Study on Cyber Warfare During 2001-2019

1st Ms. Nikita Agarwal
School of Computer Science
MIT World Peace University Pune,

2nd Ms. Pooja Kalambe
School of Computer Science
MIT World Peace University Pune,

3rd Ms. Prachi Ghag
School of Computer Science
MIT World Peace University Pune, India

4th Dr. C. H. Patil
School of Computer Science
MIT World Peace University Pune, India

***Abstract* - The paper defines that cyber Warfare s a vast topic with various subtopics receiving attention from the research community. It's a new type of warfare, merely a new weapon that is merged with the traditional conflict. In this generation of mankind, the arrival and the global expansion of the internet is being proved as the fastest and the most powerful technological revolution. Today we are in the situation where we have to decide which governing laws apply to cyber warfare and how much it really applied. Cyber warfare. During research it seemed critical to understand the current situation and the boundaries that are crossed and cyber warfare.**

Keywords – breach, effected, hacked, operation, deteriorate, targeted. Track III: Cyber Security

I. INTRODUCTION

Cyber warfare refers to the use of technology to launch attacks on nations, governments and citizens, causing comparable harm to actual warfare using weapon. War continues to spread online known as cyberwarfare; the spread of malicious online viruses may be the future of war. The term 'cyberwarfare's different from the term 'cyber war'. Cyber warfare includes techniques, tactics and procedures, which may be involved during a cyber war. The term war inherently refers to a large-scale action, typically over a protracted period and may include objectives seeking to utilize violence or with the aim to kill. A cyber war could accurately describe a protracted period of back-and-forth cyberattacks (including n combination with traditional thing happened where the Abkhaz separatists had conducted war in 1992-1993.The relations between Russia and Georgia began to deteriorate, the reason behind that was the election of Vladimir Putin and Russia in 2000 and a pro-Western power in the Georgia n 2003.This deterioration led to diplomatic crisis by April 2008. The South Ossetian separatists started shelling Georgian villages by 1August 2008, with a response from peacekeepers of Georgia in that area. In the year 1992 a ceasefire agreement was broken by the Artillery attacks of pro-Russian. On 7th August to stop these attacks and restore the orders. To make an end to these attacks and restore order the Georgian Army was sent to the South Ossetian conflict zone.

Before the response from Georgian military, the Russian troops had almost crossed the Russo-Georgian state border and advanced into the South Ossetia conflict zone by 7 August. Georgia was blamed by Russia for "violence against South Ossetia ", because of this a large-scale land, air, sea invasion of Georgia was launched on 8 August with the name "peace enforcement" operation. The Russia and South Ossetia forces fought Georgian forces for many days until the Georgian forces went back. Undisputed parts of Russia were attacked by the air forces that were beyond conflict zone. In history, this war is considered as the first cyber warfare coincided with military action. [3]

military action) between nations. [1]

I. Cyber Warfare- History glimpse from 2001 to 2019

A. 2001 to 2006

No cyber warfare took place during this year the cyber warfare was emerging during these years.

B. 2007: Operation dust storm

According to the Cylance's research team SPEAR a report of five-year campaign was released that targeted Japanese oil, gas, and electrical utilities. This campaign was observed as Operation dust storm. Dust Storm's activities proof are found in Japan, Asian countries, us, Europe, and a number of other Southeast Asian countries. The important tools of their trade are phishing, emails containing Flash exploits and zero-days implanted into Microsoft workplace documents.[2] Android Trojans s another interesting aspect of this campaign that were also used to do recon on their victims and later to retrieve specific data on those mobile devices. Persistence was achieved through custom-made backdoors created on Japan's systems.

C. 2008: Russo-Georgian War

The war between Georgia and Russia took place in August the war stationed a joint peacekeeping force of Georgian, Russian and Ossetia troops in the territory and in the state of Abkhazia a related

D. 2008: Operation cast lead

The IDF launched the Operation Cast Lead in Gaza on December 27, 2008 on the seventh day of Hanukkah. The aim of the operation was striking infrastructures, used for terror activities and rocket fire from the Gaza strip targeting Israel civilians. Around mid-day, the Israel air force began to attack Hamas, infrastructures in Gaza, including underground tunnels and rocket launching sites. After two days of strikes, the DF began naval strikes. The armed forces attacked dozens of targets throughout the Gaza strip. Such as warehouses, military posts, tunnels, projectile, launching sites to Israel, and production and storage sites.

In parallel to these strikes, the DF allowed the delivery of humanitarian aid, food, medicine, and entrance of ambulances not the Gaza Strip. In one case, the DF even authorized the transfer of two wounded Palestinian children and twenty chronically ill patients from the Gaza Strip to Israeli hospitals to receive medical care. During the operation, the DF attacked the houses of senior Hamas officials. On the night of the fourth day of the operation, three buildings of the Hamas government in the Tel Awa neighborhood were hit by the AF aircrafts, where Hamas managed, financed, planned and carried out most of the terrorist activities. An audit revealed that the offices of the Ministers of Foreign Affairs, Finance, Labor, Construction and Housing and the headquarters of the organization had been completely destroyed and the office of the head of Hamas terrorist Organization was bombed. In addition, two mosques were hit that stored Qassam rockets and Grad missiles.

The Second phase of the operation was the entrance of ground forces: On Saturday, January 3rd, 2009, AF aircrafts targeted terrorists in the Gaza Strip, and the DF ground forces prepared for the second stage of the operation. One week after the beginning of the operation, troops from the Armored Corps, infantry Corps, and Artillery Corps and tens of thousands of reservist soldiers were called and entered the Gaza Strip with the effort to take control of the terrorist organization's launching sites. Dozens of trapped buildings were neutralized, many weapons were discovered, dozens of terrorists were arrested and brought back to Israel for interrogation, and hundreds of terrorists were wounded.

E. 2008: Operation Buckshot Yankee

Operation Buckshot Yankee is all about cyber security. It took place in the Middle East in 2008.This attack led to a turning period for the defence, and it led to huge loss from the secret database of the government. It was the operation to stop a malicious code that was inside a flash drive and later was used in the laptop that were connected to the Centre Command networks and it spreads through the military networks. In response, the government also gave back by declaring cyberspace as the official way to stop cybercrimes and for safety purposes. [5]

F. 2009: Operation Aurora

In this operation, a malware attack was done against 30 major companies that included Google and Adobe also. It exploited a zero-day flaw in Internet Explorer. This misuse helped malware to load on the user's computer. Due to this, the computer control was under malware and it was able to steal information.

Later on, multiple detection was done against a threat. Then it was concluded that if we use Sophos Security Software our products proactively block the threat malicious web pages and JavaScript and it stops the malware that attempts to enter our system. Sophos Buffer Protection Service (BOPS), when activated protects against this exploit. [6]

G. 2010: Stuxnet

A malicious worm known as Stuxnet was spotted in 2010. The SCADA system and PLC's are targeted by the Stuxnet. This worm was responsible for destroying Iran's nuclear power. It allows the automation of electromechanical processes and it is used to resist the machine resources. Stuxnet design is in such a way that it is used for hacking modern supervisory control and data acquisition.

Siemens released a detection and removal tool for Stuxnet that recommends contacting customer support if a worm is uncovered. It also advises installing Microsoft updates for security and stopping the use of third parties. Siemens also advises for immediate upgrade of password access codes. [7][8]

H. 2011: Duqu

Duqu's is a remote access Trojan i.e. Rat that steals the data and targets industrial equipment and illegally collects information. Duqu search information that becomes useful in attacking industrial control systems. Duqu purpose of Duqu is to gather information and then use it later.

Duqu has a modular structure due to which special payload was used to attack any computer system by any mode. One of the Duqu's action that was stated according to the McAfee was to steal digital certificates and was used to attack systems to help the upcoming viruses to appear as secure software. Duqu uses encrypted dummy file and 54x54 pixel JPEG files as source to bring in data to its command and control center. The code analysis is done by security experts to determine the information the communication contains . The beginning research shows that the original malware sample removes itself automatically after 36 days and it generally stores this information in configuration file due to which its detection becomes difficult. [9]

I. 2011: The Jasmine Revolution

In the year 2011, many Tunisians were taken to the streets to call for an economic and social change in their country. They had activists who had a demand for an end to the government's online censorship rule and freedom of expression that were included among the fundamental changes. The battle took place in the internet blogs, forums, twitter feeds, Facebook pages.

Tunisian became the first nation in the Arab world that removed their leader by the popular uprising of web protestors and this was possible due to the modern communication infrastructure of Tunisia's .This revolution helped in overthrowing a corrupt government ,including intense protest and hacking of the user passwords and names of the whole population of Tunisia by AMMAR. Many unknown people were involved by introducing Denial of Service attacks at AMMAR and other government sites during the revolution. [10]

J. 2012: The Shamoon attack

The Shammon attack was initiated with two purposes. The first was to replace all the data in drives with the image of a burning American Flag and then the address of the infected computers was sent to the networks. The virus contained three parts-Dropper, Wiper, and Reporter.

The Dropper is the main part and it is the source of infection. It drops the Wiper and Reporter on the computer, which is infected, then duplicates itself in the network, and it executes and creates a service itself only. The Wiper is the destructive one. It collects all the files from different locations of infected computers and removes them. The Reporter sends the information collected to the attacker and the removed file is replaced with the tainted files so they are not recovered. Over 30000 Windows based systems started to be overwritten with a great pace on 15 August at 11:08 am local time and this was spotted by Symantec [11]

K. 2013: Yahoo

Yahoo did not announce until 2016 while negotiating for its sale to Verzion, that it had been the victim of a "state sponsored" attack on 2014.500 million accounts had been compromised, but it got worse. In December 2016, Yahoo announced another breach that happened in 2013 compromising about 1 billion user accounts. After some months, Yahoo had to study its estimates and announced that all 3 billion-user accounts had probably been affected and it decreased Yahoo's value by about $350 million. [12]

L. 2013: The Eastern Railway Defacement

The Eastern Railway (ER) website was hacked during the growing tension between India and Pakistan. The messages were displayed claiming that it was done to punish India's unproven violation of the Pakistan air space. The official website of Eastern Railway was found tainted with a large number of messages in its scroll section. The scroll section that contains the important official announcements was filled with the sentences like "Cyber war has been declared on Indian cyberspace by Whackerz-Pakistan", "Indians hit hard by Zaid Hamid", and "You are hacked"

A new window used to open as we clicked in messages present in the scroll and it displayed that" Mianwalian of Whackarez" have hacked the website for the revenge of Pakistan air space destruction. When enquired it was found that the ER departments were unknown about the whole scene and even the site was not blocked for a long time and after some hours the site started to work normally.

After search it was found that the case was related to SQL injection. Prateek Agarwal, an expert in Cyber Security, said that as we feed data into any website then it gets changed to specific SQL commands and goes to the database. [1]

M. 2014: The Sony Corporation Attack

This attack took place in October 2014; its motive was to take revenge. The computer systems of Sony Corporation were hacked and the attackers stole a huge amount of private data from the Hollywood Studio, displayed them every week, and exposed it in every field from journalists to potential cyber criminals. According to the reports, it is said that this attack is attached with the North Korean Government, who showed their anger against Sony-backed film "The Interview" which was an action-comedy movie based on North Korean leader Kim Jong UN.

The theatrical release of the movie "The Wednesday "was cancelled by the Sony Corporation as it was leaked during this attack. The employees of Sony Corporation who tried to log onto their systems were greeted by the message "Hacked by Guidance of Peace". The Sony corporation employees are still not able to use their old computers because some code left behind are completely not removed from the system. [13]

N. 2014: JPMorgan Chase

J.P. Morgan Chase stated a hack that affected 7 million small businesses and 80 million individuals. This attack took place against servers, which caused a data breach and huge loss. In terms of impact and loss of data, the JPMorgan cyber-attack was one of the largest and it took place in spring 2014.By the way attacking it was concluded that it was sponsored by Russia backed state. They stole the employee permit of one of the IT specialists at JPMorgan using which they were able to log onto the server. The information that were extracted was financial records, first name and last name rather than the. black market in Russia to sell on the forums that spammers use. [14]

O. 2015: The Anthem attack

The heat insurer Anthem announced a medical breach of information held by Anthem Inc. Anthem Inc. on February 4,2015 disclosed that criminals had broken into their servers and had stolen over 37.5 million records that confined personal recognizable information that were very sophisticated. On February 24, 2014, Anthem raised the number to 78.8 million people whose personal data was affected.

Now the person whose data was stolen during this attack will have the fear of their identity theft for the rest of their life. Anthem advised people whose data was stolen to have periodic look on their accounts and remain vigilant and to check their security system. In 2017, Anthem agreed to settle the hearing for $115 million, the largest ever data breach clearance and

Anthem had US$100 million insurance policy for cyber problems from American International Group. [15]

P. 2015: Ukraine power grid

Ukraine power Grid cyber-attack took place on 23 December 2015
and it is considered the first recognized cyber-attack on a power grid.
Three supply companies of Ukraine were hacked by hackers and
were able to get information and it disturbed the electricity supply to the customers. The attack was very complex and it had several steps. There was a prior compromise of corporate networks by using spear phishing emails with Black Energy malware, seizing the SCADA under control, remotely switching substation off, disabling infrastructure components, spoiling files on the servers and
workstations with Kill Disk malware. DOS attacked the call center so that customers are not updated about the blackout. Entirely up to 73 MWh of electricity was not supplied. [16]

Q. 2016: US elections

The US election was hacked and most of the intelligence Agencies and CIA were pointing towards Russia for this hacking. Still trump oddly tried to deflect attention by saying that the CIA is lying and are wrong. This issue was completely ignored by journalists during the election and instead tried to parade out real or fake emails from Hillary Clinton as proof of dangerous national security actions. The dangerous action was that it was letting other countries hack our elections. Yet all were fooled and mislead by combination of fake news, fake social media and head fakes by twitter bots and automated Facebook posts. Therefore, it was time to look at cyber security and cyber war after what had happened during 2016 elections and with all evidence this pointing to support the candidacy of Trump. [17]

R.2017: WannaCry

WannaCry ransomware attack took place in May 2017 and is considered, as the worldwide cyber-attack. Its aim was to target computers running Microsoft Windows Operating System and encrypting information and asking for ransom payments in the form of Bitcoin Cryptocurrency. It entered older Windows system through EternalBlue and the misuse was uncovered by the United States National Security Agency (NSA) .Few days before the attack EternalBlue was robbed and leaked by a group called The Shadow Brokers .While the Microsoft have released some patch to slow down the misuse, much of the spread was from organizations that were using the older version of Windows.Wanna Cry took benefit by installing entrances onto infected systems. The attack was expected to have affected over 200,000 computers across 150 countries, with a loss ranging from hundreds of millions to billions of dollars. [19]

S. 2017: Equifax

Equifax being one of the major reporting agencies. Equifax on September 7, declared some troubling information for customers that a cyber security failure had headed the hackers to get access to information of about 143 million people. In terms of severity, it was very hard to beat Equifax though it was not the largest. Hackers were able to extract people's names, birth dates, address, driving license number, social security numbers and they stole the credit card of about 209,000 people. The credit agency hired Mandiant, an independent cyber security firm, to conduct an investigation on what happened and they took the disputes app down entirely. [18]

T. 2018: Marriott Hotel Chain

The cyberattack on Marriott Hotel Chain collected personal details of roughly 500 million guests Remote Access Trojan (RAT) along with MimiKatz, a tool for sniffing out username/password combos was found in the system memory. These two tools could have helped the attacker's control of the administrator account. It was not clear how the RAT was placed onto the server, but such Trojans are often downloaded from phishing emails. It is known that the Chinese intelligence services had done this because they used the same technique and they are supposed to be working on behalf of the Ministry of State Security. Starwood and Marriott were guilty of basic security failings and t bear a loss of $28 million. [20]

U. 2019: Electric Power Grid

In June 2019, the New York Times published an article claiming that the U.S.intelligence services had carried out a cyberattack against Russia. Russia's electric power grid has been the target of cyber incursions. The article caused a stir among the experts and government officials in Russia and the United States and other countries. [22]

CONCLUSION

The objective was to research the historical and the present cyberwarfare that took place. Cyber Warfare may be the greatest threat to the nation in coming years. It has never been possible for a person to attack a nation but cyberwarfare had made it possible. The cyberwarfare is carried out without harm of human life and it costs very less as compared to weapon war. The cyberwarfare is a boom today for attacking a nation or any private data. [23][24]

REFERENCE

[1] Cyber Warfare Conflict Analysis and Case Studies Mohan Gazula
[2] Operation Dust Storm, hackers Target Japanese Critical infrastructure by Pierluigi Paganini
[3] 2008 Georgia Russia Conflict Fast Facts by CNN Library
[4] From Cast Lead to Protective Edge Lessons from Israel's Wars in Gaza Raphael S. Cohen, David E.

Johnson,
David E. Thaler, Brenna Allen, Elizabeth M. Bartels, James Cahill, Shira Efron
[5] Operation Buckshot Yankee:By Jeffrey Higa
[6] Operation Aurora Detect, Diagnose, Respond Jan 27, 2010
[7] Centre for Security Studies (CSS), ETH Zürich stuxnet, Schmitt Analysis and the Cyber "Use-of-Force" Debate by Andrew C. Foltz Zürich, October 2017
[8] Stuxnet research reveals possible fourth accomplice, newly discovered versions of Duqu malware by Bradley Barth
[9] Duqu: The Most Sophisticated Malware Ever Seen
[10] Events of the Tunisian Revolution the Three First Years Adele Ananke Nasser
[11] Overview of Cyberattack on Saudi Organizations JISCR Alelyani, Harish Kumar G R King Khalid University, Saudi Arabia
[12] Cyber Warfare: A Review of Theories, Law, Policies, Actual incidents- and the Dilemma of Anonymity Reich, P.C., Weinstein, S., Wild C., & Cabanlong A.S.
[13] 13[The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace
[14] JPMorgan Chase by Philip Mattera The JP Morgan Cyber Attack
[15] The Breach of Anthem Health - The Largest Healthcare Breach N History by Robert Thomas
[16] Analysis of the Cyber Attack on the Ukrainian Power Grid Defence Use Case
[17] UK politics becoming mired n 'culture wars', study by: Daniel Richards
[18] Question: My Research Paper on EQUIFAX DATA BREACH
[19] The Wannacry Ransomware, a Mega Cyber Attack and their Consequences on the Modern India
[20] Research Paper: Marriott Hotels, Resorts, and Suites
[21] All 3 Billion Yahoo Accounts Were Affected by 2013 Attack
[22] US and Russia clash over power grid 'hack attacks' Web Reference
[23] Internet Live Stats (www.internetlivestats.com).
[24] Cyber War Preparedness, Cyberspace Arms Control and the United States; No. 3 August 2014. 98
[25] MIT Technology Review; Article; First Detailed Public Map of U.S. internet Backbone Could Make it Stronger; by Tom Simonite; September 15, 2015.