such as the security of national critical infrastructures and strategies like military deterrence and arms control demand a greater appreciation for the capabilities and challenges of computer scientists, who fight their battles on the front lines of cryptography, intrusion detection, reverse engineering, and other highly technical disciplines.

International Telcommunications Union secretary general Hamadoun Toure gave his warning at a World Economic Forum debate where experts said nations must now consider when a cyber attack becomes a declaration of war.

The world needs a treaty to prevent cyber attacks becoming an all-out war, the head of the main UN communications and technology agency warned. A cyber war would be worse than a tsunami -- a catastrophe," the UN official said, highlighting examples such as attacks on Estonia last year. He proposed an international accord, adding: "The framework would look like a peace treaty before a war."

On 30 July 2010, the United Nations Secretary-General transmitted the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ("Group").

V.I. OPTION FOR STATES

Any state can unilaterally declare that a cyber attack (of certain characteristics) is an act of war. But such a declaration may be found reasonable by some states as an act that they may find reasonable, legitimate, and actionable, while others may not agree. However, if the state responded to a cyber attack by retaliating, those skeptical of the claim might regard the response as illegitimate if it used a different modality from that of the attack itself.

Next issue is When does a cyber-attack that may or may not be sponsored and supported by another nation cross the line and become an official act of war? At what point should a state become responsible for non-state actors within its territory? And for nations reliant on the Internet and other ICT modalities that are the primary victims of these attacks, what should the rules of engagement be when faced with the onslaught of rival countries determined to probe weaknesses and wreak havoc on other countries' critical information infrastructures? Is it productive for a nation to adopt a pro-active approach to cyber warfare?

VI. II. LIABILITY OF STATES

What should the rules of engagement be for nations to take with respect to taking action via law or technology or other measures (trade embargoes, for example) against other countries

[20] Major Graham H. Todd, "Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition" *The Air Force Law Review,* Vol. 64, 2009, p. 70.

that attack or spy through cyberspace? Is it technologically feasible to do so to protect private sector and/or critical information infrastructure networks? Would it be effective in terms of national interest to do so rather than to engage in conflict in cyberspace or traditional warfare? Does a democracy have to wait until it is attacked by foreign actors before it may take aggressive measures to protect its critical information infrastructures?

However in 2011, an attacker's most important advantage remains a degree of anonymity. Smart hackers hide within the international, maze-like architecture of the Internet. They route attacks through countries with which a victim's government has poor diplomatic relations or no law enforcement cooperation. In theory, even a major cyber conflict could be fought against an unknown adversary. Technologically we are lagging behind the intruder and sometimes helpless.

V.III. CONFLICTS OF JURISDICTION

Law enforcement and counterintelligence investigations suffer from the fact that the Internet is an international entity, and jurisdiction ends every time a telecommunications cable crosses a border. In the case of a state-sponsored cyber attack, international cooperation is naturally non-existent.

If more than one State asserts jurisdiction over a particular cyber attack or a dispute when conflict may involve more than one State.

VI. Conclusion

We need to remember that Cyber defence suffers from the fact that traditional security skills are of marginal help in defending computer networks, and it is difficult to retain personnel with marketable technical expertise. Talented computer scientists prefer more exciting, higher-paying positions elsewhere. Moreover, the world's growing dependence on a powerful but vulnerable Internet – combined with the disruptive capabilities of cyber attackers – now threatens national and international security. Only individual effort of technology and legal control of any nation does not have solution to this issue. Here we need to move a plan of an international treaty as suggested by UN. A successful cyber attack against public services would have a catastrophic impact on public confidence in the government, even if the actual damage caused by the attack were minimal. Most cyber attacks are likely to remain difficult to trace to official sources. States are likely to increasingly see the cyber domain as an area in which to wage war... it is difficult to see international agreement on what acts are and are not acceptable in a cyber war. Even if regulation of this kind was to emerge, it is likely that it would make little difference. We can conclude that aalthough the government can play a key role in protecting such systems (e.g., through the development of policies, standards, and law enforcement), it can do little without support technological infrastructure and global cooperation.

Moreover, cyber defence suffers from the fact that traditional security skills are of marginal help in defending computer networks, and it is difficult to retain personnel with marketable technical expertise. Talented computer scientists prefer more exciting, higher-paying positions elsewhere. As a consequence, at the technical level, it can be difficult even knowing whether one is under cyber attack. At the political level, the intangible nature of cyberspace

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, 2022

can make the calculation of victory, defeat, and battle damage a highly subjective undertaking.

Cyber attacks may rise to the level of a national security threat only when an adversary has invested a significant amount of time and effort into a creative and well-timed strike on a critical infrastructure target such as an electrical grid, financial system, air traffic control, etc. This threat can be identified in the following categories:

1. Dedicated and persistent Cyber Space actors such as recreational hackers, corporations seeking a competitive advantage, organized criminals, terrorists, and states.
2. Practice of computer espionage, as well as the subversion of political, economic, and/or non-military information bearing on a nation's capabilities and vulnerabilities.
3. An adversary launches an attack on our forces or infrastructure through computers that are located in a neutral country.
4. The attacks appear to be coming from computers outside the country, but they're being routed to computers that are owned by your persons located in the country of attack, the routers are also in your country.