Surrey Model United Nations 2019

European Union

BACKGROUND GUIDE

Director's Letter

Dear Delegates,

My name is Isabela Moise, and as your Director I would like to welcome you all to Surrey Model United Nations 2019. As a Grade 11 IB student at Port Moody Secondary, I can decidedly say that Model United Nations is one of the most strenuous yet rewarding activities to be a part of.During my first conference, I had unintentionally registered for an advanced committee, but during the sessions I soon became enchanted by the rapid-fire debate, intellectual rebuttals, and complex stances expertly portrayed by experienced delegates. Absolutely engrossed, I continued to partake in MUN, motivated to perform at the same level as those amazing debaters. It is this moment of ignited passion that I wish for each and every one of you to experience, whether you are a budding delegate, or a wizened veteran. And this love of MUN comes with many added advantages, such as the well-appreciated dive into diplomacy, as well as knowledge into international relations and current events.

As your dais team, Andrew Liu and I will ensure that you will have a stellar time at SurreyMUN. Both Andrew and I are proud to be a part of the SurreyMUN team. We are happy to meticulously prepare to ensure that each and every delegate has an exciting and memorable MUN experience.

Optimizing your time here at Surrey MUN is a two-way initiative, one that rests in your hands as well as ours. Before even stepping into the conference, be sure to equip yourself with innovative, accurate, and well-founded solutions and points of discussion. But most importantly, regardless of how thoroughly you understand the topic of cyber safety, or how lengthy your compilation of solutions is, without any vocal contributions, all of your preparation would be for naught. So remember: even the greatest of orators began as terrible speakers, but they improved through practice. Ready yourself with strong arguments, and arm yourself with confidence to share, contribute, and debate. With that, I look forward to everything this committee has to offer; alongside Andrew Liu, I await this conference in anticipation.

Best Regards,

Isabela Moise
Director of EU

Committee Description

Established in 1945, the European Union was intended to maintain stability between European neighbours out of the Second World War.To achieve such a vision, economic and political partnerships were cemented, with the first, the European Coal and Steel Community, in 1951. The goals of the EU are vast, with themes surrounding human dignity, freedom, democracy, equality, rule of law, and human rights[1]:

The EU also serves as the largest trade bloc in the world, with free trade being one of its fundamental principles. To this end, the EU is committed to liberalizing world trade, enabling nations internationally to benefit. In addition, the EU contributes to humanitarian aid by assisting victims of both man-made and natural disasters worldwide. The EU is integral to diplomacy and strives to foster stability, democracy and fundamental freedoms on an international scale, seen through their heavy involvement in world affairs.

In recent years, the topic of cyber safety has emerged as a pressing issue for the EU. The threat of a cyber attack against individuals or countries has the potential to cause damage economically, politically, and socially. This issue intensifies as technology moves forward. Already, both internationally and within the EU, the magnitude of cyber attacks has been displayed, with the tremors still reverberating throughout Europe. As the EU faces increasing pressure to address cyber safety, delegates must fashion solutions to account for all actors in this topic.

Topic Overview

Technology has ingrained itself upon every level of society, from individuals as they utilize online social media, to businesses that stash blueprints within the cloud, to governments as they host elections and rely on online campaigning. While such a reality promotes connectivity and allows economies to flourish, if left unsecured, damage and consequences may ensue.

As shown in recent years, massive demonstrations of warranted fear and indignation erupted after the revelation of numerous cyber attacks against nations. An example of this is within the Kremlin's meddling in the US elections. Another pressing instance within the EU was Estonia's involvement in the world's first cyber war, resulting in the downing of Estonian banks, media outlets, and government bodies. As many as 80% of European companies have experienced at

[1] https://europa.eu/european-union/about-eu/eu-in-brief_en

least one cyber incident during 2017.[2] This statistics stresses upon the vulnerability of enterprises against malicious cyber attacks, and the potential information and tools of firms and clients alike that could be jeopardized. Even individuals fall prey to online attacks, as internet users across Europe experience more than 4,000 ransomware attacks every day.[3] This staggering reality is far-reaching to every niche in society, indicating that no one is exempt from these attacks, and is an issue pertinent to all of society. In light of these developments, the EU has faced growing pressure to reinforce their defences against cyber attacks, as it is critical to ensure that devices and networks alike are protected and equipped to deter cyberattacks.

Timeline

1989 - The Morris Worm

The Morris worm was one of the first recognised malware attacks to affect the world's budding cyber infrastructure.[4] The worm was a standalone malware (software intentionally designed to cause damage to a computer, server or computer network program that would replicate itself and spread to other computers.)[5] This attack served as the first warning for nations that the internet's connectivity could serve as a vulnerability to information, as well as a benefit.

2000 - MafiaBoy

A Canadian 15 year old by the name of Michael Calce unleashed a Distributed Denial of Service (DDoS) attack on numerous renowned commercial entities such as Amazon, CNN, eBay, and Yahoo in 2000. This attack made these online services unavailable by overwhelming them with traffic from multiple sources.[6] The attack further emphasized the array of vulnerabilities that large internet presences were exposing. Fearing further damage, entities began cyber safety initiatives to compete with the adeptness of hackers.

2007 - The First Cyber War

In 1947, the Bronze Soldier was unveiled in Estonia as a representation of the USSR's victory over Nazism. However, ethnic Estonians saw the Red Army soldiers as occupiers, not liberators,

---

2 https://www.orange.com/en/content/download/44597/1336574/version/2/file/Le%20paquet%20cybersecurite_VA_CLEAN.pdf

3 https://www.orange.com/en/content/download/44597/1336574/version/2/file/Le%20paquet%20cybersecurite_VA_CLEAN.pdf

4 https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

5 https://searchsecurity.techtarget.com/definition/malware

6 https://www.digitalattackmap.com/understanding-ddos/

and viewed the Bronze soldier as a painful reminder of the war. In response, the Estonian government decided to move the statue to a military cemetery in 2007, which sparked outrage in Russian-language media. As a result, Estonia was bombarded with cyber attacks wherein online services of Estonian banks, media outlets, and government bodies were halted by unprecedented levels of internet traffic seen as a torrent of spam sent by botnets and a flood of automated online requests that overwhelmed Estonian servers.
Such actions caused a massive state of confusion and panic before order could be restored, and its effects are felt to this day. Estonians remain advanced in their cyber safety capabilities, and a deep hatred has been cemented against Russians who would support the attack.

2008 - Georgia Hacked

Computer networks in Georgia were hacked by a group of Russian hackers with close links to the Russian mafia and government. The attack was specified to be similar to that of Estonia's sufferance. The Georgian Government stated that the disruption was caused by attacks carried out by Russia as part of the two nations' conflict with regards to the Georgian province of South Ossetia. This additional Russian attack sparked outrage as well as fear within the international community, as Russia asserted itself as a powerful online force that was to be respected and monitored.

2009 - Israel Suffers From a Major Cyber Attack

Attacks against Israel's cyber infrastructure during their January military offensive in the Gaza Strip briefly paralyzed government sites, and was a result of a coordinated plot executed by an estimated half a million computers. Due to its resemblance to the attacks on Estonia and Georgia, Israeli officials suspected Russia of the crime, under the sponsorship of Hamas. Most strikingly of the attack was the 3 hours downing of the Home Front Command's site.

The attack was unprecedentedly severe, and consisted of four waves that continually increased in intensity, peaking at 15 million junk mail deliveries per second. In total, 2,500 websites were defaced during the attacks, while several databases were leaked online.[7][8] This attack eradicated the sense security within Israel, as citizens and government members alike became painfully aware of their weak status in comparison to cyber dominators such as Russia. Spurred by these sentiments, Israel has launched multiple initiative to better their security response, in order to re-assert citizen's confidence within the government.

[7] https://www.haaretz.com/1.5065382

[8] https://www.businessinsider.com/israel-faced-a-wave-of-cyber-attacks-2014-8

2009 - Google's Chinese servers are hit

Always a tumultuous subject, Google's presence within China was rife with compromise and disgruntled dealings. A striking moment between Google and the Chinese government took place when Google detected a security breach involving Chinese bugs. Reports revealed that hackers had gained access to several of Google's corporate servers and intellectual property, with a prime interest in accessing the Gmail accounts of Chinese human rights activists. Upon further investigation, it was brought to light that numerous Gmail accounts of human rights advocates in China located in the United States, China, and Europe had been routinely accessed without authorization. The primary suspect was the Chinese government, due to its past of flagrant disregard for human rights. These cyber attacks compelled Google to re-evaluate its presence within China, before finally relocating servers to Hong Kong in order to escape China's repressive tendencies.

2009 - Biggest Fraud Case in US History

Over 90 million credit and debit card numbers were stolen from TJX, Office Max, Dave and Busters restaurant chain, Barnes and Noble, and other retailers by a group of cyberthieves in 2009.[9] The perpetrators were in search of poorly protected wireless networks and found easy access into several retailer networks. Once accessed, the hackers would force their way into the corporate network, where they siphoned transaction data in real time from the magstripe data on credit and debit cards. This crime involved the decryption of PIN codes, which was the first of its kind, and shook government agencies and retailers to their cores, forcing them to face the obvious inadequacy of their security as well as the rising advances of hacking potential.

2012 - Red October

"Red October" was the name given to the exploit that stole sensitive information from leading infrastructural websites such as embassies, oil and gas institutes, nuclear stations, trade and aerospace targets, and smartphones of government workers. The victimized organizations were located worldwide, from Eastern Europe, former USSR member states, as well as countries in Central Asia, Western Europe and North America. The attack involved malware that was sent into an entities' system, which then attacked the encrypted information with software used by that of the European Union and NATO. Following the victim's opening of the malicious document on a vulnerable system, the embedded code initiated the setup of the viral software

[9] https://www.wired.com/2010/03/tjx-sentencing/

onto the machine, allowing for communication with the master server run by the hackers and supplying the system with additional spy modules. It is estimated that over 7 terabytes of data was stolen, which included geopolitical intelligence, credentials to access classified computer systems, and data from personal mobile devices and network equipment. [10]The attack identified "soft targets", or entities that were severely lacking in cyber security, despite the valuable information they stored, compelling the victims to better their safety. In addition, "Red October" can be credited with other attacks that occurred following the event, as the sloen information was utilized to further political agendas and aggressive acts against nations.

2016 - Presidential Campaign Hacking

In what can be described as a series of unfortunate events, the FBI contacted the Democratic National Committee's help desk to warn the IT department of a malware breach, transmitting electoral information back to Russia. However, the DNC management was never properly notified of the breach. Further on, following a suspected phishing email requesting the email of the campaign chairman, which was duly supplied, hackers working for the Russian government accessed the DNC computer system. An onslaught of executive emails and addresses ensued, oppositional research on Donald Trump, cell phone numbers, staffer's email and chat exchanges were obtained. Following the naming of the Russian government as the perpetrator, their mission of swaying the public towards Donald Trump through a slew of stolen emails and correspondences of the Democratic party was exposed. Many have questioned the integrity of the 2016 election, as well as Donald Trump's legitimacy as president, having been elected through a tampered process that some claim as undemocratic.

Historical Analysis

When the first computer worm was developed in 1989, threats against online infrastructure became apparent. This Morris Worm spread around computers primarily in the US and made itself known by slowing down computers to the point of unusability. 6,000 computers were affected, amounting an estimated USD 10 - $100 million in repair bills.[11] Many took steps to protect themselves from these dangers, investing in rudimentary computer defense software such as firewalls. From 1990 - 1999, many computer viruses designed to spread from one computer to another were developed. Malware like this invaded via users' email, damaging systems worldwide, becoming the first incidents of cyber-vandalism on a massive scale.

[10] https://www.adaware.com/blog/operation-red-october-the-astonishing-hacking-ring-that-shook-the-world

[11] https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

However, until this point, these malicious programs remained ill-intended but otherwise harmless, with its main purpose being to showcase weaknesses in online infrastructure. But following the turn of the 21st century, hackers began to take advantage of this weakness, with large-scale attacks ranging from credit card fraud, such as in the TJX fraud case, to the DDoS attacks on national sites, like those of Estonia, Georgia, and Israel. The repercussions of these actions hindered the very lives of citizens, and caused nationwide panic and fear. Within Estonia, for example, citizens were unable to withdraw money from ATMs or access other online services. Communications were also hindered, as newspapers and broadcasters were unable to upload articles to be printed in time, and government employees could not communicate with one another via email. Georgia experienced similar grievances, wherein official websites such as the central government site, as well as the homepages for the Ministry of Foreign Affairs and Ministry of Defence, were downed in a DDoS attack in which hackers directed their computers to simultaneously flood a site with thousands of visits in order to overload it and bring it offline. Furthermore, during the cyber attack against Israel, the command site was designed to instruct citizens in the specific of protecting themselves from cyber attacks, and the closing of this resource threw citizens into further panic.

The motivation behind these attacks vary among economic, personal, ideological, or political reasons. Often, financial gain act as a strong motivator for cyber attacks. Industry experts estimate that these attacks resulted in about $1.6 billion in repair expenses in 2000 alone. Developing malware, phishing, performing identity theft, and carrying out money request attacks appeared to be a secure and lucrative exploit, as seen by the nearly USD 700 million per year garnered through attacking online banking accounts in 2015 alone[12]. If not financially motivated, cyber criminals tend to be driven by passion, anger, indignation, or an array of other powerful emotions. Evidence of this can be seen within disgruntled employees, who claim nearly 47%of cyber attacks against global organizations.[13] This statistic speaks to the online vulnerabilities that companies reveal to employees. In other words, it is possible to surmise that more focus should be directed towards securing internal systems, in addition to strengthening external defenses, in order to avoid an attack from the inside. Many attacks are carried out for ethical, ideological, or moral reasons, with the intent to damage or disable online infrastructure to attack an individual, corporation, organization or government. Lastly, a commonality among many notorious cyber attacks is that foreign governments incite attacks for political gain.

[12] https://globalnews.ca/news/2332720/your-online-bank-account-at-risk-of-a-cyber-attack/
[13]https://www.ft.com/content/b7dbc0de-1b04-11e8-aaca-4574d7dabfb6

Comprehending the motivations that spur attacks against a variety of entities allow for the identification of perpetrators. The efficient condemning of the guilty parties can serve as a deterrent for future attacks, as well as enables persecutors to minimize the consequences that may have been brought about by the attacks. Furthermore, predicting the reason behind potential attacks allows entities to accurately forecast which information is the most coveted, and can act accordingly by strengthening security.

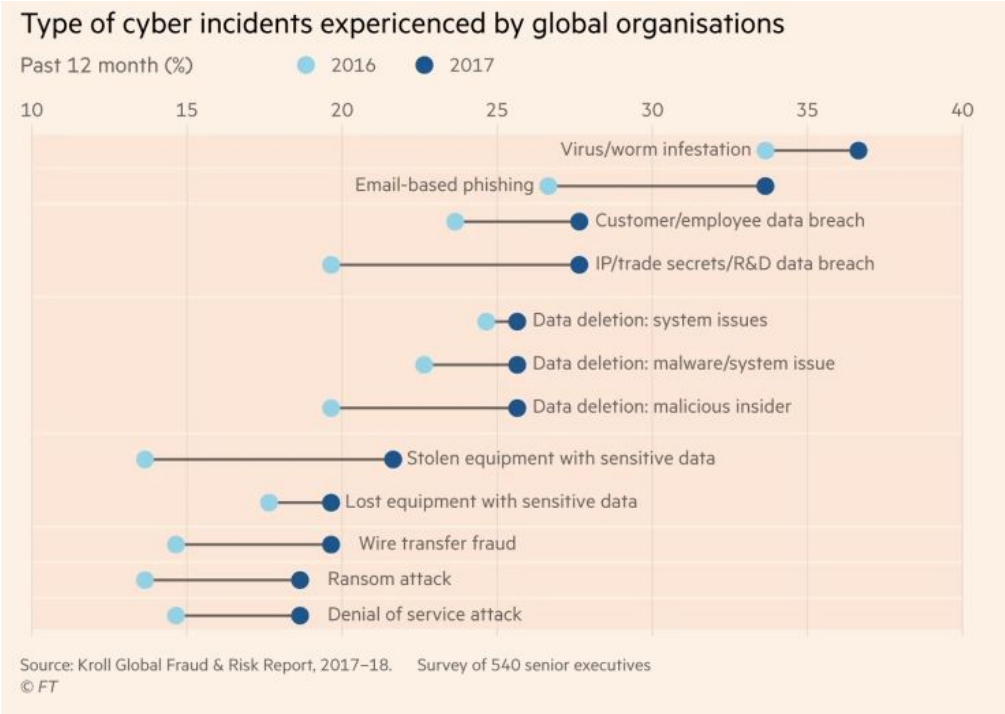
The reason that cyber warfare can bear a more powerful appeal than that of physical battle is that smaller nations, like that of North Korea, are able to obtain equal footing with global goliaths like the United States, at a fiscally responsible cost. North Korea alone boats 1,800 cyber warriors, a significant figure for a nation of 24.9 million people, supported by little to no centers of higher learning.[14] This case is common for many small nation-states, especially for those that lack universities with notable computer science programs, as cyber warfare has been deemed as a wiser investment than conventional weapons. There are many reasons that can be attributed to the profitability of online attacks, such that smaller countries are able to execute attacks without as much risk of being detected and persecuted.

Despite the inability to employ a large amount of resources in comparison to countries such as America, which invested $110 million in Plan X, a "foundational cyber warfare program", smaller nations can remain just as effective with a smaller digital army.[15] In addition to an alternative to conventional weapons, cyber war programs can also assist small nation sin developing further through theft of another nation's advanced commercial or military technology. Stealing advanced information serves as a more financially conscious action than investing billions in discovering such innovations for oneself, bringing about the consensus for smaller nations: "Why build it when you can steal it?" In fact, due to its economical and destructive efficiency, more than 140 countries have some level of cyber weapon development programs, with only more to come during the 21st century.[16] It is best to understand the full scope of what cyber warfare offers, be it to individuals or entire state-nations in order to best combat each potential perpetrator.

Current Situation

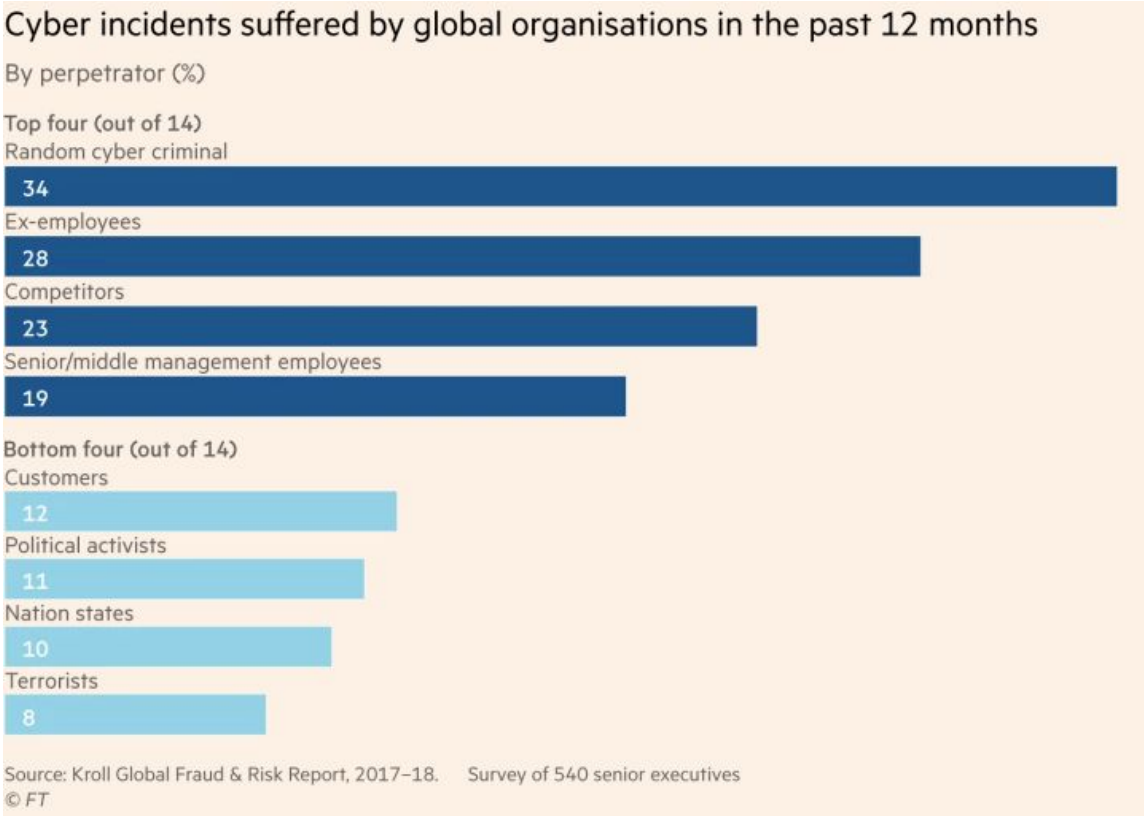
The type of cyber incidents experienced by global organisations has only multiplied, with hackers enhancing their methods and means, while online entities scramble to fend them off.

[14] http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/
[15] https://www.cccblog.org/2012/06/01/early-details-about-darpas-five-year-110-million-plan-x/
[16] http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/



Such cyber threats faced by organisations and nations alike are considered the "new normal", with perpetrators emerging from a variety of different sources, ranging from random cyber criminals, to terrorists, to disgruntled employees. Within recent years, attacks such as worms, virus', phishing, etc. have increased exponentially in both volume and intensity as the overall level of sophistication rose meteorically. This can be seen in the fact that 36%[17] of companies surveyed within a Kroll survey had been affected by a virus or worm attack, - a rise of 3% from 2016, while 33% had suffered an email-based phishing attack, 27%[18] had suffered a data breach, and 25% were affected by data deletion. The major flaw that nation states, businesses and individuals all bear is that while they continue to prioritise cybersecurity, cyber resiliency remains lacking, - that is if complacency has not drowned out all efforts of cyber safety to begin with.

[17] https://www.scmagazineuk.com/cause-recent-cyber-attacks-complacency/article/1474019
[18] https://www.ft.com/content/b7dbc0de-1b04-11e8-aaca-4574d7dabfb6



Cyber Security

Cybersecurity refers to methods and processes of protecting electronic data.This includes identifying electronic data, as well as implementing technology and business practices that will protect it. The processes and methods within this line of work is designed to deter cyber criminals, and prevent an attack from occurring, thereby sparing any servers or systems from harm.

Cyber Resiliency

Cyber resilience refers to the ability to respond and recover effectively to online attacks as well as to resume operations quickly. This is to assume that the cyber security methods have failed, and the perpetrators have compromised the system in whatever malware form they have used. As a result, procedures executed by individuals and programs alike are then required to minimize the damage of the hack, and measures that were previously put in place are authorized to eliminate the threat.

UN Involvement

Recognizing the threat that the lack of cyber safety can induce upon countries, both the United Nations and the European Union have worked in succession to combat the online threats. Within the UN, there was much criticism that member were not taking the issue of cyber safety gravely enough. In response to these claims, and the growing pressure to address the ever-increasing tide of danger, the UN formed the United Nations Group on Cybercrime and Cyber Security[19]. The purpose of this Group is to forge policies in regards to cybercrime and cyber security , as well as ensure the collaboration and organization between member nations. One of the main tasks of the Group was to develop a draft policy on cyber crime and cyber security that focuses upon external factors. The most important policy was in regards to the methods that the UN could use to mainstream cybercrime and cyber security issues into national programs. In addition to this Group, a session of the UN was held for the sole purpose of conveying the importance of cyber safety, highlighting the growing impact of cybercrime, the enormous resources lost, the risks posed to the UN's electronic support of members, and the targeting of the UN's own systems. Finally, an impressive feat was accomplished by a wide array of lead organizations within the UN working in conjunction, including UNESCO, UNODC, UNDP and UNCTAD to develop an action plan to protect the work of the United Nations system and those that are served by them. This plan was composed of resolutions, which included principles and actions for specific organizations to enact, while constituting an important step for the UN system working together to make cyberspace a safer place.

In regards to the EU, in September of 2017[20], the European Commission passed policies and legislation of their own, in an attempt to expand the EU's Cybersecurity structures and build a greater resiliency. The plan was composed of three main pillars: building greater resilience, enabling a robust deterrence against cyberattacks, and a global vision for cybersecurity strategy and defence cooperation. Within the new strategy of resiliency, the directive aims firstly to improve the EU's cyber resilience by promoting cyber hygiene, with a shared belief that cybersecurity is a common societal challenge, with obligations set amongst all types of entities, including digital service providers who are now compelled to notify authorities and the general public of any type of security breach within no more than three days. In terms of deterrence, the

[19] https://www.unsystem.org/content/action-cybercrime-and-cyber-security
[20] https://www.unsceb.org/content/action-cybersecuritycybercrime-0

directive aims to discourage cyber criminals and attackers from committing offenses through improved technology. The proficiency of this detection technology is meant to serve as discouragement that will instill doubt and fear of consequences upon the potential perpetrators, dissuading them from attacking before they even begin. Finally, as the digital world knows no border, a priority was stated to encourage cross-border information-sharing in Europe and beyond, as well as the promotion of a strengthened international cooperation to facilitate prevention and deterrence of cyber attacks. In addition to this directive, a new law was passed to implement an unprecedented EU-wide labelling system that would enable executors to measure cybersecurity standards of items sold in EU countries, and consumers to become more aware of the capabilities of those that claim to protect data more effectively.

Possible Solutions - 1 page

The issue of cyber safety is one that permeates countries, businesses and individuals. A number of different solutions and methodologies have been suggested and implemented within these different scopes. Some bearing different themes, such as concentrating on cyber security during an attack, to focusing on disabling an attack before it even begins.For the most viable success, a diversity of solutions must be combined in order to fabricate a versatile resolution that can tackle all of the complicated facets of the issue. Even within the scope cyber security and cyber resilience, an array of different methodologies are continuously present and being proposed.

Resilience

In this strategy, an essential prerequisite is the mechanisms for resiliency. As stated previously, Cyber resilience refers to the ability to respond effectively to online attacks if they were to occur, as well as to recover and resume operations quickly. One method of completing this is by implementing mandatory automatic backing up of data regularly. This is to combat sophisticated ransomware attacks that encrypt all data, as hackers demand a ransom and threaten to destroy all of the information if demands are not met. Fortunately, if institutions are compelled to keep thorough and regular backups on a separate network,restoring any wiped data becomes a secure and efficient solution. However, this can lead to further issues, in terms of feasibility, and the requirement to create and obtain an entirely new network. This is also under the assumption that this network is not compromised as well, and the data is free enough to risk being placed in two locations. For entities such as governments with more sensitive information, many may refuse this method unless given a better alternative, for fear of exposing themselves to further information leaks. Another suggested solution is the implementation of mandatory security incident simulations, similar to that of emergency practices during natural disasters. As is customary with mandatory fire drills across all entities, assuming the mentality of an incoming attack with regards to data breaches can assist in strengthening cyber resiliency. This allows organizations to review the techniques that must be executed in the event of a true cybersecurity

incident. This is turn can improve confidence among stakeholders, and employees alike. It should be noted that the execution for this may be overly complicated, taking precious time from businesses,- an aspect that may compel many to object to such policies. Furthermore, including cyber safety as part of academic and vocational training curricula will ensure individuals are more prepared the day of an attack, and can therefore minimize the damage done unto the entities.

Deterrence

As previously mentioned, deterring criminals and online attacks before they even begin is a recommended tactic to avoid the need for cyber security initiations. As such, the most effective defence against cyber attacks is preventing one from occuring at all, through the implementation of enhanced technological forensics. These improved forensics would gain notoriety such that it would deter cyber criminals, for fear of being caught and punished. Although such improved cyber forensics could come at a cost of personal freedom and privacy, such as with the uptake of the new IPv6[21] (Internet Protocol version 6) as it provides the clear benefit of assigning to users a unique IP address for identification purposes and location definition. As such , this collection of IP addresses themselves have the potential of falling into the wrong hands, which would result in a devastating leak of personal information. If this practice was widespread, it would facilitate online investigations and help identify malicious actors faster, but may also expose a new line for hackers to identify and target individuals.

Defence Against Structural Weakness

Beyond the preventative tactics that may dissuade criminals, implementing strong defensive initiatives if, - or more likely when an attack occurs will enable entities to minimize the attack. The present environment in which cyber crime is committed also serves to explain the prevalence of the phenomenon. Despite the fact that an exponential amount of personal and sensitive information is stored online, thereby increasing the incentive for hackers in their search of potential rewards, neither computer security nor applications like email filters have improved dramatically in terms of coverage[22]. According to the anti-virus manufacturer Norton, for example, as many as 41% of computers did not have up-to-date security protection in 2012. This leads to a significant weakness within computer systems and networks, as even the most basic of

---

21 https://www.orange.com/en/content/download/44597/1336574/version/2/file/Le%20paquet%20cybersecurite_VA_CLEAN.pdf

22 http://i.viglink.com/?key=535fb381c276aba2df16c56f4cdce13c&insertId=e0a61f5be34123fe&type=CD&exp=-100%3ACILITE%3A10&libId=jlk3to3e01021li9000DLjfm4ct5i&loc=https%3A%2F%2Fitstillworks.com%2Fcauses-cyber-crime-1846.html&v=1&iid=e0a61f5be34123fe&out=https%3A%2F%2Fwww.ebay.com%2Fsch%2Fi.html%3F_nkw%3Dcomputer&ref=https%3A%2F%2Fwww.google.ca%2F&title=Causes%20of%20Cyber%20Crime%20%7C%20It%20Still%20Works&txt=%3Cspan%3Ecomputer%3C%2Fspan%3E

securities are not consciously implemented. As a result, implementing policies and regulations that mandate the establishment of security protocols and programs can allow users to inevitably become more protected against minor attacks. However, an issue that has arisen in the past is if a conventional security program or operating system is universally utilized, everyone is made vulnerable if a back door, or weakness is found within the security. This in turn calls for regular updates and internal attempts at hacking, and developing the defense measures in a continuous cycle, - a costly and inconvenient feat for any entity.

Bloc Positions

Northern European countries

These prosperous nations are most prominent in championing the relevance of cybersecurity. However, they are tired of picking up the tab for southern Europe and are fighting for more control over the south's fiscal policies, especially in terms of future funding initiatives, like those that will take in place towards furthering online safety.

Southern European countries

These nations wish the opposite. As a result, while they deem cybersecurity is a prominent issue, they wish to deal with it more independently, as opposed to having an enveloping, cohesive solution/project, they wish to develop more personalized solutions, that cater to the country, and that promotes independence.

Top EU Countries for cyber-security[23]

Estonia

Despite the size of this northern European country, they are fierce in the cyber security field. Driven by the 2007 attack, which was the first large-scale coordinate online attack, Estonia has dramatically increased security, and has been credited with paving the way in online data protection. Improvements have included further safety on national networks, the development of a decentralized system and added digital components to its digital infrastructure. As Estonia becomes increasingly confident within the online sphere, the country invests more of its identity online, with acts allowing citizens to vote in general elections online.

[23] https://www.itu.int/pub/D-STR-GCI.01-2017

Norway

Similar to that of other Nordic countries, Norway has put in place a dedicated cyber defence unit. The unit acts based on a culmination of expertise of military, national security and police security intelligence.

Germany

Germany has gone great lengths to maintain a strong cyber security presence, following the attack in 2015 wherein government websites were hacked by group demanding Berlin cease in their support or the Ukrainian government. In response to this attack, the German government created the National Cyber Defence Centre as well as the National Cyber Security Council. In addition, to protect industries and individuals from potential threats, Germany has passed legislation requiring more than 2,000 essential service providers to implement new information security standards or risk facing severe penalties.

United Kingdom

Cyber security is an issue that remains a top priority, with the UK government's £860 million investment within the Cyber Security Strategy was implemented in 2011. Initiatives they have implemented include a voucher scheme to help the UK's SMEs (Small and medium sized enterprises) protect themselves from cyber crime. In addition the government's intelligence-gathering operation (GCHQ) and the Ministry of Defence collaborate to help counter threats to the UK.

Netherlands

The Netherlands launched the Dutch Cyber Security Council, or DCSC, and began their initiative towards becoming a cyber security power. The DCSC represents a cross-section of industries from both the private and public sectors. Based upon DCSC reporting, the Netherlands has one of the highest percentage of internet users in the world, and legislators keep this in mind as they continuously update policies and focus their efforts towards investigation and prosecution of cyber crimes.

Latvia

Latvia has in place a Cyber Security Strategy that was based upon insights that the country gained during its time as the head of the European Council. The initiative is designed to develop and implement cyber-cleanliness in everyday work with IT. Furthermore, Latvia has established a Cyber Defence Unit compiled of experts from the pubic and private sectors that discuss and advise future policies to shield entities from malicious online attacks.

Finland

Alongside its aforementioned allies, Finland is a global forerunner in cyber-security. Counterintuitively, Finland boasts thousands of worms, malware and viruses designed to protect the country's military, government, businesses and critical infrastructures against cyber-attacks.

Sweden

Similar to that of the Netherlands, Sweden has established a cross-sector approach to cyber-security. Not only that, but it continues to expand its defence network to harness the technical expertise of the private sector and to facilitate a better-inform policy making process. The communication between all Nordic countries allows for the promotion of information exchange and the addressing of all issues surrounding cyber-security. This display of transparency allows for universal learning and development to better the security of each nation.

Top EU Countries in need of cyber-security[24]

Matla

Considered the most vulnerable country in the EU, Malta suffers from an array of vulnerabilities. This is due to Malta's exceptionally high percentage of exposed internet connections of 73%, as well as its lack of cybersecurity legislation and poor international cooperation. [25]

Greece

Similar to that of Malta, Greece bears 77% of exposed nodes, and contains an annual 22% average rate for malware encounters reported by citizens.[26] Furthermore, the nations' priorities lie elsewhere, primarily the condition of the economy and the employment rate of their citizens, indicating that any cyber security initiatives will be as a reaction to an attacks, versus the proactive initiative taken by other nations.

Romania

Despite Romania's status as the center of international cyber fraud investigators, harboring a brilliant legion of former criminal hackers who have helped the country compete above its status in the tech industry, it remains vulnerable. With a cyber vulnerability score of 41% as of 2018, as well as 18% of the population who have experience cybercrime, Romania is a soft target waiting to be assaulted. [27]

[24] https://www.itu.int/pub/D-STR-GCI.01-2017
[25] https://www.websitebuilderexpert.com/eu-cybercrime-risk/
[26] https://www.websitebuilderexpert.com/eu-cybercrime-risk/
[27] https://www.websitebuilderexpert.com/eu-cybercrime-risk/

Guiding Questions

1. Cyber attacks have increased as technology advanced, and yet some nations continue to fall behind. Why does this happen, and what can be done to ensure a level technological playing field?
2. What are the implications of a cyber war against countries? How can consequences be mitigated?
3. Is there a specific group that nations should focus upon in terms of those that perpetrate online attacks? Should nations as a whole, or specific groups be deemed a more notorious threat to be focussed upon such that their actions are combated?
4. Consider the future possibilities of cyber attacks as smaller and less militarily-able countries gain further access to technology, in addition to as larger nations become more brash in their ways of online attacks, as well as how such battles can be avoided
5. Consider the human element of cyber attacks, in terms of the lack of preparedness that ost entities face in spite of the rising threat of online attacks. Why do you think this is so, and how can this be minimized, and entities better equipped?
6. Businesses are especially prone to online attacks, especially those without the technological expertise to avoid online attacks. Should there be government assistance, or mandated programs/policies? How will the business' resources and financial capabilities be factored into the initiatives implemented to assist in their securing of online data?
7. Within the path towards implementing solutions, consider how much your country values the individual freedom of its citizens in contrast to combating cyber threats? Where is the line drawn between the security of citizens, and the imposition on their privacy and freedoms?
8. Should there be a better effort in promoting awareness of cyber safety among populations? Is this a serious issue in your country? Why or why not, and how can this situation be rectified to establish a better-secured nation?

Further Readings

http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-cyber-security-package

https://www.bbc.com/news/39655415

https://www.csoonline.com/article/3269726/hacking/what-is-cyber-resilience-building-cybersecurity-shock-absorbers-for-the-enterprise.html

https://itstillworks.com/causes-cyber-crime-1846.html

https://www.unsystem.org/content/action-cybercrime-and-cyber-security

https://www.ft.com/content/b7dbc0de-1b04-11e8-aaca-4574d7dabfb6

Bibliography

"2016 Pres. Election Investigation Fast Facts." CNN, Cable News Network, 28 Jan. 2019, www.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html.

"2016 Presidential Campaign Hacking Fast Facts." CNN, Cable News Network, 24 Nov. 2018, www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

"Action on Cybercrime and Cyber Security." Expenditure by Agency | United Nations System Chief Executives Board for Coordination, 3 May 2013, www.unsystem.org/content/action-cybercrime-and-cyber-security.

"Action on Cybersecurity/Cybercrime." United Nations Environment Programme | United Nations System Chief Executives Board for Coordination,

"EU2017." EU2017.MT, www.eu2017.mt/en/Pages/A-Brief-History-of-the-EU.aspx

"Operation Red October: the Astonishing Hacking Ring That Shook the World." Adaware,

www.adaware.com/blog/operation-red-october-the-astonishing-hacking-ring-that-shook-the-world.

“Significant Cyber Incidents.” Nuclear Stability in a Post-Arms Control World | Center for Strategic and International Studies, Center for Strategic and International Studies, www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

“The Council of the European Union.” Acuerdos Internacionales Sobre Acción Por El Clima - Consilium, Consejo De La UE, 5 Oct. 2017, www.consilium.europa.eu/en/council-eu/.

“Top 10 Most Notorious Cyber Attacks in History.” ARN, 4 Feb. 2019, www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/.

“Why Cyber Warfare Is so Attractive to Small Nations.” Fortune, Fortune, fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/.

Bell, Terena. “What Is Cyber Resilience? Building Cybersecurity Shock Absorbers for the Enterprise.” CSO Online, CSO, 7 May 2018, www.csoonline.com/article/3269726/hacking/what-is-cyber-resilience-building-cybersecurity-shock-absorbers-for-the-enterprise.html.

Bond, David. “More Countries Are Learning from Russia's Cyber Tactics.” Financial Times, Financial Times, 15 Mar. 2018, www.ft.com/content/b7dbc0de-1b04-11e8-aaca-4574d7dabfb6.

EU. “The EU in Brief.” European Union, Publications Office of the European Union, 4 July 2018, europa.eu/european-union/about-eu/eu-in-brief_en#the-eu-in-the-world.

EU. “The History of the European Union.” European Union, Publications Office of the European Union, 24 Jan. 2019, europa.eu/european-union/about-eu/history_en.

European Central Bank. “Cyber Resilience.” European Central Bank, www.ecb.europa.eu/paym/initiatives/cyber-resilience/html/index.en.html.

European Central Bank. “Why Is Cyber Resilience Important?” European Central Bank, www.ecb.europa.eu/explainers/tell-me/html/cyber-resilience.en.html.

European Union “History of the European Union.” EU, europarlamentti.info/en/European-union/history/.

European Union. How the European Union and the United Nations Cooperate.

Ingersoll, Geoffrey. “Mercenary Hackers Appear To Be Behind An Insane Global Espionage Campaign.” Business Insider, Business Insider, 15 Jan. 2013, www.businessinsider.com/red-october-cyber-espionage-campaign-2013-1.

McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” BBC News, BBC, 27 Apr. 2017, www.bbc.com/news/39655415.

Mercer, Edward. “Causes of Cyber Crime.” It Still Works, 10 Jan. 2019, itstillworks.com/causes-cyber-crime-1846.html.

Nato. “The History of Cyber Attacks - a Timeline.” NATO, www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.

Olcott, Jake. “Cybersecurity Vs. Cyber Resilience: A Quick Comparison Of Terms.” BitSight, www.bitsighttech.com/blog/cyber-resilience.

over 55,000 High Level Government Computers.” Daily Mail Online, Associated Newspapers, 16 Jan. 2013, www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html.

Passeri, Paolo. “Cyber Attacks Timeline.” HACKMAGEDDON, www.hackmageddon.com/category/security/cyber-attacks-timeline/.

Pfeffer, Anshel, et al. “Israel Suffered Massive Cyber Attack during Gaza Offensive.” Haaretz.com, Haaretz Com, 11 Jan. 2018, www.haaretz.com/1.5065382.

Prigg, Mark. “Operation Red October Revealed: The Astonishing Hacker Attack That Has Infiltrated

Rosen, Armin. “Israel Faced A Huge Wave Of Cyber Attacks During Its War With Hamas - And Iran Could Be The Reason Why.” Business Insider, Business Insider, 18 Aug. 2014, www.businessinsider.com/israel-faced-a-wave-of-cyber-attacks-2014-8.

Swaine, Jon. “Georgia: Russia 'Conducting Cyber War'.” The Telegraph, Telegraph Media Group, 11 Aug. 2008, www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

Wikipedia contributors. "European Union." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 5 Feb. 2019. Web. 6 Feb. 2019.https://en.wikipedia.org/w/index.php?title=European_Union&oldid=881959337

Wikipedia contributors. "History of the European Union." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 24 Jan. 2019. Web. 6 Feb. 2019. https://en.wikipedia.org/w/index.php?title=History_of_the_European_Union&oldid=879958168

Zetter, Kim. “TJX Hacker Gets 20 Years in Prison.” Wired, Conde Nast, 4 June 2017, www.wired.com/2010/03/tjx-sentencing/.