LmunA 2023

Research report

Forum:	GA6
Issue:	Establishing structures for resolving cyber-crime related conflicts and encouraging international collaboration on cyber security.
Student Officer:	Juul den Elzen
Position:	Main chair

LMUNA

Lorentz Lyceum
Model United Nations
Arnhem

Introduction

Cybersecurity is a pressing issue, with cybercrimes having international effects. There is a large breadth of possible cybercrimes which can be committed. From identity theft to internet fraud, to espionage, and cyberterrorism. That so much of the population has access to the tools required to commit cybercrimes means they happen more frequently and on a larger scale. Not only are individuals susceptible to cybercrime, but corporations and governments are too. Not all hackers are financially motivated and wish to profit. For espionage, the 'bugging' of devices occurs nowadays. As well as hacks such as the SolarWinds hack, where government data is accessed and decrypted. There are also Hacktivists (hacker activists), who seek to advance their political or social views. Examples of this are the famous hacktivist group 'Anonymous' who originated in the 2000's. They famously hacked over 450 Chinese government websites in 2011, in order to protest the Chinese treatment of their citizens.

In 1988, the first cyber-attack named the 'Morris Worm' took place. It was a DoS (Denial of Service) attack, which made the software it was used on unavailable to its users. Although most computers of today are immune to the vulnerabilities, the 'Morris Worm' exploited, the fact remains, approximately 2,220 cyberattacks occur each day. With over 800,000 attacks occurring annually across the globe. Internationally, nations have recognized an imperative need for national and international agreements surrounding cybersecurity. As nations understand and continue to learn the threat cybercrimes can pose.

This growing number of cybercrimes and cybercriminals truly enhance the need for legal frameworks. Nations have to decide if working together to solve this problem is the best way to handle it.

Definitions of key terms

Cyber Crimes

The definition of Cyber Crimes refers to any criminal activity that involves a computer, networked device, or a network for criminal means.

Cyber Security

Cyber Security involves the processes used to secure and safeguard assets which carry information from being attacked or stolen.

Supply Chain Attack

An attack in which there is an attempt to damage an organization by targeting the less secure elements of their supply chain. So, someone using an outside provider who has access to your data to infiltrate your digital infrastructure. (SolarWinds cyberattack)

Brute Force Attack

This is an attempt to guess a password through logic or a random guess. This can be circumvented by only allowing a specific number of guesses or attempts before a program shuts off.

Dark Web

The encrypted parts of the internet which are not catalogued by search engines. They are most notoriously used by criminals, to communicate and to be capable of sharing data or preforming transactions without being detected by law enforcement.

Data Breach

When files and data have been breached/accessed by a hacker or a third party who should have no access to them.

Drive By Download Attack

A common method of spreading malware. The criminal looks for a ‘weak’ website and adds code to the website which is nefarious in nature. The only part the victim plays is accessing a website, which either directly downloads malware, or the victim is brought to a different website which is controlled by the cybercriminals.

Encryption

The process of protecting data by converting plain data into secret code with software (typically).

Fileless Malware

Malware stored in within the volatile data storage components such as RAM, memory processes and more. This is different to most malwares which require contact with hard drives and thumb drives. Typically, being picked up by vising a website. A reboot can typically remove the malware, although it isn't typically detected by antivirus programs.

Malvertising

The use of online adds to spread malware, downloading malware once clicked upon.

Man-in-the Middle Attack

A cyber-attack where the victim believes they are conversing solely with another individual (i.e., The bank), but all of the messages and data go through the man-in-the-middle.

Phishing

A type of internet fraud which aims to gain a user's credentials through deceit. For example, a phishing email which acts as though it is your Netflix account aiming to confirm your email and password.

Ransomware

Programs designed to extort money. Blocking access to a computer or withholding data which will only be released upon a monetary payment. Can also take the form of a text message 'from the government' about missing taxes. Where the payment goes to the cybercriminal and there were no missing taxes to send.

General overview

History of Cyberattacks

There have been millions of cyberattacks which have occurred since the 1st cyberattack in 1988. Cyberattacks have grown in complexity as the internet and technology has. Leading to a struggle to defend and prevent cyberattacks. The United States of America's Department of Justice (DOJ) made comment on the number of cyberattacks which are reported, only 1 in 7. Thus, it is clear to see that many cyberattacks go unseen. Perhaps seemingly as a testament to their lack of success, however, some cyberattacks have a larger impact than others.

In 1999 there was a cyberattack on NASA which shut down its servers for 21 days. The attack was performed by a 15-year-old. In 2007 there was a large cyberattack in Estonia which shut down 58 websites. These websites were government, banking, and media sites. This has been considered the first cyberattack on a country as a whole as opposed to a company or organization. In 2017 one of the biggest ransomware attacks of all time took place. 200,000 companies across various industries were attacked, and the cost to fix the repercussions cots approximately 6 billion pounds.

These cyberattacks, are examples of the different types of individuals which can be affected, and the different ramifications. Companies can lose access to data and can have data stolen and sold. Additionally, companies can be forced to pay to regain access to their data and software or be fined for improper cybersecurity.

Types of Cyberattacks

There are a number of different types of cyber-attacks. These attacks have been given names to help differentiate between them. The most common types of cyberattacks which attract most civilians are Malvertising, Phishing, Brute Force Attack, Drive By Download Attack, and the Man-in-the-Middle Attack. These types of attacks are different in their nature, and in the intended purpose.

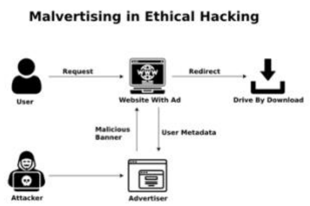

Figure 1“What Is Malvertising?” GeeksforGeeks, GeeksforGeeks, 17 Aug. 2022, www.geeksforgeeks.org/what-is-malvertising/.

The Malvertising Attack and the Drive By Download Attack go hand in hand. With consumers clicking on a website and having their information and data shared to the attacker. This type of attack can be seen in Figure 1. The User can be seen accessing the add and being redirected to the download. In this manner the user has unknowingly had personal data transferred and downloaded Malware. Consumers are not always aware of how exactly viruses are downloaded from the internet.

Brute Force Attacks are less common to occur with websites having intricate password requirements, the creation of google suggested passwords, and having software that locks out a user after a number of unsuccessful password attempts. These attacks consist of the attacker simply guessing available combinations until they have made their way into the system. However, this is not to say that users who use passwords such as 1234 are not still susceptible to brute force attacks.

Additionally, Phishing and Man-in-the-Middle Attacks are similar in nature. With both attacks aiming to gain confidential credentials of users through deception. In the case of Phishing, the consumer believes they are giving up their confidential data to a reputable source, for example confirming their bank number with what they believe is the bank. With a man in the middle attack, consumers are unaware there is someone else receiving every message or statement they make.

Lastly, with a Supply Chain Attack, this is a way for cybercriminals to take advantage of weaknesses along the supply chain. As most businesses, organizations and governments make heavy investments to ensure they are cybersafe. Exploiting the weakest link can allow attackers to gain access to data of these more protected organizations without tackling their defences.

To conclude, most types of cyberattacks rely on deception. Users should be vigilant with understanding who they are giving their data too, and how their data is protected. Users should additionally be aware, that the loss of personal data for entrance into government cites allows hackers with larger targets an easy backdoor. Cyberattacks can occur on different scales, and there should be protection for civilians, companies, governments, and nations.

Legal Measures

It should be noted, it is easy from an outside perspective to question the lack of laws and legal protections. However, Hoda Al Khzaimi remarked; "The way we build regulations for cybersecurity is centralized. The regulations this system creates are valuable, but the process takes time. It can take two years for a regulation to be developed. Standardization can take 18 months. A cyberattack takes seconds. The speed at which emerging technologies are implemented often outpaces our ability to build security measures around them. We need to go beyond simple compliance with regulations if organizations are to be cyber resilient." (Hoda Al Khzaimi, Director, Centre for Cyber Cybersecurity, New York University (NYU), Abu Dhabi; Founder and Director, (EMARATSEC) Centre for Emerging Technology and Advanced Research in Cyber Security, AI and Cryptology, NYU).

Digital Innovation happens rapidly. Legal changes less so. As democracies and the United Nations require legislature to be debated upon. There have been a number of useful legal measures which have passed in various countries. The Budapest Convention was the first international agreement which aimed to harmonize national laws involving computer crime and increase cooperation between nations on the topic of cybersecurity. 67 UN recognized states and 10 international organizations are recognized as members or observers of the Budapest Convention.

Major parties involved

United States of America

The United States of America is highly relevant in the cybersecurity industry, as they has the most cybersecurity firms operating from within their borders US. The United States was a victim with some of their government agencies with the 2020 SolarWinds hack. They have several effective regulations related to cybersecurity, such as the Cybersecurity Information Sharing Act (CISA). CISA encourages the sharing of cybersecurity threat information between the government and the private sector. Negatively the 2nd largest number of cyberattacks originate from here. On a global scale, the United States foreign policy regarding cybersecurity, is that it aims to promote responsible behaviour for nations in cyberspace.

United Kingdom

The United Kingdom is combating cybercrimes, with regulations, laws and more. Very few cyberattacks globally originate from the UK, and relatively few devices are infected with malware. Additionally, the UK incorporated the EU GDPR (General Data Protection Regulation) into their laws, through the 2018 Data Protection Act. Additionally, the UK government backs 'Cyber Essentials' a certification scheme created to help ensure basic cybersecurity controls. The UK also wishes to promote responsible behaviour in cyberspace.

LmunA 2023

Republic of Korea

The Republic of Korea has a large number of laws, regulations, and standards to combat cybercrimes. South Korea has the Personal Information Protection Act (PIPA), which dictates in which ways personal information may be used. Further South Korea has the Information and Communications Network Act (ICNA), Cybersecurity Management Regulations, Protection of Communication Secrets Act, and more. South Korea collaborates with its allies to enhance collective cybersecurity.

State of Israel

Israel is recognized as a major player in the cybersecurity industry. They have numerous cybersecurity start-ups, companies, government acts, and more. Additionally, Israel has a number of laws regarding cybersecurity. With laws ranging from Protection of Privacy Law, Computer Law, Critical Infrastructure Protection, and more. These laws ensure a right to privacy, and dictate what offenses are punishable, and the minimum protections important infrastructure sectors such as the energy sector must have. Israel collaborates with international partners in this field, whilst sponsoring and encouraging innovation in cybersecurity.

European Union

The European Union has a number of cybersecurity regulations which dictate and suggest what countries can do for better protection. Notably, the EU Cybersecurity Strategy which gives a general outline for how the EU wishes to go about cybersecurity. Further, the EU notably enforced the General Data Protection Regulation (GDPR), the EU Digital Services Act (DSA) as well as the Digital Markets Act (DMA) which were in the news in early 2023. As they were reason why the EU was unwilling to allow Meta’s app Threads to be downloaded from the app store. There were concerns about the how the app would use personal data.

The People’s Republic of China

The People’s Republic of China has some data protection regulations, and cybersecurity laws. The Cybersecurity laws include legal frameworks with provisions related to cybercrimes (such as accessing computer systems without authorization). Regarding data privacy, namely the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) are referenced. These laws contain provisions for data security, as a measure against personal data being breached (through hacking). These laws are considered positive, although China has gained some controversy for their governments use and access of personal data. China notably promotes ‘cyber sovereignty’, which entails a nation right to regulate internet activities within its own borders.

Timeline of Key Events

1988 Robert Morris creates the “Morris Worm”, one of the first major cyber-attacks. Gaining media attention and resulting in the first US felony conviction for cyber-crimes.

1990 The council of Europe adopted the “Convention on Cybercrime” (also referred to as the Budapest Convention). The objective was to pursue a common criminal policy aimed at protecting society from cyber-related crimes. The first international treaty dealing with cybercrime.

2001 United Nations adaptation of the “UN Convention against Transnational Organized Crime. Subsections include mentions of “encouraging countries to adopt measures to prevent and combat the use of information technology for the purpose of trafficking in persons”.

2005 The European Union Agency for Cybersecurity (ENISA) was founded. Their mission was to achieve a high common level of cybersecurity across the EU member nations.

2010 The International Cyber Security Protection Alliance (ICSPA) is a global organization set up to ensure funding, assistance and expertise can directly be offered to law enforcement cyber-crime units.

2016 The European Union passed the General Data Protection Regulation (GDPR). The regulation consists of data privacy requirements and is an important part of EU privacy laws.

2020 SolarWinds cyber-attack. This was an attack which targeted the SolarWinds Orion software. The software is a performance monitoring system, based in Texas, employed by several different organizations. The hackers gained access to the networks, the systems, and the data of several SolarWinds customers. Some of these companies being federal US agencies. This has been the largest attack of its kind to date. It was a supply chain attack, and the hack was encoded into an update, that once the new software was shared allowed the hackers access to a multitude of organizations. The attack was believed to have been perpetrated as a Russian espionage operation.

2020 As the COVID-19 pandemic was occurring, the World Health Organization (WHO) reported a number of cyberattacks targeting various healthcare organizations.

Previous attempts to solve the issue

The previous attempts to solve the issue have not yet been wholly successful. The UN has addressed this issue before. The UN has supported the Budapest Convention (The Cybercrime Convention held by the Council of Europe) and has made mention in a number of resolutions to the importance and need to strengthen cybersecurity.

International collaboration within cybersecurity does not yet formally exist between most countries. Rather the European Union collaborates to ensure a minimum cybersecurity standard, and companies and businesses converge to cybersecurity conventions for collaboration. However, there is no UN cybersecurity council. Thus, most references to cybersecurity made by the EU are when other topics are debated, and cybercrimes could tie in. Such as in 2001, when there were mentions of cyber protection and the use of information technology to help prevent human trafficking.

This is not to say that there are individual countries which lack any regulations or laws against cybercrimes. Rather, a large number of countries have adopted similar regulations surrounding data processing and the privacy of their citizens.

Possible solutions

Although nations are making an effort to avoid the misuse of data, the occurrence of most cybercrimes is not from the government. Rather cybercriminals try to mislead consumers into clicking the link (drive by download attack), giving up information (phishing, man-in-the-middle attack), or paying (ransomware). A solution which would work to decrease the number of victims to these cybercrimes would be educating the would-be victims. Ensuring they are aware of what these internet scams can appear as, and ensuring they are vigilant.

Additionally, requiring a basis level of security on tech products (devices and apps) which are distributed would help to ensure there are a fewer number of data breaches with sensitive information. An example of this would be the EU Digital Markets Acts which holds platforms accountable for what they do with consumer data, and how they protect it.

Further, the UN could promote the creation of a new IGO dedicated to cybersecurity advancements. This IGO could be responsible for research and innovation, as well as could work in conjunction with nation’s criminal taskforces to track down cybercriminals. This could be useful in solving and preventing cybercrimes which occur internationally.

Further reading

This is a link to a number of cybersecurity statistics. How many data breeches occur in different sectors, how many cyberattacks there are globally, where the sources are from, etc.

Fox, Jacob. "Top Cybersecurity Statistics to Know for 2023." *Cobalt*, Cobalt, 1 Sept. 2023, www.cobalt.io/blog/cybersecurity-statistics-2023#:~:text=How%20many%20people%20get%20hacked,over%20800%2C000%20attacks%20each%20year.

This is a link to the GCI (Global Cybersecurity Index), it is useful to be aware of the different factors that go into ranking countries, and to see on which fields countries need to improve.

"Global Cybersecurity Index." *ITU*, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed 22 Sept. 2023.

Bibliography

"10 Biggest Cyber Attacks in History: Clear Insurance." *Cyber Attacks Are on the Rise. Whilst Modern Technology Presents Many Conveniences and Benefits, There Are People Who Misuse It Which Poses a Threat to Businesses and Data Privacy Globally. When Data Breaches Happen, It Can Have a Far-Reaching Impact. It Goes beyond the Target Company, Affecting Customers, Suppliers and More. Scarily, Experts Expect The*, 19 June 2023, clearinsurance.com.au/10-biggest-cyber-attacks-in-history/.

"100+ Cybersecurity Terms & Definitions You Should Know." *ALLOT*, 20 Dec. 2022, www.allot.com/100-plus-cybersecurity-terms-definitions/.

Brush, Kate, et al. "What Is Cybercrime? Definition from Searchsecurity." *Security*, TechTarget, 23 Sept. 2021, www.techtarget.com/searchsecurity/definition/cybercrime.

Chief Cybersecurity Officer at Enisa | Euractiv Jobsite, jobs.euractiv.com/job/chief-cybersecurity-officer-254114. Accessed 22 Sept. 2023.

"China - Data Protection Overview." *DataGuidance*, 29 Aug. 2023, www.dataguidance.com/notes/china-data-protection-overview.

"Chinas Emerging Data Protection Laws Bring Challenges for Conducting Investigations in China." *DLA Piper*, www.dlapiper.com/en-us/insights/publications/2022/07/chinas-emerging-data-protection-laws-bring-challenges-for-conducting-investigations-in-china. Accessed 22 Sept. 2023.

Council of Europe, rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e. Accessed 22 Sept. 2023.

"European Network and Information Security Agency (ENISA) - Main Contents." *European Network and Information Security Agency (ENISA) - EU Monitor*, www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vh6tfw7n7epz#:~:text=ENISA%2C%20the%20European%20Union%20Agency,respond%20to%20information%20security%20problems. https://www.iap-association.org/getattachment/Resources-Documentation/IAP-Arrangements/MoU-International-Cyber-Security-Protection-Alliance-and-IAP.pdf.aspx#:~:text=The%20International%20Cyber%20Security%20Protection%20Alliance%20(ICSPA)%20is%20a%20global,both%20domestic%20and%20international%20markets. Accessed 22 Sept. 2023.

"Foreign Policy Cyber Security." *National Archives and Records Administration*, National Archives and Records Administration, obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity#:~:text=We%20are%20working%20to%20develop,liberties%20and%20rights%20of%20everyone. Accessed 22 Sept. 2023.

Fox, Jacob. "Top Cybersecurity Statistics to Know for 2023." *Cobalt*, Cobalt, 1 Sept. 2023, www.cobalt.io/blog/cybersecurity-statistics-2023#:~:text=How%20many%20people%20get%20hacked,over%20800%2C000%20attacks%20each%20year.

"Global Cybersecurity Index." *ITU*, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed 22 Sept. 2023.

Global Cybersecurity Outlook 2023 - World Economic Forum, www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf. Accessed 22 Sept. 2023.

Gov.Uk, assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf. Accessed 22 Sept. 2023.

"History of the Assembly." *Global Privacy Assembly*, globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/. Accessed 22 Sept. 2023.

"If so Much Cybercrime Is Undetected and Unreported, What's the Answer?" *Axim*, 20 June 2022, www.aximglobal.com/if-so-much-cybercrime-is-undetected-and-unreported-whats-the-answer/#:~:text=The%20Department%20of%20Justice%20(DOJ,left%20hidden%20in%20an%20organization.

Korean Policies of Cybersecurity and Data Resilience, carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164. Accessed 22 Sept. 2023.

LmunA 2023

Saheed Oladimeji, Sean Michael Kerner. "Solarwinds Hack Explained: Everything You Need to Know." *WhatIs.Com*, TechTarget, 27 June 2023, www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

"Ungge 2021 Report :: Eu Cyber Direct." *Horizon*, eucyberdirect.eu/atlas/sources/ungge-2021-report. Accessed 22 Sept. 2023.

"What Is Malvertising?" *GeeksforGeeks*, GeeksforGeeks, 17 Aug. 2022, www.geeksforgeeks.org/what-is-malvertising/.

"What Is the Morris Worm? 5 Things to Know: Security Encyclopedia." *What Is the Morris Worm? 5 Things to Know | Security Encyclopedia*, www.hypr.com/security-encyclopedia/morris-worm#:~:text=The%20Morris%20worm%20functioned%20as,explore%20whether%20it%20could%20operate). Accessed 22 Sept. 2023.