An Analysis of Significant Cyber Incidents and the Impact on the Past, Present, and Future

Seth E. Smith

Old Dominion University

An Analysis of Significant Cyber Incidents and the Impact on the Past, Present, and Future

Seth E. Smith

Old Dominion University

COVA CCI Undergraduate Research

Fall 2021

December 1, 2021

Abstract

This report discusses data collected on significant cybersecurity incidents from the early 2000s to present. The first part of the report addresses previously discussed information, data, and literature (e.g. case studies), pertinent to cybersecurity incidents. The findings from this study are framed by scholarly sources and information from the Federal Bureau of Investigation, a number of notable universities, and literature online, of which all support information discussed within this report. The second part of the report discusses data compiled upon analyzing significant cyber incidents and events from the Center for Strategic and International Affairs (CSIS). Finally, the last portion of the report considers possible solutions to this ever-growing issue.

Introduction

From 2003 to present, over 793 significant cybersecurity incidents have taken place worldwide (Center for Strategic and International Affairs, 2021). The severity of this has left a catastrophic mark upon the globe, leaving countless countries and organizations unsure of how to proceed in an age where no information, data, or intelligence is truly safe from outside actors. A 2021 report by Cybersecurity firm SonicWall stated that, "between 2019 and 2020, ransomware attacks rose by 62 percent worldwide, and by 158 percent in North America alone" (Ramachandran, 2021). The alarming increase in cybersecurity crimes, whether hacking, election interference, ransomware, shows that a solution to this ever-growing issue must be found. This research report aims to not only analyze, interpret, and explain the data provided by the Center for Strategic and International Affairs (CSIS) and cybersecurity incidents and crimes of the past two-decades but also provide solutions, to ensure the well-being of the globes data and to prevent the crumbling of society as we know it. The following report includes an analysis of a data set compiled using CSIS reports, case studies, graphs, and other data sets of which guide the reader through the complexities encompassed within this essay and provide proper evidence proving that without immediate action our information will be unsafe indefinitely.

Literature Review

Dispersed throughout the "interwebs," there is an overwhelming amount of data and information detailing the negative impacts cybercrime has had on the globe. It is forecasted that in 2022 cybersecurity defense spending will reach approximately $133.7 billion (Gartner Research, 2018). While this is certainly alarming, it is vital to see how this current state has been reached. While there is not too much knowledge on when cybersecurity became a main concern of the public (specifically in the United States), in the "1990s and early 2000s, public awareness of the potential for data breaches began to rise" (Groot, 2020). As Digital Guardian states, "most information on data breaches focuses on the time period from 2005 to present-largely due to the advancement of technology, making data breaches a top concern for both enterprises and consumers" (Groot, 2020). This is crucial to note, mainly because a lot of the data that the public has access to (e.g. data from the CSIS, of which was utilized upon writing this report) begins around the 2003-2006 time frame to present. One example of this is a report conducted by Valeriano and Maness in *Journal of Peace Research*, in which data was collected on cyber interactions and conflicts from 2001-2011. Data collected in their report found approximately 110 cyber incidents and 45 cyber disputes. Similar to the data described in this report China and The United States have the highest number of incidents (Valeriano and Maness, 2014).

In addition, U.S. News and World Report notes that the main perpetrators over the past decade have been Russia and China, and that there are certain "hot spots" around the globe both attracting cyber activity and acting out cyber-attacks. "This is only growing to the point that more and more nations are budgeting offensive cybersecurity operations" (Baumgartner, 2021). The United States as well as several European countries have and continue to combat from outside cyber aggression/cyber-attacks (specifically from Russia and China). More

recently, a 2017 attack by Russia on Ukraine, caused a catastrophic impact on the international shipping company Maersk, causing roughly $10 billion in economic damages. While the attack was initially intended to cripple Ukraine and "support Russia government efforts," the attack had a global impact. In October of 2020, a federal grand jury indicted six Russian computer hackers, who were responsible for the attack. Assistant Attorney General for National Security, John C. Demers, commented that in the history of cyber-crimes and attacks there has never been one as malicious, irresponsible, and persistent as Russia, "wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite" (Demers, 2020).
In addition, the attack was one of if not the most destructive computer attacks solely attributed to a single actor, by unleashing the NotPetya malware. Demers notes that no country or society will "recapture greatness while behaving in this way" (Demers, 2020). Instances like this is a primary reason there is an international concern for cybersecurity and the safety of one's information.

In K. Lieberthal and P. Singer's essay, *Cybersecurity and U.S. China Relations,* the authors note that there is "no relationship as significant to the future world politics as that between the United States and China" (Singer and Lieberthal, 2021). The authors state that while "cyberspace" and cybersecurity as a whole did not exist a few decades ago, there are now an estimated 55,000 new pieces of malware found daily and over 200,000 computers worldwide compromised daily (Singer and Lieberthal, 2021). While this is not all fault of China, in recent years the number Chinese attacks on U.S. and U.S. allies, in a public and private capacity have become extremely prevalent. In the summer of 2020, NPR reported that the White House publicly blames China for a major attack on tech "powerhouse" Microsoft. The cyberattack on Microsoft reportedly inserted computers with malware with the main goal to surveil systems owned by other businesses, local and state governments, military contractors, etc. Even more recently the United States largest gas pipeline-Colonial Pipeline, fell victim to a cybersecurity ransomware attack, crippling half of the East Coast's fuel supply. The perpetrator of the attack has not been identified however, it is believed to be at the hands of a Russian or Eastern European actor.

The research and data discussed throughout contributes to cybersecurity literature and research community for several reasons. Despite the general consensus among acadamia that there has been an uptake of cybercrimes worldwide, there is a lack of research focusing on the most significant cybersecurity incidents and their components. The data within this essay successfully does this. In addition, due to the specificity of the data in this report, more educated conclusions can be drawn to prevent further cybersecurity incidents. These various weaknesses within current research and data, strengthens and instills a uniqueness of the data included within this report. Finally, various other sources are noted throughout to support many of the claims and statements made, helping the reader to further understand the importance of cybersecurity research.

Several other researchers, universities, are beginning to realize the importance of cybersecurity and the uptake in incidents the past few decades. Much of the information gathered by scholars alike, greatly compliments data found when writing this report. Virginia Tech and Duke University are two such universities making a great impact on the space as it pertains to cybersecuirty research and crimes. In September of 2021, Virginia Tech announced the formation of the Virginia Tech National Security Institute, with its main objective to conduct academic research in many fronts including technology, policy, and national security. Dan Sui, Vice President for Research and Innovation at Virginia Tech notes that the universities current strengths in security research and investigation, easily supports the expansion for further research not only in the Commonwealth of Virginia but the globe. Much of the research conducted completely aligns with data found within this report. Duke University is another academic community, heavily invested in cybersecurity crimes and research. Anna Gotskind, a researcher for Duke University mentions the increase in cyber hacking since the Digital Revolution began in the 1970's (Pariona, 2017), with immense growth in the early 2000's. This compliments data within this report exactly-a minimal number of crimes beginning in early 2000s (2003-2007), with a rapid increase thereafter. Gotskind also discusses The Solarwinds Attack and the Future of Cybersecurity. Her realization-that it is evident that the number of cybersecurity crimes will continue to rise and that transparency as well as using "best practices" is the primary way to prevent cyber-crimes and attacks. NATO is also one such organization that has seen the rise in cyber incidents and is committed to cyber defense and "best practices." NATO is developed to "training, policy, and doctrine" better recognizing the importance of protecting the globes data and "protecting digital systems from cyber risk" (Ducaru, 2016).

(Moore, 2020), notes many trends in regards to cybersecurity threats. Phishing attacks is one such cyber-attack which has become more "sophisticated" and the number of crimes increased in the past decade. Moore, understands the level of skill that many hackers hold, "for example using machine learning to much more quickly craft and distribute fake messages in the hopes that recipients will unwittingly compromise their organization's networks and systems" (Moore, 2020). Ransomware attacks is another prevalent method hackers enlist to steal data and information from individuals, organizations, etc. Moore also mentions the rise of cryptocurrencies like Bitcoin or Ethereum and credits it with helping to fuel ransomware attacks by allowing ransom demands to be paid anonymously with little to no way of tracking. Moore's findings overlap with the findings in this report.

Finally, data showing that the United States is a main victim of cyber-attacks is prevalent throughout several studies, research papers, not excluding this one. Whether outside actors targeting large corporations, elections, or personal information, due to the United States power and global voice, it is at risk of constant cyber-attacks. Pew Research Center notes that 75% of Americans say "it's likely that Russia or other governments will try to influence elections (specifically the 2020 election)" (Pew Research, 2020).

Pew Research Center also conducted a survey in 2020 finding that American's confidence has significantly decreased in the federal government's efforts to protect U.S. elections from outsider threats.

Analysis and Data

When collecting and analyzing data, the cyber incidents as reported by the CSIS were cataloged in the following fashion. Hacking (1), the unauthorized attempt to access or exploit a computer or network with the intention to steal data for an illicit purpose. The second category of incident or crime is unauthorized access (2); when an individual or outside party gains access without permission of a computer, application, network, data or any other resource(s). Malware (3) is “malicious software” (IBM, 2021), that upon injection into a computer or program, will render it inoperable. Typically, this form of cybersecurity hacking will wipe a computer. Thefts of Secrets/Intellectual Property (4), “theft involves robbing people or companies of their ideas, inventions, and creative expressions-known as intellectual property-which can include everything from trade secrets and proprietary products and parts to movies, music, software” (Federal Bureau of Investigation, 2016). The next category is Surveillance/Espionage (5); a form of cyber-attack with the main objective to steal any data (typically classified) to be utilized to gain an advantage in a company or government setting. A Phishing attack or “phishing scam (6) is used to steal data, credentials, etc. A common style of attack is sent via email, typically a link when upon opened, perpetrators are able to gain access to personal information. Another category of incident when analyzing data was Online Disinformation (7). Online Disinformation is the spread of inaccurate data or content with the intention to cause harm to a party. There are countless reasons an actor may utilize online disinformation as a tactic to cause harm, common reasons include political, emotional, etc. Online Propaganda (8) is another tool used by hackers, often for political purposes, similar to Online Disinformation. Online Propaganda often spreads false or misleading information about a party or individual. Another tool used by hackers is Website Defacement (9); an attack on a website, typically replacing content on the site with a message of their own. Messages vary but will include crude content, a religious message, or other. The final type of crime/incident categorized within the data-Election Interference. This is classified as any effort to subvert elections through social media, voting machines, etc. Russia is infamous for meddling within elections of outside countries for personal interests including but not limited to The United States, Europe, and Africa.

It is important to also note that there are two main types of threats, an outsider threat (included but not limited to, organized criminals, professional hackers and amateur hackers) and internal threats (include but not limited to, employees' carelessness of security policies and procedures, disgruntled current or former employees, business partners, clients, contractors).

Description of Experiment

Analyzed and computed over 700+ significant cybersecurity crimes that have occurred from 2006-present. Once data was compiled into Microsoft Excel (by month, year, type of crime, country, perpetrator, victim(s), description of incident), I was then able to see common trends and patterns amongst the data. The various graphs below describe much of the data gathered, helping to make an educated guess on why these cybersecurity crimes have continued to increase, why some countries are common victims, why some countries are common perpetrators, etc.

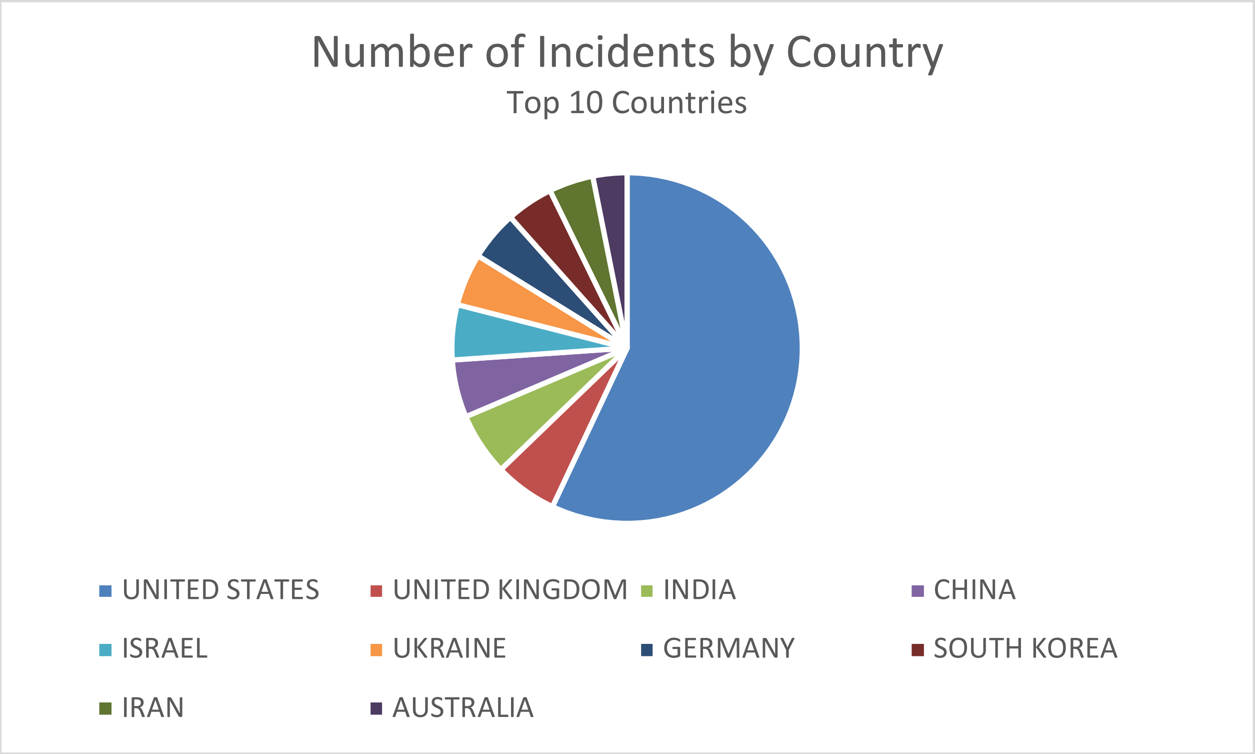
Number of Incidents

The Center for Strategic and International Studies accounts for over 793 significant cybersecurity crimes since the early 2000s. With over fifty countries subject to cybersecurity crimes, the graph below displays the number of significant incidents various countries have faced beginning in 2006 to present. Per the data, the

United States has experienced a vastly greater number of crimes, since the early 2000s. BBC reports that one reason the United States has been a "long-time" victim of cybercrimes is due to the global impact and power the United States holds. Due to this, The United States in recent years has not only enlisted the help of the Department of Defense but also the Federal Bureau of Investigation, Department of Homeland Security, allies, and academia (Deppa, 2017). With the world's largest military, the third largest population, and immense economic influence, countries alike will constantly have to combat with cyber-crimes. The data below shows the number of cyber incidents by country from 2006-present. In order, the countries with the greatest number of incidents is as follows- the United States (236), the United Kingdom (24), India (24), China (22), Israel (21), Ukraine (20), Germany (19), South Korea (18), Iran (17) , and Australia (13). While cybercrimes and threats can occur for a number of reasons, most of the countries in the "top 10 incidents (see graph 1)" have extremely large populations, economies, and global influence which results in these countries being greater targets. In terms of population China has the largest ($1.4 billion), India ($1.38 billion), and the United States with the third largest ($329.5 million). In terms of nation(s) economy, United States ($19.485 trillion), China ($12.238 trillion), Germany ($3.693 trillion), India ($2.651 trillion), and United Kingdom ($2.638 trillion), have the largest economies to date. Having both a great population and a flourishing and (changed this word) high economy is a driving factor why these countries are constantly under attack.

Note: Refer to Graph 1

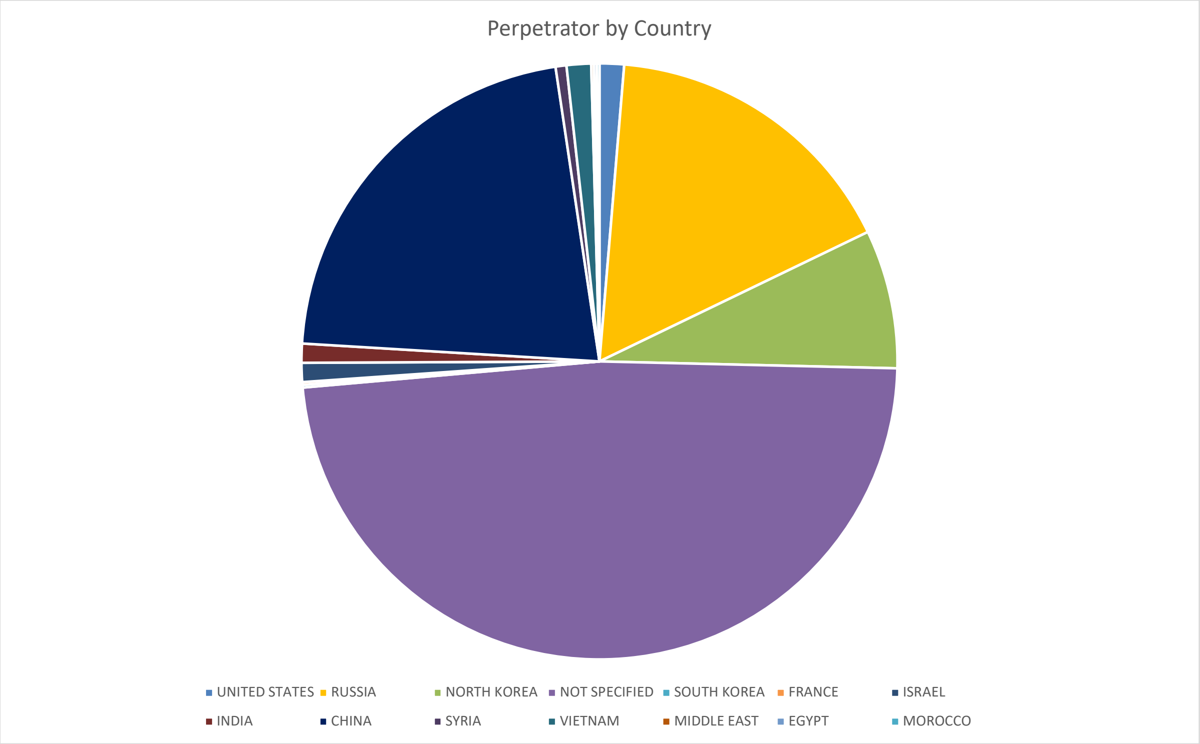
Graph 1: Number of Incidents by Country (Top 10 Countries)



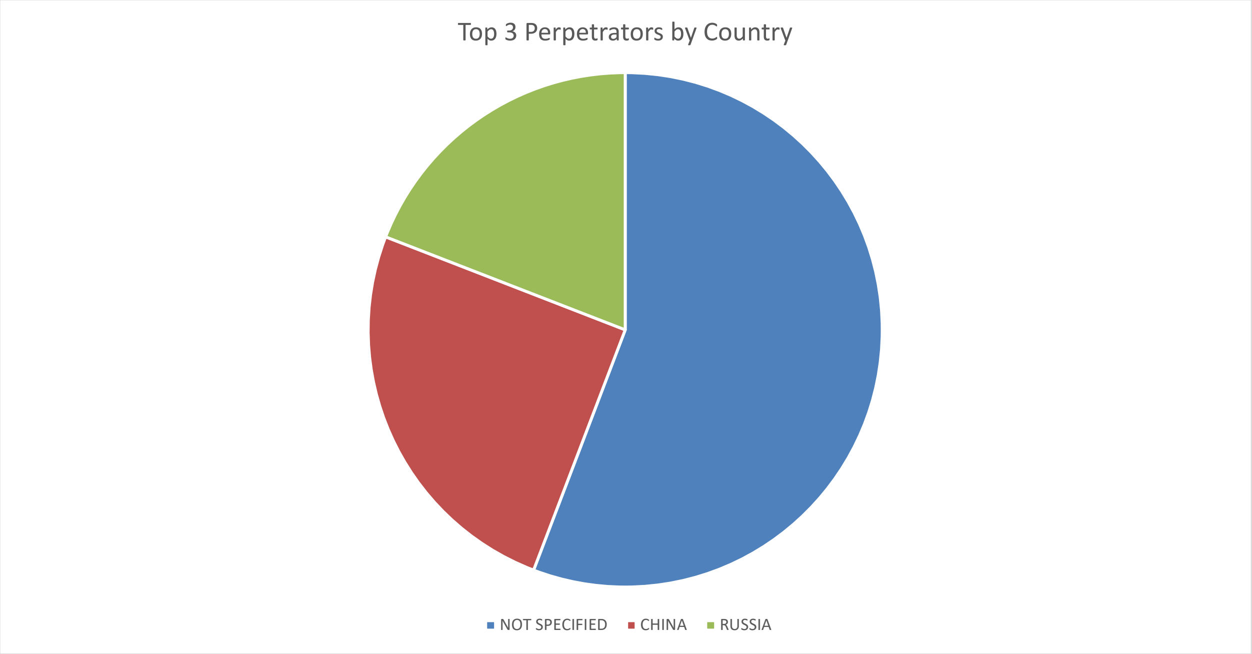
Perpetrator by Country

Since 2006, there have been countless countries, of which have either been identified or outspoken about their involvement in cyber crimes and attacks. The graph below displays the main perpetrators of significant cyber events. The largest is that of "not specified." There are some cybersecurity crimes/events that have occurred where the perpetrator is still unknown. An example of a cybersecurity crime where the perpetrator was "not specified" was a 2014 incident where ten percent of Dairy Queen outlets were hacked and customer credit card data compromised. "Like the Target hack, hackers reportedly exploited a third-party system to obtain access" (Center For Strategic and International Studies, 2021). Russia, China, and North Korea are also some of the main perpetrators.

Graph 2: All Perpetrators by Country



Graph 3: Perpetrators by Country (Top 3)

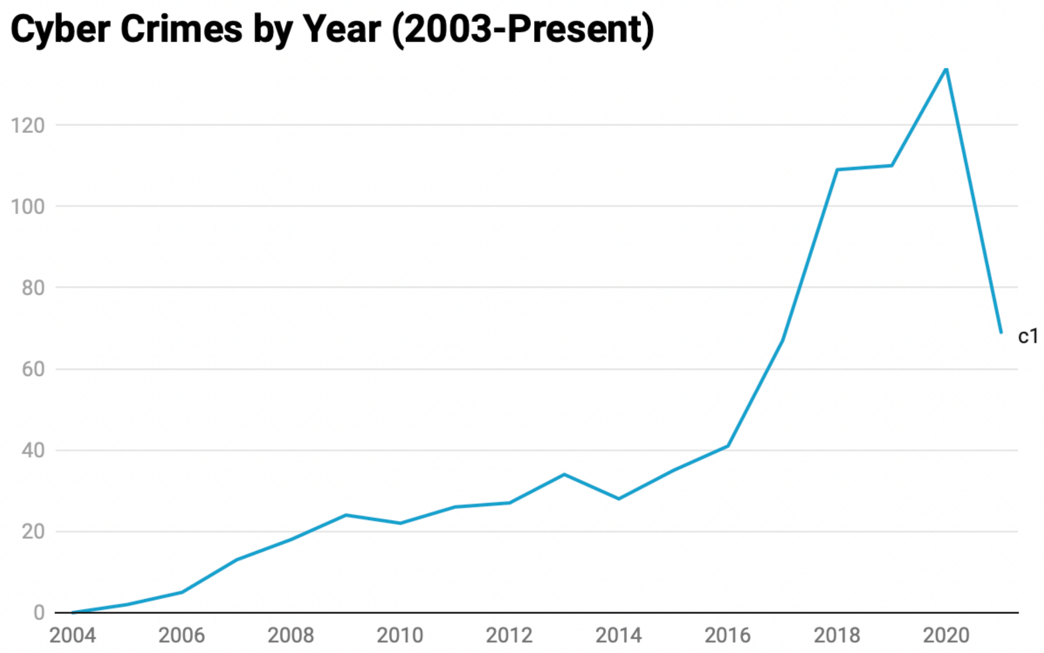


Russia and China are two of the largest perpetrators and cyber-threats of the past two decades. An overwhelming amount of the attacks from both China and Russia centered around election interference, surveillance/espionage, and hacking. At the White Houses' 2021 Annual Cyber Symposium, Adam Segal remarks of the overwhelming percentage of the entries within the White Houses' cybercrime database, where China, Russia, Iran, and North Korea make up roughly 77 percent of the crimes against the United States (Segal, 2021). The data found upon conducting this report aligns with this assessment by Segal as well—Russia, China, "not specified," and North Korea are the main perpetrators in cyber-crimes and incidents, not only attacking the United States but globally as well. Siers remarks on the reason behind many countries desire to act out a cyber-attack, in specific North Korea. Over time, North Korea has developed a group of "cyber-warriors," with the main objective to attack primary adversaries such as South Korea, The United States, and Japan. In closing, Siers notes that "cyber-crime is the ideal weapon for a cash strapped nation" (Siers, 2014).

Crimes by Year

The following graph depicts the rise in cyber-crimes globally from 2003/2006-present. This exponential growth is due to various reasons including economic, social, technological, and political. While the number of cyber incidents has continued to increase since 2003 the growth is in part due to the advancements in technology. As computer systems and technology have evolved it has made it increasingly easier for hackers with nefarious intentions to steal data. Per graph 4, there is a gradual increase in cyber incidents and a drastic increase in the number of crimes in the 2015–2016-time frame. The United States saw a large number of attacks, specifically from Russia, with their involvement in the 2016 U.S. elections. Lastly, it is vital to note that while it appears there is a decrease in crimes after 2020 (beginning in 2021), this is certainly not the case. The significant cyber incidents noted by the CSIS stop towards the beginning of 2021, not depicting current data. Due to the COVID-19 pandemic, there has been a massive surge in malware and ransomware attacks (Patterson, 2021). Cyber incidents have flourished due to the vast number of people working from home-privately used computers lacking professional anti-virus software and other protective options (Wiggen, 2020).

Graph 4: Cyber Incidents/Crimes by Year (2003-Present)



Conclusion

In June of 2001 Thomas T. Kubic, Deputy Assistant Director, FBI, spoke before the House Committee on the Judiciary, Subcommittee on Crime, Washington D.C., commenting on the nature of cyber-crimes/incidents and the drastic and immediate need for expertise, research, and investigation into the matter. Kubic notes that while it is often unclear of the overall purpose of an attack, investigations have led to the understanding that one such reason behind "computer intrusion" is to facilitate ongoing criminal activity and seek financial gain" (Kupic, 2001). Also, one should expect the number of significant cyber incidents to continue to increase due to the "advance of the digitalization" (Wiggen, 2020), thus a way to more skillfully combat cyber incidents and crimes must be found. One primary way to do so is investigating and research, as well as awareness. By analyzing trends and data, one can better prepare for attacks. A primary example of this is in the past decade, many large corporations (e.g. Microsoft) now require employees to partake in annual cybersecurity training to not only make employees aware of potential attacks (e.g. phishing) but to also prepare them for the "new digital age." While the advancement in data and technology the past two decades is remarkable, the number of cybersecurity incidents as a result of the technological advances is alarming. If there is no immediate change to the current situation, what will be the result of the worlds data and information?

References

BBC. (n.d.). *The role of the US as a world power - the USA's international influence - higher modern studies revision - BBC bitesize*. BBC News. Retrieved November 19, 2021, from https://www.bbc.co.uk/bitesize/guides/z6frqp3/revision/2.

Business News today: Read latest business news, India Business News Live, Share Market & Economy News. The Economic Times. (n.d.). Retrieved November 19, 2021, from https://economictimes.indiatimes.com/?back=1.

China, russia biggest cyber offenders - US news & world report. (n.d.). Retrieved November 19, 2021, from https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows.

Council on Foreign Relations. (n.d.). *The cybersecurity threat from Russia*. Council on Foreign Relations. Retrieved November 19, 2021, from https://www.cfr.org/event/cybersecurity-threat-russia.

Cybersecurity and u.s.-china relations - brookings. (n.d.). Retrieved November 19, 2021, from https://www.brookings.edu/wpcontent/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

Deppa, C. S. (2017). U.S. Cyber Command: An Overview. *American Intelligence Journal*, *34*(1), 12–15. https://www.jstor.org/stable/26497111

Ducaru, S. (2016). Is Cyber Defense Possible? *Journal of International Affairs*, *70*(1), 182–189. https://www.jstor.org/stable/90012603

Editor, C. S. R. C. C. (n.d.). *Unauthorized access - glossary*. CSRC. Retrieved November 19, 2021, from https://csrc.nist.gov/glossary/term/unauthorized_access.

Election security spotlight - disinformation and misinformation. CIS. (2021, June 15). Retrieved November 19, 2021, from https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disinformation-and-misinformation/.

FBI. (2016, May 3). *Intellectual property theft/piracy*. FBI. Retrieved November 19, 2021, from https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft.

GDP by country. Worldometer. (n.d.). Retrieved November 19, 2021, from https://www.worldometers.info/gdp/gdp-by-country/.

Gotskind, A. (2021, April 14). *The Solarwinds attack and the future of Cybersecurity*. Research Blog. Retrieved November 19, 2021, from https://researchblog.duke.edu/2021/03/02/the-solarwinds-attack-and-the-future-of-cybersecurity/.

Hartig, H. (2020, August 27). *75% of Americans say it's likely that Russia or other governments will try to influence 2020 election*. Pew Research Center. Retrieved November 19, 2021, from https://www.pewresearch.org/fact-tank/2020/08/18/75-of-americans-say-its-likely-that-russia-or-other-governments-will-try-to-influence-2020-election/.

Jeffery, L., & Ramachandran, V. (2021, July 8). *Why ransomware attacks are on the rise - and what can be done to stop them*. PBS. Retrieved November 19, 2021, from https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.

Moore, Michelle. (2021, November 16). *Top cybersecurity threats in 2020*. University of San Diego. Retrieved November 19, 2021, from https://onlinedegrees.sandiego.edu/top-cyber-security-threats/.

Siers, R. (2014). NORTH KOREA: THE CYBER WILD CARD. *Journal of Law & Cyber Warfare*, *4*(1), 1–12. http://www.jstor.org/stable/26441246

(2020, October 19). Retrieved November 19, 2021, from https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360. http://www.jstor.org/stable/24557484

Virginia Tech Launches National Security Institute; Eric Paterson appointed executive director. VTx. (2021, September 28). Retrieved November 19, 2021, from https://vtx.vt.edu/articles/2021/09/research-virginia-tech-national-security-institute-launched.html.

What is a cyber attack? IBM. (n.d.). Retrieved November 19, 2021, from https://www.ibm.com/topics/cyber-attack.

What is a website Defacement attack: Examples & prevention: Imperva. Learning Center. (2020, September 17). Retrieved November 19, 2021, from https://www.imperva.com/learn/application-security/website-defacement-attack/.

Wiggen, J. (2020). *The impact of COVID-19 on cyber crime and state-sponsored cyber activities*. Konrad Adenauer Stiftung. http://www.jstor.org/stable/resrep25300

WP Post Author Franklin Holcomb , Franklin Holcomb , & posts, S. author's. (2021, May 10). *Countering Russian and Chinese Cyber-Aggression*. CEPA. Retrieved November 19, 2021, from https://cepa.org/countering-russia-and-chinese-cyber-aggression/.