Committee: DISEC 2

Topic: State-Sponsored Espionage and Cyber Security

Chair: CJ Coleman-Benjamin

School: Royal Russell

Summary

Espionage is seen to be a practice usually performed by governments, where they use spies in order to gain political and military information. There have been many well-known espionage/intelligence agencies, such as America's Federal Bureau of Investigation (FBI) and the UK's Secret Intelligence Service, commonly known as the MI6.

Since the technological popularity spike within the late 1990s, well known as the "dot-com boom", technological security has developed accordingly, resulting in the development of many companies that specialise in counteracting cybercrime and cyber espionage. This also includes the UN, where the UN Office of Counter-Terrorism (UNOCT) has also branched out into the cybersecurity area, with the introduction of the "Cybersecurity and New Technologies Programme", which aims to "enhance capacities of Member States and private organisations in preventing cyber-attacks carried out by terrorist actors against critical infrastructure".

Definition of Key Terms

DoS: DoS attacks, or Denial of Service attacks, are when users are unable to access information systems, devices, or other network resources due to the actions of a malicious person by flooding a server with many requests in a short amount of time.

DDoS: DDoS, or Distributed Denial of Service attacks, are identical to DoS attacks; however it occurs using multiple computers/machines to flood a targeted information system.

Cyber Terrorism: "Computer-based attacks at aiming and disabling vital computer systems so as to intimidate, coerce, or harm a government or section of the population."

Cyber Crime: "A crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (hate crimes, etc.).

Phishing: "Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message"

Firewall: “a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.”

White-Hat Hacker: A hacker, commonly hired by companies, who uses their skills in order to ascertain any flaws with a companies’ system (website/software/application, etc.), and reports such flaws to the business.

Background Information

Since the production of the first personal computer, the Apple I, developed by Steve Wozniak and Steve Jobs, cyber threats grew more and more prevalent as time went on. With the first recorded cyber attack in history known as the Morris Worm, which slowed down computers significantly, such that the device was rendered useless, this marked the beginning of cybercrime. After that, situations such as NASA being hacked by 15-year-old Johnathan James in 1999, causing an estimated $1.7 million worth of damages to NASA, became more and more commonplace.

A number of countries have been accused of cybercrime/cyber espionage on an international level, mainly Russia, China and North Korea. Although many of these were baseless accusations and conspiracy theories, there was a lot of evidence that proved said countries were the perpetrators when it came to international cybercrime incidents, such as North Korean government-linked hackers stealing around $30 million worth of cryptocurrency.

Major Countries and Organizations Involved

Russia was often accused of cyber-attacks upon other countries, such the “Moonlight Maze” cyber-attack on the US in 1996, where it infiltrated the pentagon, military contractors, civilian academics, the Department of Energy and several other American government agencies. It took nearly 3 years for the US to assemble a specialist taskforce designed to counteract this data breach.

Although certain countries have been known to commit cybercrime and cyber espionage on an international level, there have also been incidents where countries have been “exposed” by certain hackers to the point where they can be accused of infringement on human’s rights, such as certain photos and videos of the Xinxiang Police files being brought into light, where it shows the human rights abuses committed by the Chinese government against the Uyghur population.

Timeline of Events

Date	Description
1986-7	German Computer hackers led by Markus Hess hacked into American defence contractors, universities, and military bases. Sold the information gathered to the Soviet KGB. Later convicted of espionage in Feb 1990.
1999	A series of cyber-attacks in the US, resulting in the loss of a large amount of America's confidential military information, known as the "Moonlight Maze" operation.
2001	First passed resolution related to Cyber Security.
2007	Series of DoS attacks on Estonian government websites. Russia was blamed for these attacks, and a citizen of Russian ethnicity living in Tallinn was convicted for his ties to these DoS attacks.
2019	UN general assembly adopts a new resolution in regards to cybercrime and cyber espionage.

Relevant UN Treaties and Events

The first ever resolution with reference to cybersecurity, on the 22nd January 2001. This resolution, in addition to January 2002's Resolution 56/121 both tackle issues with cybersecurity, with focus on "Combating the criminal misuse of information technologies ".

January 2003's Resolution 57/239 had a focus on the "Creation of a global culture of cybersecurity".

January 2004's Resolution 58/199, as well as March 2010's Resolution 64/211 both had a focus on the "Creation of a global culture of cybersecurity and taking stock of national efforts to protect criminal information infrastructures".

Previous Attempts to solve the Issue

Due to the nature of this issue, it is very difficult for the United Nations to find a way of tackling it without infringing on people's right to privacy. Despite this, there have been many efforts of tackling such an issue via the use of the aforementioned resolutions in the section above.

Many countries have their own independent ways of solving the issue, such as the North Korean government heavily restricting the public's access to certain parts of the internet, such that there are only a handful of North Korean-regulated sites that said people can access. Whether or not this is a viable attempt at solving the issue is a different question in a different section of the research report, however this option of resolving cybercrime and cyber espionage is definitely a viable option.

Possible Solutions

Due to the existence of the internet and other cyberspaces, cybercrime and cyber espionage come into existence. This also means that it is very difficult to properly regulate, without verifying every computer on a regular basis. Not only is this time consuming, but it is very cost ineffective. Most other solutions, such as enforcing a monitoring application on all devices during production, similar to what's currently happening in North Korea, where only certain websites are allowed for public use, with those websites being heavily monitored, becomes an infringement on human rights to privacy. So, what can we do in order to reduce, let alone prevent, cybercrime and cyber espionage?

Most countries in the west, including but not limited to, the United States of America, the United Kingdom, France, etc. Believe in "free internet", which is a term described as allowing citizens free use of the internet with almost no restrictions (certain restrictions, which conflict with other laws, have to be in place, such as but not limited to terrorist activities, child pornography, etc.), however less democratic countries, such as North Korea and Russia, governments may feel threatened by so called "free internet", and move towards limiting its usage, as well as using it in order to spread propaganda to its citizens. These conflicting views are one of the reasons why an internationally-recognisable body is too idealistic.

A common technique used to prevent cybercrime by both public and private companies is to have a regularly updated system, constantly improving its firewall, so that the security of the website/application is constantly reconfigured and fortified, making it harder for cybercriminals to infiltrate aforementioned websites/applications. Many individuals already specialise in supporting such ventures, commonly known as white hat hackers.

However, similarly to how the systems are regularly updated, possible hacking techniques also improve, creating a "race" between the cybercriminals improving their techniques, and companies further developing their security measures against the aforementioned cybercriminals.

Due to all of these issues, the easiest and most efficient way to stop cybercrime is to have an internationally recognised body built specifically for preventing cybercrime at a national, as well as international level. However, for that to happen, the prerequisite of having the consent of governments is compulsory, which is highly unlikely with the current state of the world's leaders.

Bibliography

https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message.

https://abcnews.go.com/Technology/story?id=119423&page=1

https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html

https://www.kaspersky.com/resource-center/definitions/white-hat-hackers

https://unric.org/en/a-un-treaty-on-cybercrime-en-route/#:~:text=In%20December%202019%2C%20the%20UN,elaborate%20a%20comprehensive%20international%20convention

https://www.sciencedirect.com/topics/computer-science/moonlight-maze

https://en.wikipedia.org/wiki/Moonlight_Maze

https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-russia-launches-its-first-cyberattack-on-the-u-s-with-moonlight-maze/#:~:text=Russia%20has%20a%20long%20history,the%20U.S.%20was%20in%20motion.

https://www.cfr.org/cyber-operations/#:~:text=Social%20Nav&text=Since%202005%2C%20thirty-four%20countries,most%20being%20acts%20of%20espionage

https://www.ncsc.gov.uk/news/uk-condemns-chinese-cyber-attacks-against-businesses-governments

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents