jims

January 2020

IT KALEIDOSCOPE

Theme : "Understanding Cyber WarFare"

Program Incharge

Dr. Praveen Arora

Faculty Incharge

Mrs. Priyanka Gandhi

Content Writers

Kirti

Hemant

Abhishek Kumar

Content Editors

Kirti

Tanya

Designer

Ankit Singhal

Cyber WarFare – New Dimension Of Conflict

Wars fought on land, in air, by sea or in space have extended into another battlefield – the ultimate fifth dimension often used by hostile countries or malicious single combatants to target other countries - the cyber space.

These wars, don't involve platoons, grenades or guns but they possess the power of shaking a nation's economy and its financial prowess, as we speak, mainly because it is the sort of war where no rules exist and even if they do, they are not the ones intuitive to traditional military personnel.

Cyber warfare, which is the use of digital attacks to break down or disrupt systems of another country, has the ability to turn every gadget you own into a weapon with the bull's eye aimed at computer systems actively involved in real world infrastructure - from power grids, flight systems to stock markets.

Even the most mundane attacks on out-of-date industrial control systems, transportation networks, and health care organisations may result in irreplaceable damage. Targeted advertising and deep fakes - recording and videos, made via artificial intelligence may lead to defamation of a country's reputation by other hostile countries to create a situation of war or even tilting the balance of fellow nations support to their side.

With the nature of cyber warfare being asymmetric and no clear set of policies and regulations being maintained for attacks that could be specific to world leaders or an entire geographical area alike, we are forced to revert to private sector organisations and the government to set the rules. But so far, no catalogues of globally recognised "cyber act of war" have been defined - which should have been the first step in stopping cyber transgressions all along.

Sony Pictures hack in 2014, targeting a civilian USA organisation, which cost more than $800 million in clean up - akin to the destruction of a Texas oil field, with its origins tracing back to North Korea , is one of the prime examples of the amount of destruction an act of cyber warfare can cause.

Technology and cyberspace are changing faster than countries can legislate internally and negotiate externally and so, it is a necessity to improve network systems and mend security potholes before we have a cyber warfare attack that maybe worse than any hostile country espionage thus far - the likes of which 9/11 or Pearl Harbour are known for.

By: KIRTI
BCA 3RD YEAR 1ST SHIFT

FUN FACTS

- 95% of cyber security breaches are due to human error.
- India is quietly preparing a cyber-warfare unit to fight a new kind of enemy.
- The FBI had to notify over 3,000 U.S. companies that they were victims of cyber security breaches in 2013.
- Oracle Java, Adobe Reader or Adobe Flash are present on 99% of computers. This means that 99% of computer users are vulnerable to exploit kits.
- In the past 5 years, more than a handful of government malware have been discovered but their origins have yet to receive full attribution. The worst of those was the leaked NSA exploit Eternal Blue that lead to the spread of Wanna Cry.

By: Abhishek
BCA 1st Year 1st Shift

jims

January 2020

IT KALEIDOSCOPE

Theme : "Understanding Cyber WarFare"

Program Incharge

Dr. Praveen Arora

Faculty Incharge

Mrs. Priyanka Gandhi

Content Writers

Kirti

Hemant

Abhishek Kumar

Content Editors

Kirti

Tanya

Designer

Ankit Singhal

History Of Cyber WarFare

For many people, it was the year 2007 in which cyberwar went from theoretical to the actual.

When the government of the eastern European state of Estonia announced plans to move a Soviet-era war memorial, it found itself under a furious digital bombardment that knocked down bank and government services offline (the attackers are generally believed to be Russian hackers but Russian authorities denied of having any knowledge of the same). However, the DDoS attacks in Estonia did not cause any physical damage. In spite of being a significant event, it was not considered to have risen to the level of actual cyber warfare, yet.

But unbeknownst to many, another cyber warfare milestone was to be hit the same year. When the Idaho National Laboratory proved, via the Aurora Generator Test, that a digital attack could be used to destroy physical objects, in this case - a generator. Following this discovery, the Stuxnet malware attack, that took place in 2010, proved that malware could actually affect the physical world.

Since then there has been a steady stream of incidents- in 2013, the National Security Agency (NSA) said it had stopped a plot by an unnamed nation (believed to be China) to attack the BIOS chip in PCs, making them unusable. In 2014, there was an attack on Sony Pictures Entertainment, blamed by many on North Korea, which showed that it was not just the government systems and data that could be a possible target by state-backed hackers.

Perhaps the most serious one happened just before Christmas in 2015, hackers managed to disrupt the power supply in many parts of Ukraine by using a well-known Trojan called Black Energy. In March 2016, seven Iranian hackers were accused of trying to shut down a New York dam in a federal grand jury indictment.

In light of such events, nations all around the globe are rapidly building cyber defense and offence capabilities. In 2014, NATO (North Atlantic Treaty Organization) took an important step of confirming that a cyberattack on any one of its members would be enough to allow them to invoke Article 5, the collective defense mechanism at the heart of their alliance. Then in 2016, cyberspace was defined as an "Operational domain" - an area in which conflict can occur. Henceforth, since then, the internet has officially become a battlefield and it may continue to be in the future.

By: HEMANT
BCA 3RD YEAR 1ST SHIFT

FUN FACTS

- There is a hacker attack after every 39 seconds on average.
- In 2018, hackers stole half a billion personal records.
- Identity theft has affected over 60 Million Americans.
- According to WEF ranking 2019, Algeria have the most unsafe cyber network.
- Japan is the most cyber-safe country in the world.
- 95% of breached records came from the government, retail and technology industries in 2016.
- Ransomware and OPM hack is leading the way in modern cyber crime events
- Only 38% of organizations have the infrastructure to handle a sophisticated attack.
- More than 77% of organizations do not have a cyber-security incident response plan.

By: Abhishek
BCA 1st Year 1st Shift