DISEC

The Question of state sponsored cyber attacks

Committee: **DISEC**

Topic: **The Question of state sponsored cyber attacks**

Chair: **Harry Gordon, Mehal Gupta**

Summary

Overview:

State sponsored cyber attacks are malicious activities that are carried out or supported by governments to achieve political military economic or social objectives. These attacks are typically more sophisticated well funded and organised than those carried out by criminal groups or independent hackers. They are often part of a potentially broader strategy of hybrid warfare where these cyber operations could compliment military or diplomatic efforts.

Key Parts:

1. Advanced persistent threats or APT's. State sponsored cyber attacks often use APTs which are long-term stealth operations aimed at infiltrating the target network. These attacks may remain undetected for up two years while attackers gain and gather intelligence. They can also disrupt operations or damage critical infrastructure.

2. Targeting critical infrastructure one of the main objectives of cyber attack is to disrupt or destroy the key infrastructure of another country. This could include power grids financial systems, military networks and or communication systems. These attacks can work to damage and nations economy defence and public services.

3. Economic or political motives cyber attacks can also be used to stabilise political systems attacks on elections media outlets and even the public opinion can weaken a country governance.

4. Difficulty in detection of perpetrators these cyber attacks often use more sophisticated techniques to hide their identities to make discovering who had caused the attack more difficult they may try to appear as if it had come from a criminal group or independent hackers thus being able to avoid retaliation from targeted countries and this ability to deny make sponsored cyber tax more difficult to counter.

Common methods:

1. Fishing and social engineering- state backed cyber attacks often use fishing emails or social engineering, which takes advantage of the human part of government, to gain unauthorised access into sensitive information or highly important systems.

2. Malware and ransomware- deploying malicious software that can damage importance systems still confidential data or demand ransoms from victims is a common method such Malware may be highly sophisticated, allowing the attackers to maintain control over these networks.

3. Zero day exploits- cyber attacks may take advantage of previously unknown vulnerabilities. This is a zero day exploit. This is particularly dangerous as there is no way to prepare to defend against these exploits, this can also allow attackers to target newer systems.

4. DDOS attacks (distributed denial of service)- these attacks use an overwhelming amount of traffic to a tech a website or network which makes it unusable and disrupt its services. This can often be used as a form of retaliation or distraction.

Previous examples:

Stuxnet (2010)- stocks net was a cyber attack that was specifically designed to the target Iran nuclear and Richmond facilities. This worm was designed to infiltrate industrial control systems specifically those using the Siemens software. It was highly sophisticated exploiting multiple zero day vulnerabilities to spread through networks and USB drives. This one caused physical damage to the centrifuge forcing Iran to temporarily shut down it's a nuclear enrichment program. This is seen as the first known cyber attack that caused tangible damage to industrial infrastructure.

Russian interference in US elections (2016)- in 2016 the US presidential election was clouded by extensive cyber interference believed to be orchestrated by Russian actors who happen to be state backed hackers had infiltrated the democratic national committee network by using fishing tactics and more work in order to steal emails and documents. These materials were then later released to the public through outlet such as wiki leaks with the aim of effecting the final vote. This interference race concerns about the vulnerability of democratic processes from cyber manipulation.

Sony Hack (2014)- in response to the planning of the release of the film the interview which had depicted the fictional assassination of Kim Jong-un of North Korea a group of hackers under the alias Guardian of peace launched a highly damaging cyber attack on Sony pictures entertainment these hackers managed to gain access to Sony's internal network and publicly releasing a vast amount of sensitive data. This highlights how cyber operations could be used to exert political pressure and silence others through digital means.

Previous legislation:

Legislation has been passed in the UN about cyber attacks by the Group Governmental Experts (GGE) reports, the latest of those was published in 2021. UN Resolution 70/237 (2015) on "Developments in the Field of Information and Telecommunications in the Context of International Security" acknowledges the potential risk of cyber attacks in the future but there is yet to be a resolution solely focused on cyber attacks as a whole.

Major Countries / Organisations Involved

USA, China, Iran, UK, France, North Korea, Russia