
CESMUN

Forum:	Commission of Crime Prevention and Criminal Justice
Issue:	The Threat of Cybercrime to Global Security
Student Officer:	Andre Emile Sadik
Position:	Deputy President

Introduction

Cybercrime are crimes that are carried out by electronic means, it encompasses a wide range of criminal activities. Cybercrime can take form in either minor cybercrimes or it may also be in form of large major cybercrime attacks that usually have a significant impact. These attacks could vastly range, in some cases large cybercrime attacks could threaten and impact global security.

In the years of 1980s and 1990s we saw a huge spike in cybercrimes where at National CSS, AT&T, and Los Alamos National Laboratory. Which are all high-profile organizations. These years were the first to experience the ideas of the "Trojan Horse" and the "Virus", therefore marking the start of an era of cybercrimes.

From then on, new cybercrimes were developed at a very rapid pace. A rapid pace where even nation intervention could not keep up with the developments, leading to billions of dollars in losses due to these major cyberattacks. Approximately around one billion and six hundred and eighty US dollars were lost during the period between the year 2000 and 2010, and this is only in the USA.

The damages from these attacks are so large on a global scale, to the point that they cannot be measured as the damages would be incomprehensible. Statistics about this matter and the spikes of the increase in cybercrime attacks could not be measured as they were not systematically tracked at the time. Latest statistics of of cybercrime spikes begin from the year 2000 and 2001.

Definition of Key Terms

"Trojan Horse"

A trojan horse virus is a type of malware virus that downloads on a victims computer while being disguised as a legitimate software or program.

“worm”

A worm refers to a type of malware that spreads itself around the users computer files without the user knowing that there are damages.

[Relevant Key Term]

[Definition]

[Relevant Key Term]

[Definition]

[Relevant Key Term]

[Definition]

[Relevant Key Term]

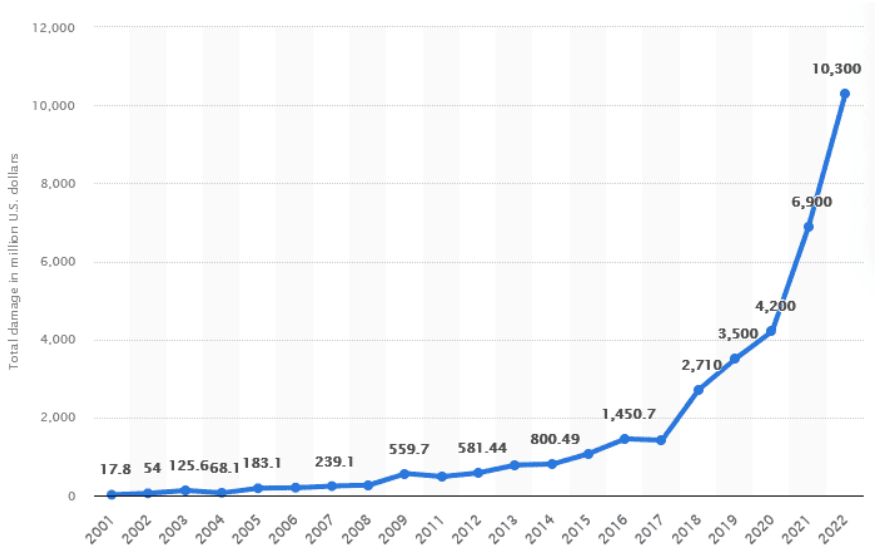
[Definition]

General Overview

The Rise of Cybercrime and its threats to Global Security

The topic of cybercrime is one of the most talked about types of crimes and it is also one of the largest and most common type of crime. Cybercrime saw a major increase during the years of 1990 which some may consider the start of cybercrime, as time went on, cybercrime had only developed and people found more elusive and deleterious

During the years of the 2000s to 2010, cybercrime had become so significant and common so much so that they had started tracking and creating statistics between the years. An estimated one billion six hundred eighty million dollars were lost in damages only in the USA between 2000 and 2010.It is important to note that computers and internet was widespread and used all over the world during that time, leaving more and more oppurtunites for cybercriminals. The years ofthe 2000s to 2010

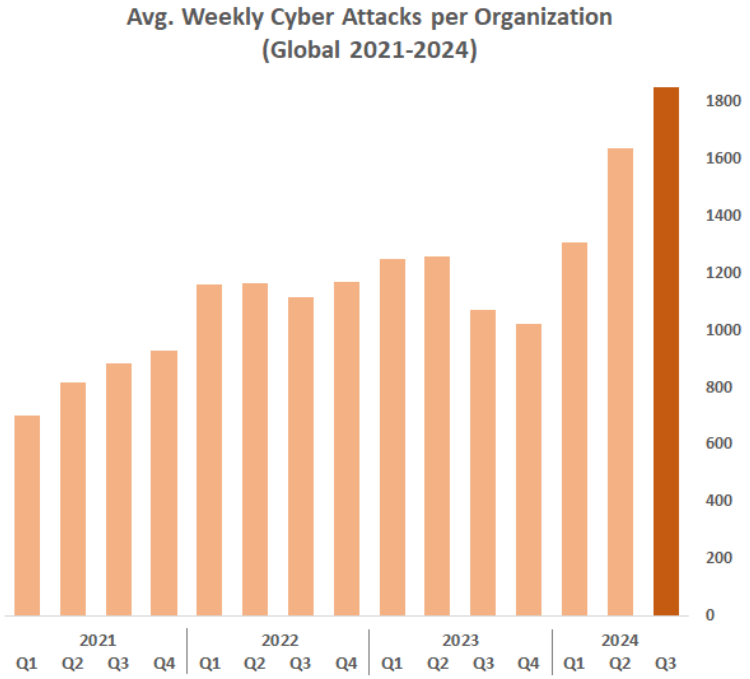


were considered by many as, ”The first Golden Era of Hacking”, Computer viruses increased significantly in 2000, including the well-known “ILOVEYOU” virus worm (May 2000), one of the most serious and destructive email-based infections at the time.

An estimated $10 billion in damages were inflicted worldwide by this virus alone. This worm was one of the first examples of a “Trojan Horse” virus, where people received emails with the subject title “I LOVE YOU”, and attached was a text file that was named “LOVELETTER”, when opened it seemed like a normal love letter. However, opening the file would activate the worm and it would spread through the computers files and gain access to personal information about the user. After one of the most prominent examples of a trojan horse, cybercrime only saw developments into more elusive ways. Where today, cybercrimes are a huge threat to global security. The seriousness of cybercrime threatens global security, this was demonstrated when a 15 year old teenager in America by the name of Jonathan Jones had managed to hack into the computers of the department of defence (DoD) and the NASA computers which are two of the most high-profile restricted and strictly confidential agency by the federal US government. This hack committed by a simple 15 year old teenager goes to prove and show that there are no limits as to what could happen to global security.

Given that there are no limits to what one can achieve and do to threaten global security, high profile organizations such as NASA and the DoD are considered to be two of the most restricted access organizations and hold some of the worlds most classified documents and information which would become a global threat if fallen into the wrong hands. Today, cybercrime is considered to be at an all time high, where 1 in 2 Americans experience cybercrimes a day and a 75% surge in cybercrimes attacks on large organizations globally per week over the last 3 years alone. Most people expected

methods of preventing and stopping cybercrimes to develop, which they have, however not enough to keep up with the new elusive cyber attacks, leading to roughly 18 times the losses between 2000 and 2010 in the years after to 2022. Therefore, this enormous spike in losses and damages has caused people to call these last 4 years, “The second Golden Era of Hacking”.



Major Parties Involved

The Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) is a component of the United States Department of Homeland Security (DHS) responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers.

UNODC and UN general assembly

The United Nations Office on Drugs and Crime is a United Nations office that was established in 1997 as the Office for Drug Control and Crime Prevention

Homeland Security

the U.S. federal executive department responsible for public security, roughly comparable to the interior or home ministries of other countries.

Department of state Justice (DOJ)

The United States Department of Justice (DOJ), also known as the Justice Department, is a federal executive department of the U.S. government that oversees the domestic enforcement of federal laws and the administration of justice.

[Major Party]

[Brief explanation]

Timeline of Key Events

Date	Description of event
[May | Day | 2000]	The "ILOVEYOU" virus was a large widespread early first example of a trojan horse type of virus which caused 10 billion dollars estimated globally in losses.
[May | 7th | 2021]	The colonial pipeline ransomware attack was a malware attack that infected the operations of a major oil pipeline in the USA, FBI was not involved in this case as it was such short notice, the company was forced to pay a ransom in bitcoin or the equivalent of 4.4 million USD. Most states in the USA were affaected by this, with 71% of gas stations running out of fuel.
[December|Day| 2015]	In December of 2015, Ukraine's power grid was shut down by a major cyberattack that left most of the country without electricity for a long period of time, this was the world's first successful cyberattack on a nation's infrastructure.
[September|14|2019]	On September 14 2019, Drones were sent to attack oil facilities in Saudi Arabias Abqaiq, during the drone attack a cyberattack occurred in Aramco Facilities with over 30,000 computers worth of data being wiped out, which largely impacted the economy, it was later revealed that this attack was the responsibility of a movement in Yemen called Houthi movement, However, because of the magnitude of this attack US intelligence agencies and Britian and France still suspect Iran of this major national attack.

[August-October|1999]	
	Considered the greatest cyberattack on the Federal Government in History, between August of 1999 and October of 1999, a 15 year old Florida-teen by the name of
[Month | Day | Year]	Jonathan James had managed to attack the NASA and the DoD which are two of the most highly restricted and high-profile federal organizations in the world. His attacks had impacts on a global scale as NASAs network had an outage of 3 weeks. James attack also left one of the most powerful nations in the world, vulnerable to attacks and important intelligence for a significant period of time.
[Month | Day | Year]	
	[Brief description]
[Month | Day | Year]	[Brief description]
[Month | Day | Year]	[Brief description]
	[Brief description]
	[Brief description]

UN involvement, Relevant Resolutions, Treaties and Events

- [Accurate reference to UN involvement, UN resolutions or significant events (Title + Link/Resolution reference)]
- [Accurate reference to UN involvement, UN resolutions or significant events (Title + Link/Resolution reference)]
- [Accurate reference to UN involvement, UN resolutions or significant events (Title + Link/Resolution reference)]

- [Accurate reference to UN involvement, UN resolutions or significant events (Title + Link/Resolution reference)]
- [Accurate reference to UN involvement, UN resolutions or significant events (Title + Link/Resolution reference)]

Previous Attempts to Solve the Issue

Many nations have attempted to address the problem of cybercrime in the past by enacting legislation that criminalizes internet offenses. The Computer Fraud and Abuse Act (CFAA), which was passed in 1986 and addressed offenses including identity theft, fraud, and hacking, was one of the first laws in the US. However, these regulations were unable to keep up with the speed at which technology was developing, which made it challenging for law enforcement to apprehend and prosecute criminals. Many times, the regulations were either out-of-date or too general to address the newly emerging types of cybercrime.

Additionally, nations began collaborating globally to combat cybercrime. The Budapest Convention on Cybercrime was established by the Council of Europe in 2001 as a multi-nation accord to make laws more comparable across national boundaries and enhancing governmental collaboration. This agreement facilitated international cooperation in the investigation and prosecution of cybercrimes such as illicit content, fraud, and hacking. But not all nations agreed to abide by the regulations, which limited the treaty's potential to address the worldwide issue of cybercrime.

In the battle against cybercrime, technology has also played a significant role. To defend against cybercriminals, security solutions including firewalls, antivirus software, and encryption have been developed. Employing techniques like data analysis and digital forensics, businesses have collaborated with law enforcement to find hackers and cybercriminals. However, because hackers are always coming up with new ways to get around security measures, the fight against cybercrime is never-ending and calls for regular modifications to technology and better training for both law enforcement and the public.

Possible Solutions

Solving cybercrime requires moving forward cybersecurity framework and progressing defense advances. One of the foremost significant steps is upgrading encryption strategies to secure touchy information, guaranteeing that indeed in case cybercriminals caught it, they cannot get to or utilize it. Governments and private companies must contribute in more grounded encryption strategies for both information at rest and information in travel. Moreover, standard overhauls and patches to software are fundamental to shut vulnerabilities that cybercriminals frequently misuse. Actualizing vigorous firewalls, multi-factor verification, and interruption discovery frameworks can moreover essentially decrease the chance of unauthorized get to to systems and gadgets, giving a strong defense against cyber dangers.

Another possible solution is the improvement and use of Artificial Intelligence AI to detect and respond to cybercrime instantly. Large volumes of data can be analyzed by AI systems to identify odd patterns that indicate a cyberattack. By continuously learning from contemporary threats, machine learning models can become increasingly adept at identifying emerging cybercrime tactics.This new technology makes it harder for criminals to take advantage of security flaws by helping to find issues more quickly and with greater accuracy. Therefore, limiting the chance of cybercrime occuring.
Both police forces and cybersecurity experts now have access to advanced tools that allow them to investigate and track cybercriminals more effectively. These tools help analyze digital records and reveal signs of illegal actions, such as traces of IP addresses, stolen login information, and encrypted messages. With this data, authorities can follow the digital footprints of criminals, even when they try to hide their true identities. As cybercrime becomes more advanced and harder to trace, this technology is increasingly important for detecting and stopping criminals who use more complex methods to cover their tracks.

As cybercrime continues to grow even larger and larger despite these efforts, cooperation between law enforcement and cybersecurity companies is more crucial than ever. By sharing expertise, tools, and information, these groups can work together to fight cybercrime more effectively. In addition, combining these technical advances with stronger legal protections will be essential in tackling

cybercrime on a global level. With the right tools and partnerships, we can create a safer online environment and stay one step ahead of cybercriminals.

Bibliography

MLA format bibliography – can be generated using easybib.com (Keep track of your sources!)

Appendices

Appendix I

CyberSecurityVentures- **https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/**

Appendix II

SecurityBrief- **https://securitybrief.co.nz/story/a-brief-history-of-cyber-threats-from-2000-to-2020**

Appendix III

Statista- **https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/**