A NEW AGE OF CYBER WARFARE

Krishan Tuli*

Abstract: *The Internet has intimate with a wide ranging enlargement over the past 20 years, from a little network restricted primarily to the scientific community to a global network that counts over 2 billion users. With enlargement came increasing applications for the web, that fed additional enlargement and still more applications, to incorporate the increase of a cyber economy, money transactions, widespread machine-controlled regulation of key management systems, Associate in Nursing explosion within the sharing and storing of knowledge (including sensitive information), the emergence of latest types of transmission like email, and social networking, among others.*

In addition to those manifold social group edges, the cyber domain, just like the physical, which incorporates multiple money systems, has spawned cyber crime. Storage of sensitive data on networks has born to cyber espionage against governments and cyber economic warfare against businesses. And in periods of crisis and conflict states are subjected to varied forms of cyber attack at each the military science and operational levels of war.

Keywords: *Cyber warfare, Espionage, Economic Security, National Security, Cyber counter-intelligence, sabotage and subversion*

*Assistant Professor, Chandigarh Group of Colleges, Landran, Mohali

INTRODUCTION

Cyber warfare is the most aggressive form of attack by antagonist or rival over the internet. It applies to the state of action which involves the denying internet services to communities or the countries and destroying the critical infrastructure or other facilities. The other use is to attack another country's computer infrastructure as a part of a foray or aggression. Cyber warfare tends to be distinguished from other forms of hostile cyber activity, as cybercrime involves activities like bank accounts raiding; cyber espionage (spying) describes stealing of secrets; in a way cyber warfare tends to describe an assault that affects the national security of the state that is being victimized. In simple words, cyber warfare is Internet-based conflict which involves politically motivated attacks on information and on their systems. These attacks can disable websites and networks, disrupt or disable essential services, steal or alter data and cripple the financial systems.

There are number of example of cyber warfare in action.

- In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2007, the attack on Estonia's internet system by the Russian state.
- Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.
- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.
- Deployment of the Stuxnet worm, which was widely believed to have been used by the US and Israel to attack computer-controlled centrifuges at a uranium enrichment facility in Iran which disrupted the country's nuclear programme.

That is why this subject is very important and has been seriously thought-out not only by the military Intelligence organizations, but also the executive officers at banks, Securities firms, and other companies. Defense and intelligence officials fear that enemy nations, terrorists and criminal groups may carry out cyber warfare assaults against networks like:

1. **The banking system** - stock exchange, logic bombs could cripple the markets and destroy records of transaction, money can be stolen by cracking networks.
2. **Electric utilities in several states and Power plants –** power grids can be knocked out causing local or regional black-outs.
3. **Telephone networks** - can be knocked down.
4. **Air traffic control centers** - plane crashes/collisions can be caused by disabling and creating malfunctions on computer systems and on-board avionics computers.
5. **Trains, subways** - crashes can be caused by mis-routing trains.
6. **Battlefield tanks** - sophisticated computer controls can be crippled.

While the information technology makes our lives more convenient, it makes us more vulnerable. This great dependence on information technology has created a new form of vulnerability for society. Public or private life can be highly disturbed by those who are able to manipulate information technology for illegal purposes.

In this digital age, warfare is no longer limited to military. In the cyber-world, a digital enemy can bypass our military and take down what is near and dear to us. Destroying critical national infrastructure such as automated power plants, stock markets and transportation systems could disable this nation without firing a shot.

It is therefore the clear rewards of information technology have new risks that need to be better understood and managed. A cyber attack could not only disrupt the daily lives, but could also endanger the national and economic security. In cyber warfare one doesn't need fighter planes and billions of dollars to launch an attack. One can pay someone some money to "launch an attack" and it will cost less than mobilizing a tank or aircraft carrier. While the tools we use to protect the systems against these bandits such as firewall are expensive and complicated, the hackers often use tools that are free and simple to operate.

CYBER COUNTER INTELLIGENCE

Cyber counter-intelligence square measure measures to spot, penetrate, or neutralize foreign operations that use cyber suggests that because the primary craft methodology, similarly as foreign intelligence agency assortment efforts that use ancient strategies to measure cyber capabilities and intentions

- On seven April 2009, The Pentagon declared they spent over $100 million within the last six months responding to and repairing injury from cyber attacks and alternative network issues.
- On one April 2009, U.S. lawmakers pushed for the appointment of a White House cyber security "czar" to dramatically intensify U.S. defenses against cyber attacks, crafting proposals that may empower the govt. to line and enforce security standards for personal trade for the primary time.
- On nine Feb 2009, the White House declared that it'll conduct a review of the nation's cyber security to confirm that the central of the US cyber security initiatives a fittingly integrated, resourced and coordinated with the US Congress and also the non-public sector.
- In the wake of the 2007 terrorist act waged against Baltic State, international organization established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in capital of Estonia, Estonia, so as to reinforce the organization's cyber defence capability. The middle was formally established on fourteen might 2008, and it received full certification by international organization and earned the standing of International Military Organization on twenty eight October 2008. Since Baltic State has LED international efforts to fight crime, the US Federal Bureau of Investigation says it'll for good base a pc crime professional in Baltic State in 2009 to assist fight international threats against supercomputer systems.

One of the toughest problems in cyber intelligence operation is that the downside of "Attribution". Not like typical warfare, working out WHO is behind Associate in nursing attack will be terribly troublesome. However Defense Secretary Leon Panetta has claimed that the US has the aptitude to trace attacks back to their sources and hold the attackers "accountable".

CONTROVERSY OVER TERMS

There is dialogue on whether or not the term "cyberwarfare" is correct. In Gregorian calendar month 2011, for occurrence, the Journal of Strategic Studies, a number one journal in this field, printed an editorial by Thomas Rid, "Cyber War won't happen." Associate act of cyber war would have to be compelled to be probably fatal, instrumental, and political. Then not one single cyber offense on record constitutes associate act of war on its own.

Instead, all politically driven cyber attacks, Rid argued, just refined versions of 3 activities that are as recent as warfare itself: sabotage, espionage, and subversion.

Howard Schmidt national leader, associate cyber security professional, argued in March 2010 that "there is not any Cyber war. I feel that's a terrible figure. I think that's a terrible conception. There aren't any winners in this atmosphere." Web Scholar, Mark Graham has equally pointed to the very fact that the 'cyber' figure is associate inherently mechanism through that conflict and war may be understood. Alternative consultants, however, believe that this kind of activity already constitutes a war. The warfare analogy is usually seen meant to encourage a military response once that's not essentially applicable. Ron Deibert, of Canada's subject work, has warned of a "militarization of Internet or in deeper a cyberspace."

The European cyber security professional Sandro Gaycken argued for a middle position. He considers cyber terrorism from a legal perspective associate unlikely state of affairs, due to the explanations lined out by Rid however state totally different from a strategic purpose of vision. States have to be compelled to contemplate military-led cyber operations a horny activity, among and while not war, as they provide an oversized type of low-cost and riskless choices to weaken alternative countries and strengthen their own positions. Thought of from a semi permanent, geopolitics perspective, cyber offensive operations will cripple whole economies, modification dogmas, agitate conflicts among or among states, cut back their military potency and equalize the capacities of advanced nations to that of low-tech nations, and use access to their essential infrastructures to blackmail them.

VARIOUS INCIDENTS

- On twenty one Gregorian calendar month (November) 2011, it had been wide reportable within the U.S. media that a hacker had destroyed a pump at the Curran-Gardner administrative division Public Water District in Illinois. However, it later curved that this info wasn't solely false, however had been unsuitably leaked from the Illinois Statewide Terrorism and Intelligence Center.
- On half-dozen Oct 2011, it had been declared that Creech AFB's drone and Predator fleet's command and management knowledge stream had been keylogged, resisting all makes an attempt to reverse the exploit, for the past time period. The Air Force

issued a press release that the virus had "posed no threat to our operational mission".

- In July 2011, the South Korean company SK Communications was hacked, leading to the thieving of the private details (including names, phone numbers, home and email addresses and resident registration numbers) of up to thirty five million individuals. A trojaned code update was accustomed gain access to the SK Communications network. Links exist between this hack and different malicious activity and it's believed to be a part of a broader, cooperative hacking effort.
- Operation Shady RAT is associate degree current series of cyber attacks beginning mid-2006, reportable by web security company McAfee in August 2011. The attacks have hit a minimum of seventy two organizations as well as governments and defense contractors.
- On four December 2010, a gaggle line of work itself the Islamic Republic of Pakistan Cyber Army hacked the web site of India's high investigation agency, the Central Bureau of Investigation (CBI). The National scientific discipline Center (NIC) has begun associate degree inquiry.
- On twenty six Gregorian calendar month 2010, a gaggle line of work itself the Indian Cyber Army hacked the websites belong to the Islamic Republic of Pakistan Army and therefore the others belong to completely different ministries, as well as the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Islamic Republic of Pakistan Computer Bureau, Council of Muslim Ideology, etc. The attack was done as a revenge for the urban center terrorist attacks.
- In Oct 2010, Iain Lobban, the director of the Government Communications Headquarters (GCHQ), said Britain faces a "real and credible" threat from cyber attacks by hostile states and criminals and government systems area unit targeted one thousand times every month, such attacks vulnerable Britain's economic future, and a few countries were already victimization cyber assaults to place pressure on different nations.
- In September 2010, Iran nation was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. The worm is claimed to be

the foremost advanced piece of malware ever discovered and considerably will increase the profile of cyberwarfare.

- In July 2009, there have been a series of coordinated denial of service attacks against major government, news media, and monetary websites in Republic of Korea and therefore the US. While several thought that attack was directed by North Korea, one scientist copied the attacks to the UK.
- Russian, South Ossetian, Georgian and Azerbaijani sites were attacked by hackers throughout the 2008 South Ossetia War.
- In 2007 the website of the Kyrgyz Central committee was damaged throughout its election. The message left on website browse "This site has been hacked by Dream of Estonian organization". Throughout the election campaigns and riots preceding the election, there have been cases of Denial-of-service attacks against the Kyrgyz ISPs.
- In September 2007, Israel administered associate degree airstrike on Syria dubbed Operation Orchard. U.S. business and military sources speculated that the Israelis might have used cyberwarfare to permit their planes to pass unobserved by microwave radar into Syria.
- In April 2007, Republic of Estonia came beneath cyber attack within the wake of relocation of the Bronze Soldier of port. The most important a part of the attacks were coming back from Russia and from official servers of the authorities of Russia. Within the attack, ministries, banks, and media were targeted.
- In the 2006 war against Revolutionary Justice Organization, Israel alleges that cyber-warfare was a part of the conflict, wherever the Israel Defense Forces (IDF) intelligence estimates many countries within the geographic region used Russian hackers and scientists to control on their behalf. As a result, Israel connected growing importance to cyber-tactics, and became, at the side of the U.S., France and some of different nations, concerned in cyber-war coming up with several international sophisticated corporations area unit currently locating analysis and development operations in Israel, wherever native hires area unit typically veterans of the IDF's elite computer units. Richard A. Clarke adds that "our Israeli friends have learned a factor or 2 from the programs we've been acting on for quite twenty years.

CONCLUSIONS

Looking at the conventions of land warfare and therefore the principles of war that represent strategy and techniques it becomes obvious that there's a considerable disconnect once considering cyberwarfare. In fact, there are unit those that merely say it doesn't exist. A disconnect between the legal, moral, and moral issues perhaps: the conventions for land warfare typically refer to the laws of land war, as within the convention. But in respondent the analysis question, the author determined to focus totally on the second a part of the analysis question to answer however the techniques and ideas for generalized approaches to situational awareness might be accomplished.

In ignoring the first a part of what constitutes associate degree attack underneath the law of war, we have a tendency to talk about a spread of attacks. The discussion among this paper answers the concept of attack centered on the kinds of attack that were potential. A part of this can be that perfidy and jus in bello in information security merely has not been delineate compactly. Merely place the utilization of the civilian network that is sort of a demand puts the complete first a part of the first analysis question into a quandary. The civilian network element as delineate adds potential perfidy to every attack and a virtually defacto risk of violations of the laws of war.

REFERENCES

1. T. K. Adams, “Radical destabilizing effects of new technologies,” Parameters, vol. 1998, pp. 99-111, 1998.
2. K. B. Alexander, “Warfi ghting in cyberspace,” Joint Forces Quarterly, vol. 3rd Quarter, pp. 58-61, 2007.
3. C. Dunlap, “21st century land warfare: Four dangerous myths,” Parameters, vol. 1997, pp. 27-37, 1997.
4. J. Arquilla and D. Ronfeldt, Networks and netwars: The future of terror, crime, and militancy. Santa Monica, CA: RAND, 2001.
5. B. Panda and J. Giordano, “Defensive information warfare,” Communications of the ACM, vol. 42.
6. U. S. Army, “FM 3.0 Operations,” T. U. S. Army, Ed., ed. Washington DC, 2001, p. 104.
7. P. Murdock, “Principles of war on the network-centric battlefi eld: Mass and economy of force,” Parameters, vol. 2002, pp. 86-95, 2002.