Committee: DISEC 1

Topic: The question of state sponsored cyber crime

Chair: VAMA KOTHRI

School: Frankfurt International School

Summary

As our world evolves in terms of technology and our scientific capabilities, a rather new threat has appeared. With the rise of the internet, complex software, computer programs, data collection, intellectual property, and more, the issue of cyber security has become prevalent in our modern world. This issue is present not only on a small scale but also on a global scale with the question of state-sponsored cybercrime. As suggested by the name, state-sponsored cybercrime are cyberattacks on other nations or organizations which are backed by a country's government. This report will discuss more what the issue is, how it occurs, the risks it poses, who is currently involved, the past of the issue, and also what solutions can be implemented in the future to counteract any threats.

Definition of Key Terms

Cybercrime: crime or criminal activity carried out through the use of the internet or computers

Cyberattacks: an attempt to damage or destroy systems, networks, or programs by a hacker

Cybersecurity: the practice of implementing methods of protecting systems, programs, and networks from cyberattacks

Malware: software with the ability and design to destroy or disrupt systems, networks, or programs

Background Information

As stated in the name, state-sponsored cybercrime is cyber-based attacks carried out on nations backed by a country. This occurs through the employment of hackers by the government or military. More commonly, however, it occurs through discreet funding. This would allow for easier deniability and diplomatic repercussions should an attack be detected. However, it also blurs lines between criminal organisations and governments. Another term for this action is 'government-based hacking'. The goal of

this type of attack is the same as other actions a country may take, to promote a national interest. This can be done by gathering intelligence on the military, corporations, technologies, economic data, or even political developments. It can also be used to disrupt important infrastructure such as power grids, transportation systems, or financial networks. Cyber attacks could also help spread disinformation or fake news to disrupt political affairs. Furthermore, they can be used to interfere with or disrupt political processes such as elections or military operations to gain an advantage.

How does it happen?

There are many methods by which a nation can launch cyber attacks to target the systems mentioned above. One such example is using malware including viruses or worms to gain access or disrupt nations' networks or systems. Another method is through phishing attacks which exploit human error by tricking individuals into giving away information or login credentials to access systems or networks. Another type of phishing is spear phishing which targets specific organisations or individuals by using more personalised or specific methods. Denial of service confuses by flooding important websites with traffic. This can be used to disrupt operations or make political statements. Furthermore, countries can exploit the supply chain and launch attacks by infiltrating networks of third-party vendors or partners by planting malware in any hardware or software they provide. Lastly, countries can launch physical attacks by physically planting malware into a computer or network through a USB or other similar means.

What risks does it pose?

Cyber attacks can pose risks to governments and any related systems but they can also pose risks to other demographics such as businesses or individuals. These risks can be collateral from attacks such as those that attempt to disrupt large systems like electrical grids or transportation. Furthermore, it can have political repercussions. Hacking in the form of surveillance also poses risks to individual privacy. Another threat is towards businesses, specifically those in the private sector. Many companies expect state-sponsored cyber crime to pose a threat to them in the coming 5 years and more within the decade. Furthermore, according to studies conducted by Businesswire 68% of executives have a false sense of security in their ability to defend against these attacks. Attacks on such companies can have long-term consequences on not only finance but also on society. They also pose reputational risks to companies. Threats against banks have also been increasing. These can affect political affairs as well as financial ones.

Cyberwarfare

While it doesn't have a clear definition and is significantly linked to general state-sponsored cyber crime, cyber warfare is slightly different in the sense it is usually a series of attacks and may result in more

catastrophic results. The methods of attacks are the same and often are deployed using the same approaches.

Major Countries and Organizations Involved

Many countries are involved in state-sponsored cybercrime as both perpetrators of the attacks and recipients of them. Some of them are listed in this section but others will also be listed in the timeline of events.

Organizations

There are many smaller organizations and companies which offer protection against general cybercrime. In terms of state-sponsored cybercrime, most organizations are government affiliated such as the US FBI or Department of Defense. There are non-governmental organizations offering protection such as Imperva (used as a cited source- see bibliography) which is a cybersecurity sector leader. The UNODC also has a Global Programme on Cybercrime.

Superpowers

Within the world of state-sponsored cybercrime, there are countries which could be considered superpowers. According to the World Economic Forum, the countries with the most advanced cyber warfare capabilities are the UK, the US, China, Russia, and Israel with North Korea and Iran being other major players. All of these countries have upped their investments in cyber capabilities in the last decade and are continuing to do so.

Timeline of Events

● 2005-2010- Suxtent Virus- this virus was a worm which targeted the Iranian nuclear program and is noted as a highly sophisticated attack. It had serious effects on the program and heavily damaged its manufacturing abilities.

● 2007- Estonia relocated a statue related to the USSR from their capital to a military cemetery and suffered several denials of service attacks on government websites, media outlets, and banks.

● 2008- Russia was accused of using cyber warfare in its attack on Georgia

● 2012- Iranian hackers targeted the Saudi Arabian oil company Saudi Arabia Aramco and almost completely crippled it

● 2014- Sony Pictures Hack- following the release of the film “The Interview” which negatively portrayed Kim Jong Un Sony Pictures was hacked by what the FBI believes was a group of North Korean hackers

as the country used similar malware in the past. The hack released confidential information as well as personal information on employees.

● 2014-16- there were claims by CrowdStrike that a Russian-organized cybercrime group Fancy Bear targeted Ukrainian rocket forces and artillery through an Android app

● 2017- WannaCry- a state-sponsored attack which affected the UK and demanded ransom in exchange for unlocking computers they infected

● 2018- Enemies of Qatar- a lawsuit by american Elliott Broidy accused the brother of the Qatari Emir of having created a cyber warfare campaign targetting anyone who would be enemies of the state including officials from Egypt, Saudi Arabia, the UAE, and Bahrain.

● 2019- alleged state-backed hackers from North Korea stole 10 million USD from the Bank of Chile's ATM network

● 2020- Sunburst- targeted many companies such as SolarWinds which provide software to government agencies

Relevant UN Treaties and Events

While there haven't been any specific resolutions made on this issue there have been some made on cybercrime as a whole. One example is the UN Treaty on Cybercrime which was adopted in December 2019 and discussed the issue of using information and communications technologies as a means of criminal behaviour. It furthermore introduced an ad hoc committee which had the goal of organizing a new international convention and thus working towards international solutions. The committee opened in March of 2022 and is expected to take 3 years to complete its work. For more information on its meetings visit this site:

https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

Another example was the Budapest Convention on Cybercrime which opened in 2001. However, this event didn't discuss state-sponsored cybercrime but rather focused on the issue as a whole as it was becoming more and more common and a bigger threat. The UNODC, as mentioned above, also has goals regarding cyber security. However, it doesn't focus on state-sponsored cybercrime. While it isn't directly UN-affiliated, the Tallinn manual was produced by scholars in 2013 at the request of NATO's Cooperative Cyber Defence Center of Excellence and discusses conduct which should be used during cyberwar between nations. Its follow-up, Tallinn 2.0 in 2017, specified the applications of international law in the use of cybercrime against other countries to prevent its use in a malevolent attack.

Previous Attempts to solve the Issue

A UN treaty on cybercrime is after years of discussion finally on its way. The UN General Assembly voted in December 2019 to begin negotiating a treaty – a treaty that focuses on cybercrime, but also has the potential to develop numerous policies on a global scale with important significance for human rights. The treaty is an important step towards helping countries realize some of the sustainable development goals.

In December 2019, the UN General Assembly adopted a resolution on “countering the use of information and communications technologies for criminal purposes” and introducing an Ad Hoc Committee. The committee was announced to elaborate a comprehensive international convention. Thus, working towards creating a new international treaty on cybercrime.

Possible Solutions

Overall strengthened cyber security: implementing strong passwords, updating software, updating security systems, training employees

● Monitoring: monitor systems and software for suspicious activities or potential threats and act on any such activity

● Incident Response Plans: implement methods to quickly respond to and counteract cyber attacks

● Work internationally/Cooperatively: share information and collaborate on counter- cyberwarfare methods and protection. Furthermore, countries can attend conferences, conventions, and more to promote cyber stability and address threats.

● Legal Frameworks: build legal frameworks and recognize cybercrime to hold perpetrators accountable by recognizing issues such as cybercrime, data protection, and intellectual property.

● Spreading Awareness: educate the public on the risks of a cyberattack to increase individual protection and also allow them to report potential threats

● If possible, invest or allocate funds into divisions of the government to focus on cybercrime.

Bibliography

Allison, George. “State Level Cyber Attacks – Why and How.” UK Defence Journal, 20 Dec. 2022, ukdefencejournal.org.uk/state-level-cyber-attacks-why-and how/#:~:text=The%20Stuxnet%20worm%3A%20In%202010,damage%20to%20the%20nuclear

%20facility.

“The Budapest Convention on Cybercrime: A Framework for Capacity Building.” Global Forum on Cyber Expertise, thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/. Accessed 31 July 2023.

“Cyberwarfare.” Wikipedia, 28 July 2023, en.wikipedia.org/wiki/Cyberwarfare.

“Government Hacking: Privacy International.” Government Hacking | Privacy International, privacyinternational.org/learn/government-hacking#:~:text=Government%20hacking%20often%20depends%20on,interfere%20with%20their%20own%20systems. Accessed 31 July 2023.

“Guides: International and Foreign Cyberspace Law Research Guide: Tallinn Manual & Primary Law Applicable to Cyber Conflicts.” Tallinn Manual & Primary Law Applicable to Cyber Conflicts - International and Foreign Cyberspace Law Research Guide - Guides at Georgetown Law Library, guides.ll.georgetown.edu/cyberspace/cyber-conflicts. Accessed 31 July 2023. Moon, Angela. “State-Sponsored Cyberattacks on Banks on the Rise: Report.” Reuters, 22 Mar. 2019, www.reuters.com/article/us-cyber-banks-idUSKCN1R32NJ.

“Significant Cyber Incidents: Strategic Technologies Program.” CSIS

https://unric.org/en/a-un-treaty-on-cybercrime-en-route/