International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

The Ukraine-Russia Cyber Warfare

Jebaselvan N. Nadar
Student, Dept. of M.C.A,
V.E.S INSTITUTE OF TECHNOLOGY, CHEMBUR
Email: 2019jebaselvan.nadar@ves.ac.in

Jyoti S. Singh
Student, Dept. of M.C.A,
V.E.S INSTITUTE OF TECHNOLOGY, CHEMBUR
Email: 2019jyoti.singh@ves.ac.in

Mentor
Dr.Meenakshi Garg
Professor, Dept. of M.C.A,
V.E.S INSTITUTE OF TECHNOLOGY, CHEMBUR
Email: meenakshi.garg@ves.ac.in

Abstract: ***In this modern era of electronics, the most important and critical role of our lives is played by computing devices and intercommunication. Although, the use of computers and their servers would increase the capacity of firms or consortium who constantly use the same to conduct tasks and pursuits in an economical and systematic manner, it brings threats along with it. Anybody can or may utilize those threats to cause vandalization to profit making states or economies.***

Cyberspace or the internet is a hazardous battlefield and those countries that don't feel unsafe may be the most jeopardized by Cyber War. In this Internet world, no one is safe. Through the internet DDoS can be easily ordered. It does not include much of spending over weapons or anything exceptional and simultaneously can create higher misfortune and economic failures. It is easily understood from the military viewpoint that cyber attacks and defense against them are an irreplaceable and requisite part of naval pursuits and undertakings. Besides only being employed in land, air or water one-on-one; the military or Naval consider web/cyberspace to be the next area of employment of their forces .

There is a hypothesis that states cyber activities as an inextricable and integral part for the future of the military functioning. Thus, at any time after receiving an order, developed countries destroy its enemies war room, logistics and other important military functions and disrupt its total communication creating a blind spot with the aim of gaining an advantage in the battlefield. Ultimately, the primary and the key purpose will be to attain dominion over information on the battleground.

Introduction:

While cyberspace once had the potential to become a global village free from geopolitical tensions; this idea is now very far from the truth indeed the online space has its trenches and barbed wires. They're just made from ones and zeros rather than steel and cyberspace usually reflects or corresponds to real world tensions. Cyber warfare is a broad term encompassing everything from digitally supported military operations against nation-states to political hacktivism promoting certain agendas raising awareness or even taking down governments.

Cyber warfare has many forms hacking hacktivism espionage misinformation and propaganda campaigns on social media and other forms of cybercrime fall under this umbrella. The aim is usually to cause substantial damage to a target attackers either try to disrupt the target's online systems to spy on someone or to snatch sensitive data that can later be used against an adversary. But, often cyber attackers cause real world consequences too,

for example: the disruption of the colonial pipeline activities resulted in a fuel shortage in the U.S, while attacks on hospitals can even cause death. Furthermore, cases of hackers disrupting the electrical grids of certain countries have caused power outages. People also employ cyber warfare measures for political and social activism. One of the most recent examples of such hacktivism is the anonymous group currently targeting Russian media to battle Russian propaganda.

Cyber warfare usually goes hand in hand with regular warfare or in some cases precedes it. The most recent example we face is the ongoing Russian invasion of Ukraine, even before russian troops swarmed across the border, Ukraine experienced continued assaults from hackers. Attacks took down Ukrainian governmental websites and new forms of malware flooded the country targeting firewalls and wiping data. However, next to Ukraine's cyber army defensive efforts, Anonymous also started a cyber war against Russia after the invasion began in Russian media. Playing a key role in the Kremlin propaganda apparatus was their key target; battles also continue on social media where people try to fight against propaganda in comment sections by providing counter-arguments to trolls, provocateurs and people misguided by the Russian media.

But in today's scenario, Russia is using a hybrid war approach where first a cyber or information sector is destroyed by the Russian cyber army and then the ground forces make a move accordingly. This gives Russia an overall advantage in the war. Through this technique the sources of the Russian Army are used fully without wasting any Logistics. Let's get a clear aspect of the above scenario with an example,

The Russian army is targeting an area in Ukraine; before sending the troops the Russian's use the cyber Army capabilities to destroy or disrupt the cyber infrastructure of that specific area including military cyber infrastructure. Now it's literally a havoc in that area without any internet and any proper communication thus blinding the Ukrainian troops in that area at this specific time. Russian ground Army troops go in and get a clear advantage, this is a hybrid tactic which is followed by Russia.

Even before the war got started a week prior, there were various attacks on Ukrainian government websites and military websites and also banks.

The Ukrainian Army has also started its own cyber campaign against Russia by attacking critical Government and military infrastructure such as hacking into their machines and leaking the data publicly by dumping them. This data includes government employee top security credentials.

An anonymous hacker group has also declared Cyber War on Russia. This is for helping Ukrainian cyber army and according to data leaks from one of the sources from Dark web, NSA is also secretly helping Ukrainian cyber Army by providing cyber tools and zero day vulnerabilities and also by providing high and modified hardware which are enhancing the cyber capabilities of Ukrainian cyber Army.

Cyber warfare can be even more deadly than nuclear Warfare if any one of the sides starts an attack which causes a nuclear plant meltdown or opens a Dam above a populated area causing destruction or disabling air traffic control causing in airplane crashes, etc.

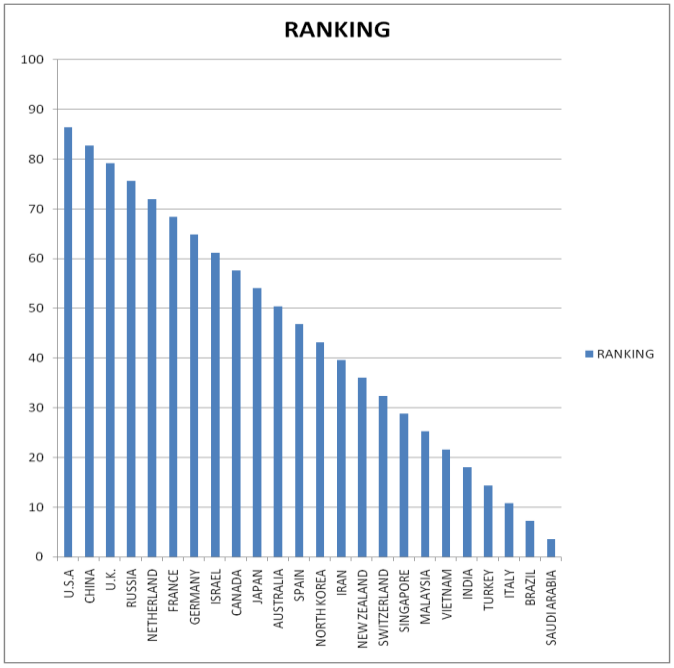
In this way cyber capabilities have already reached an advanced level.

CYBER ARMY:

Before the birth of the internet, the war was only fought on land, water and air. But after the rise of the use of the Internet, in order to safeguard their information and cyber infrastructure; countries have made their own cyber Army to protect the nation's infrastructure from getting stolen or destroyed and also at times of war cyber army can also attack

enemies cyber infrastructure which causes destruction or disruption of their infrastructure. Thus giving and overall advantage in war

The below diagram shows the Ranking of Cyber Armies Of the countries-



Cyber attack on Ukraine:

[Early days]

In 2021,Cyber group aligned with Russian security services had already started the ground work required for military incursion. This information was made public by Microsoft as Russian started gathering zero day exploits of microsoft.

The Russian cyber group also started a trial cyber attack in later 2021 by successfully gaining access to several different Ukrainian energy and its providers and in 2022 some of these targets were hit by destructive computer viruses and malware that disabled the computers by wiping out all the data.

[Before the invasion]

A vast amount of Cyber operations were carried out by the Russian Cyber Army just before the week ahead of Russian invasion on February 24.

A group of cyber security researchers has found out that Russian cyber Army was using a destructive Malware called a whisper gate which was closely mirrored to a 2017 Russian cyber attack against Ukraine known as Notpetya. Notpetya had already destroyed data on thousands of local computer at that time. After Whisper Gate the cyber Army started a spate of distributed denial of service [DDOS] attacks on Ukrainian banking and government websites because of which the services went offline thus causing lots of losses and havoc in Ukraine.

New types of Malware similar to Whisper Gate were engineered and were also launched simultaneously on Ukrainian websites.

[War starts]

As soon as the war starts on feb 24 russian forces entered Ukraine and in order to to gain an advantage the cyber Army crippled tens of thousands of modem which provided internet to the Ukrainian citizens and the government. This attack becomes one of the biggest publicly known cyber attacks to have taken place during a conflict. The Russian Cyber Army also started a cyber-attack on Viasat, a US controlled satellite and by doing this they successfully destroyed the communication in Ukraine. After a day or two Elon Musk used spacex satellites to give free internet services and communication services to Ukraine thus giving a bit of relief to Ukrainian citizens and military.

[Hybrid War]

After the invasion Russian cyber army and Russian state sponsored hackers compromised several important Ukrainian organizations, nuclear power plant, media firms and government entities. There was also an incident where hackers disrupted services from Kyivs TV media station first and then

the military carried out missile strikes all over that area, a perfect example of Cyber hybrid Warfare tactics followed by Russians.

On April 12, a major attack was carried out against INDUJTROYER, a Ukrainian Power Grid company. This attack was not successful as Ukrainian cyber forces were able to tackle them off from their systems, saving the whole country from a total blackout.

CYBER ATTACK ON RUSSIA:

The Ukrainian Cyber Army also started attacking the Russian military cyber department in order to slow them down they also started DDOS attacks on Russian banks and government sites.

The Ukrainian cyber Army had also dumped confidential credentials of higher ups in Russian forces on WikiLeaks. While doing all this, the Ukrainian government started campaigns and also started seeking help on social media to all the hackers worldwide to help in the Cyber War against Russia.

Various cyber groups started helping the Ukrainian cyber Army by hacking websites and by performing DOS attacks on Russian servers. A famous group of hackers known as ‘Anonymous' declared war against Russia. Anonymous hacked 1500 Russian websites including the Kremlin that controlled the news agency, ministry of defence, space agencies, Russian Oil Company, internet providers and even TV news channels. All the information that was obtained such as confidential credentials from these hacks have been dumped on the Internet. These credentials include email id and their passwords, bank details etc.

Russian Timeline of Hacking AKA getting prepared for Cyber Warfare:

Russia has been launching cyber attacks against the Ukrainian government, private industry and even critical infrastructure that truly have no precedent in history. For almost the last decade, Ukraine has now become the pole star of Russia's clash with the west, as in some means, it has been under the obscurity. The recent history of Ukraine states it as a country having scriptures and lessons about the essence of cyber warfare. Looking into Ukraine, we as a country and every country can understand what Russia is competent and proficient of in its digitized severance and how one should be planned and inclined for it. In 2014, Russia hacked the Ukrainian Central Election Commission and also Ukraine had a revolution and it pulled away from Russia's sphere of influence. And then, later that year, on account of its presidential election, the state of Russia financed for the interruption of hackers into its Central Election Commission and basically made a try to sham and forge the results. They planted an image of deceit that evidently showed that the candidate won by a descent. It is a fact that he won lone single figured percentages of the poll. Now, actually, the Central Election Commission caught these fake results in time and managed to foil this, but Russian TV nonetheless broadcast those fake results which kind of shows how they were teamed up and worked in favor of these hackers.

Putin and the Kremlin have always wanted to paint the new Ukrainian democratic government as controlled secretly by neo-Nazis and so trying to spoof that the results showed that the actual victor of the election was this neoconservative & right-wing extremist was just another kind of candidate who bet all others of this detailed knowledge.

In 2015, Russia hacked Ukraine's power grid. Avery recent infamous group of state financed hackers, called Sandworm, takes charge over the cyber war by

Russia in Ukraine. A whole succession of assault that hit Ukrainian media and agencies owned by government of Ukraine was launched by Sandworm. Furthermore, for the very first time in history, hackers themself in actual, triggered a blackout by assaulting on the Ukrainian power grid, a cyber attack just before Christmas. But just to kind of add insult to injury, sandworms also destroyed hundreds of computers inside of these utilities. They kind of strafed them with fraud phone calls, just to create an extra layer of pressure and tension and they even switched off the power supply kept for backup to control rooms themselves. Thus, amidst their own blackout even the operators of the control room faced a blackout. The blackout being created, lasted for six hours or so only because the Ukranians successfully turned on the power back on using manual power. But according to me, it was deliberately directed to have a sort of terrorizing effect and it shocked the world. And it also kind of gave Sandworm this reputation as the most disruptive, the most cyber war-oriented hacker group in the world.

In 2016, Sandworm attacked Ukraine's power grid again, this time in Kyiv. After the first assaults in Ukraine by Sandworm, almost after a year, it came back with a new, even more varied assemblage of cyber assault against the government agencies, finance, infrastructure, defense ministry, etc of Ukraine. The hackers demolished one trillion bytes (terabytes)of data on these bureau of networks. The country's financial statement & budget was totally wiped off by them. This succession of cyber assaults climaxed in an assault that was carried out over the power grid which caused creation of blackout once again but slightly changed, it was in the capital of Kyiv this time. The second blackout only lasted an hour, but in some ways it was nonetheless kind of an escalation of what Sandworm had inflicted the year before. In actual, they impaired safety systems in this transferral station with a motive of causing a glut of current supply on power lines or actually exploding a transformer, when the Ukrainian operators hurry and sprint to switch the power back on. Truly vicious and physically devastative effects of a sort that were spanking new inside of an electrical service. And that broke down only because of a tiny error in the Sand Worms malware.

In 2017, Sandworm released the Notpetya Malware. On the morning of June 27th, a ransom ware text appeared on CPUs of every Ukrainian across the whole country, in all kinds of networks, from government agencies to banks and private industries, hospitals etc. It appeared to be encrypting CPUs & exacting a ransom in the techniques that hackers (cyber criminals)often do.

Even after paying the demanded ransom amount one couldn't decyrpt their files. It was actually facts and figures (data) dismantling piece of cipher delineated to cause maximal havoc. As everyone knows the viruses and worms cannot be controlled, so when they crossed the limit for which they were programmed for they started spreading throughout the world, it immediately hit MNCs like Maersk a shipping firm, FedEx and Mondelez companies which owns Cadbury and Nabisco and also a pharmaceutical giant Merck. In that instance Maersk had 10's of 1000's of delivery trucks waiting outside the ports around the globe and also container shipments all over the world were waiting that is they were at a still point as no one knew what was there source and destination. And for Merck, a company who creates vaccines had to borrow their own vaccines from the Center for Disease Control as there whole manufacturing unit was put to an end because they lost their secret patented formula, they lost billions of dollar because of this one cyber attack which was targeted for ukraine but accidently targeted the whole world.

After Notpetya, Sandworm also attacked other targets around the world, one of them was 2018 Winter Olympics because of which all the Tv stations were shutdown. But we haven't seen Sandworms to be reiterating in any evident way in Ukraine. Now,

just before the life-sized physical Russian annexation of Ukraine that happened a series of cyber assault that demolished hundreds of CPUs in Ukrainian government and military agencies was seen, although we don't have any conclusive evidence yet that it really was Sandworm this time.

Conclusion:

Cyber warfare is too dangerous compared to nuclear or any other form of warfare. It is also cheap and can be achieved from any corner of the world.

As more and more computers are added to a network, the rate of vulnerability also increases and exploiting such vulnerabilities becomes easy for the hackers.

These systems can be from a private organization or government organization and these hackers can be state sponsored hackers.

In short, this gets acknowledged as cyber warfare, and as everything and every business uses the internet such an attack disrupts the whole system causing the damages in millions and even in billions. If in such warfare hospitals, airports, nuclear plants are also caught then it causes losses in lives. In cyber warfare everyone and everything is an exploitable asset and a new secured and updated technology is also an exploitable asset because of the term ZERO DAY EXPLOITS.

As the world gets highly interconnected through the internet day by day the cyber warfare also gets vast and becomes more critical than ever.

Special camps can be organized and people can be taught the importance of cyber security and how one can keep themselves safe from cyber threats.

There is no perfect solution against Cyber crimes but we can try out our best to minimize them and try to build a safe and secure future in this digital world.

References:

https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

https://en.wikipedia.org/wiki/Russian%E2%80%93Ukrainian_cyberwarfare

https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

https://www.computerworld.com/article/3658951/russia-is-losing-the-cyberwar-against-ukraine-too.html

https://thehill.com/policy/cybersecurity/3472214-russias-cyber-warfare-against-ukraine-more-nuanced-than-expected/

https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

https://theconversation.com/how-ukraine-has-defended-itself-against-cyberattacks-lessons-for-the-us-180085

https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

https://eurasiantimes.com/cia-expert-decodes-why-russia-fails-in-cyber-war-in-ukraine/

https://www.cshub.com/attacks/news/russia-ramps-up-hacking-and-jamming-efforts-in-ukraine