International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

Emerging Cyber Threats and the Challenges Associated with them

Rohit Sharma[1], Dr. Mona Purohit[2]

[1]Department of Cyber Law & Information Security, Barkatullah University Bhopal, INDIA
[2]Department of Legal Studies and Research, Barkatullah University Bhopal, INDIA

Abstract- *In this cyber era the internet on one side is making the world smarter and faster with the concepts such as smart grids, smart phones, smart vehicles and smart cities, and on the other side the same internet is letting the world on the verge of destruction by making it exposed and vulnerable against the cyber-threats. As the cyber attacks are becoming more and more advance and sophisticate the security and legal challenges arising from them also become more complex.*

Keywords: **cyber-threats, cyber-attacks, ransomware, security challenges, legal issues in cyberspace**

1. INTRODUCTION

"The Internet is the crime scene of the 21st Century"[1]. This one statement given by Cyrus Vance Jr., the District Attorney of Manhattan, New York, USA is enough to understand the grave problems creating by cyber threats in the world.

Crimes are not new to the world. In fact, their history dated back almost to the origin of mankind. Money, power, land, revenge and religion were among the prime reasons for all sorts of crimes and war in which humans have been engaged since ages. 21st century is not anything different than the past centuries. These still remain as the major reasons for the war and crimes, the only difference is that now along with the physical world, the cyber space also becomes the battleground.

This paper presents some of the emerging cyber-threats along with the security and legal issues related to them.

2. EMERGING CYBER-THREATS

In today's world, the internet is no longer an option; it becomes an essential element of our lives. Almost every country in the world understands the power of the internet for its growth and development and therefore to become digitally empowered, governments are also launching new policies and schemes to encourage people for using the internet. But, along with dramatically increase in the use of cyber technology, there has also been exponential growth in the cyber-attacks and cyber-crimes. In this section, major emerging cyber-threats are being discussed, which are as follows:

1. Ransomware
2. Cyber-threats to Satellites
3. Cyber-threats to Nuclear and other weapons
4. Cyberwar

2.1 RANSOMWARE

Ransomware [2] is another type of extortion taking place in cyberspace i.e. type of cyber-extortion. This is a type of malware attack in which the attacker encrypts the device or files present in the device and demands money from the users in order to provide the decryption key. Thus, ransomeware means the malware which demands the ransom in order to release the files or unlock the device. Though ransomeware were present in cyberspace for quite sometimes but since 2016, there has been a storm of ransomware attacks in the world with the biggest one being the WannaCry ransomware [3] attack which spread to over 150 countries. This malware exploited the vulnerability in the Microsoft's Windows and it spread globally affecting the fields like healthcare, automobile, financial and educational institutions etc. it demanded the ransom in the form of bitcoins [4] which is one of the most popular emerging cryptocurrency [5][6].

2.2 CYBER-THREATS TO SATELLITES

Space technology is one field which is fully dependent on computers for its functionalities which in turn makes it highly vulnerable to cyber attacks. Though we never realized but our lives depend a lot more than we usually imagined on the satellites revolving around the earth thousands of miles away from us. Cyber attackers are very well aware of this dependency and therefore any major attack on the satellite system of a nation is enough to bring that nation down on the knees. [7]

2.3 CYBER-THREATS TO NUCLEAR AND OTHER WEAPONS

Nuclear and other weapons of mass destruction are threat to humanity. The peace makers of the world are working continuously to discourage the nation-states to use them even during the major conflicts. In a report (2016) by OEWG to the UN, the growing vulnerability of nuclear weapons to the cyber-attacks is being mentioned [8].

When these weapons are in control of the responsible nation-state, then also they possess a great danger to this world, then one can only imagine the consequence if their control falls into the hands of cyber-attackers[9][10].

2.4 CYBERWAR

Though the cyberwar and the use of cyberwarfare are one of the most talked about concerns of this century but its prediction was already made in the last decade of the 20th century by Arquilla and Ronfeldt in their article "Cyberwar is Coming!" which was published in the year 1993 [11]. Despite being one of the major concerns of the international peace making bodies and several nation states but still there is no universally accepted definition of either cyberwar or cyberwarfare. May be it is because the need of understanding the potential consequences of a cyberwar is seems to be more important than just a focusing on the definition of it.

Although, predicting the exact nature of the cyberwar is not an easy task but two things that are concrete about the cyberwar are: the direct involvement of two or more nation-states and the consequences of the cyberwar would be massively destructive in terms of life and financial losses. This destruction can target the either one or all of the following areas i.e. critical infrastructures, space programs, military, aviation etc. [12]

3. CHALLENGES ASSOCIATED WITH EMERGING CYBER THREATS

With each passing day, the cyber threats are becoming dangerous and sophisticated than ever; hence creating more challenges for security experts and policy makers.

3.1 SECURITY CHALLENGES

There is no doubt that cyber attackers are experts of cyber technology. They are good not only in exploiting the vulnerabilities in the systems but they also know how to use or we should say 'misuse' the advance services and facilities provided by the cyber companies for the benefit of their users. Many security issues that we are facing now are the result of using these strategies by the attackers. The major security challenges are mentioned below:

- The basic structure of the internet itself possesses the biggest security challenge for the experts because when internet was developed, the communication between the computers was the prime motive not the absolute security of the systems and the networks.

- Cyberspace is constantly evolving and so as the cyber threats, therefore to be completely certain about the coming cyber attack and rightly predicting about the attacker and nature of the attack is not possible. This unpredictability and uncertainty about the cyber threats makes the security process more complicated because it is like fighting an unknown enemy.

- Cyberspace is borderless and the cyber attackers are very effectively taking advantage of this to launch the attack from anywhere to anywhere.

- The cyber attackers always go behind the mask to avoid revealing their true identities. To do this, they make use of the same services which are being given to the genuine users for the protection. The techniques such as IP spoofing, use of dynamic IP addresses, VPN services etc. help the attackers to hide their identity and location [13].

- Earlier in case of ransomeware, by tracing back the route of payment, it was possible to track the culprits but with the emergence of cryptocurrencies, tracing and detection is not possible since the cryptocurrencies provides anonymity in the payment process [3].

3.2 LEGAL ISSUES

Every new emerging cyber threat is making the already tangled legal issues more complex. Some of those arising legal issues are been discussed below:

- When the world is living in the fear of cyberwar, the first issues arises is the applicability of "Law of War" (also known as "Law of Armed Conflict or LoAC") in the cyberwar. There are many views on this issue. Some are completely in favor of

applying the LoAC in cyberwar while some are in favor of separate laws. But, most agree on the fact that under 'some circumstances' the LoAC in its current form can be applied to the cyber attacks also. Now which 'circumstances' should come under this category is still a topic of debate [14][15].

- The issue of selecting the mode of counter attack is again a disputable topic whether the current LoAC be applied in cyberwar or separate laws for cyberwar would be adopted. Many suggest to use military attacks and even the Weapons of Mass Destructions (such as nuclear, chemical, biological weapons) in response to the cyber attack of that scale while some argues that in cyberwar the response should remains confined to cyber-attacks only[15].

- Most of times, the cyber attackers go unpunished which in turn encourages other potential attackers to follow their path. The major reasons for this are the hidden identities of the attackers and the issue of attribution. Failing to reveal the real culprits in case of cyber attacks raises the issue of attribution. In all the major cyber attacks of the recent times, many accusations have been made but nobody or no nation has been officially considered responsible for those attacks. This is because most of the times the attackers are group of anonymous hackers which are good in hiding their identities and locations (see section 3.1) so it is difficult to catch them. Under such circumstances, to find out whether a foreign nation-state is responsible for the attack or it was an act of random group of cyber criminals becomes challenging.

- The increment in the occurrence of global ransomware attacks gives birth to another legal complication i.e. the territorial issue which means that when an attack affects about hundreds of countries, then according to which laws or laws of which country, the legal implications should be applied.

4. CONCLUSIONS

With the growing dependency of physical world on cyberspace, now the effects of cyber attacks do not confine only to the cyberspace but they have started to affect our daily lives. As the cyber threats are increasing; cyber security, along with the military security, is also becoming one of the major concerns for the world. The absence of clear international laws on cyberspace and proper security measures are also making the situations challenging. Therefore, there is an urgent need for properly defined international laws and proactive security measures for the cyberspace.

5. REFERENCES

[1.] Joseph Berger. "Access to Details on Wealthy Donors Fueled Theft Ring". The New York Times, 16 December, 2011.

[2.] http://www.nytimes.com/2011/12/17/nyregion/uja-federation-donors-were-targets-in-identity-theft-indictment-says.html?_r=1&scp=1&sq=UJA&st=cse

[3.] Ali, A. (2017). "Ransomware: A research and a personal case study of dealing with this nasty malware". Issues in Informing Science and Information Technology Education, 14, 87-99. http://www.informingscience.org/Publications/3707

[4.] EY Technical intelligence analysis (2017). "Wanna Cry attack". EYG no. 03390-173Gbl

[5.] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Security and Privacy (SP)", IEEE Symposium on (pp. 104-121). IEEE.

[6.] Hileman, D. G., & Rauchs, M. (2017). "2017 Global Cryptocurrency Benchmarking Study".

[7.] Sontakke, K. A., & Ghaisas, A. (2017). "Cryptocurrencies: A Developing Asset Class". International Journal of Business Insights & Transformation, 10(2).

[8.] Livingstone, D. and Lewis, P. (2016), "Space, the Final Frontier for Cybersecurity?", Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecuritylivingstone-lewis.pdf

[9.] United Nations, "Report of the Open Ended Working Group Taking Forward Multilateral Nuclear Disarmament Negotiations", UN document A/71/371, 1 September 2016, para. 55.

[10.] Unal, B. and Lewis, P.(2017). "Cyber Threats and Nuclear Weapons Systems". Research Paper, London: Royal Institute of International Affairs

[11.] Unal, B. and Lewis, P.(2017). "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences". Research Paper, London: Royal Institute of International Affairs,

[12.] https://www.chathamhouse.org/publication/cybersecurity-nuclear-weapons-systems-threats-vulnerabilities-and-consequences.

[13.] Arquilla, J. and Ronfeldt, D. (1993). "Cyberwar is Coming!". Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/reprints/RP223.html.

[14.] SANS Institute (2004) "Information Warfare: Cyber Warfare is the future warfare" Global Information Assurance Certification Paper.

[15.] Radware (2016). "A game of cat and mouse: Dynamic IP address and cyber attacks".

[16.] Hongju Koh, Harold,(2012). "International Law in Cyberspace". Faculty Scholarship Series. Paper 4854.

[17.] http://digitalcommons.law.yale.edu/fss_papers/4854

[18.] Michael Gervais (2012), "Cyber Attacks and the Laws of War", 30 Berkeley J. Int'l Law. 525

[19.] http://scholarship.law.berkeley.edu/bjil/vol30/iss2/6