The Linkage Between the Climate Change and the Cybercrimes

Min Kim
William & Mary

The Linkage Between the Climate Change and the Cybercrimes

Min Kim, William and Mary

COVA CCI Undergraduate Research Project Spring 2023

Research Mentor: Professor Shobha Vatsa, ODU

Contents

Abstract

At the beginning of the new era, the rise of the Fourth Industrial Revolution has been rapidly transforming society into a new form that has never been experienced before. While previous industrial revolutions have also contributed to societal growth through phenomenal inventions and discoveries, the Fourth Industrial Revolution has the potential to break the most conventional rule, and one that has dominated social and economic activities: physical interaction. In the near future, sitting at the office, having an in-person meeting, or going on a business trip may no longer be needed as physical barriers are destroyed by cyberspace. However, two significant issues have also risen, and the threat they pose is growing day by day.

Climate change, the by-product of the First Industrial Revolution, has been growing through the Second and the Third Industrial Revolution and has begun to express its tremendous influence. Simultaneously, cybercrimes, a newly emerging issue, have quickly grown in size through the ever-increasing cyberspace that exists today, posing enormous financial and ethical problems to society. As climate change and cybercrimes are issues thought to be mutually exclusive of one another, attempts to attack them individually have been made. However, despite the perceived differences between these two issues, they may not be entirely unrelated. This paper argues that there may be a potential connection between climate change and cybercrimes and suggests practical solutions that can be implemented to address both issues together effectively.

Introduction

Since human civilization was formed, there have been four distinct industrial revolutions. The first industrial revolution, which is known as a significant transition from manpower to steam power, enabled humans to perform tasks that were previously considered impossible. For example, the rickshaw, which could merely carry three people, was replaced by the steam locomotive, providing transportation services to hundreds of people. Also, spinning jenny powered by steam was as productive as several hundred people doing the same work. The second industrial revolution, the period when the steam engine was replaced by electricity, encouraged the division of labor and enabled mass production. The introduction of the conveyor belt allowed companies to specialize their workers in a specific task. The third industrial revolution introduced various computing machines that automated redundant processes. Currently, we are in the middle of the fourth industrial revolution, which is blurring the boundaries between physical, biological, and digital worlds through the introduction of artificial intelligence, IoT, robotics, blockchain, and other prospective technologies.

Technological advancements throughout the industrial revolutions have played a crucial role in enhancing the quality of life for people and have been significant in improving the social, political, and economic status of developed countries, laying the foundation and increasing the potential for the next industrial revolution. However, this progress has also resulted in two critical problems that now threaten the contemporary world: Climate Change and Cybercrimes. Climate change, which was the by-product of the first industrial revolution, has grown significantly through the second and the third industrial revolution and is now beginning to express its tremendous influence on the world. Simultaneously, cybercrimes, a newly emerging issue, have quickly grown

in size through the ever-increasing cyberspace that exists today, posing enormous financial and ethical problems to society.

Climate Change is a phenomenon that refers to the statistically significant increase in global temperatures that have been occurring since the first industrial revolution. Scientists attribute this global warming trend, which was observed since the mid-20th century, to the human expansion of the "greenhouse effect" — warming those results when the atmosphere traps heat radiating from Earth toward space [9]. Since the preindustrial period, global temperatures have increased by 1.1 degree Celsius. The surge of carbon dioxide in the air has resulted in the melting of the ice sheets in the Arctic Sea, causing a negative cycle to form: less ice leads to further increases in air and ocean temperature, which melts more ice. While the cause is simple, the effects of climate change have the potential to destroy the entire social and economic system that humankind has built. Sea level rises, which will cause land with low altitude to sink. Big port cities around the world would be the first target of rising sea level, which will impact the global trade system. Hurricanes become stronger and more intense, causing severe damage to civilizations. More droughts and wildfire would cause arable lands to become deserted and useless. Finally, changes in precipitation patterns would completely destroy the pre-existing agriculture patterns and practices [9]. While there have been multiple attempts to at least mitigate the effects of climate change, due to the conflicts between the developed and developing countries, the selfishness and cost-saving methods of firms, and pervasive insensitivity, they have not been as effective as they would have been in the perfect setting.

Cybercrimes encompass all criminal activities performed in cyberspace. Cyber criminals seek to exploit human or security vulnerabilities in order to steal passwords, data, or money directly. The most common cyber threats include hacking - including of social media and email

passwords, phishing - bogus emails asking for security information and personal details, malicious software – including ransomware through which criminals hijack files and hold them to ransom, and distributed denial of service (DDOS) attacks against websites – often accompanied by extortion. Like climate change, cybercrime is a global threat since cyberspace is not restricted by borderlines. Criminals and the technical infrastructure they use are often based overseas, making international collaboration essential [10]. While cybercriminals can target anyone, wealthy individuals or firms should be especially cautious since a single incident could lead to significant economic and reputational damage. Additionally, there is also one more special group that needs to be extra careful of cybercrimes: biological and chemical companies. Almost any industrial facility that stores or handles substantial amounts of chemicals, including extremely hazardous substances, and uses computer controls or monitoring could be vulnerable to a cyber-attack [2]. Such attacks could cause hazardous substances to leak, leading to damage not only to the company but also to the environment and people's lives. Thus, it is a socially optimal choice to implement specific measures to prevent cyber-attacks against these companies.

Literature Review

Although it is commonly believed that there is no connection between cybercrimes climate change except the fact that they are positively correlated with each other without any causal relationships and the evidence suggests that they do have some linkages between them. While there have been numerous attempts to solve each issue individually, trying to address both issues together has not been fully considered. Efforts to link them together to find how they interact and pose threats to society could be advantageous for coming up with better solutions. This paper discusses three main linkages between the two issues, some of which produce expected outcomes while others are more surprising.

The first linkage between climate change and cybercrime is that they complement each other to exacerbate the damage to infrastructures. Due to their interconnectedness, both climate change and cyber threats are security risks that can affect the safety and security of fundamental resources such as water, energy, and infrastructure [3]. The increased use of technology to manage energy usage and promote sustainability means that more devices are vulnerable to cyber-attacks. As more criminals target supply chains, infrastructure investment and other related industries, workers, customers, and business owners are all affected and suffer the consequences. Critical infrastructure in the energy sector is particularly more vulnerable to the effects of climate change because it has such a heavy reliance on online networks [1]. Several recent examples of cyber-attacks against the energy infrastructures support the point. On May 7, 2021, the US Colonial Pipeline experienced a ransomware cyberattack that forced the company to shut down its fuel distribution network. It is widely believed that the company reportedly agreed to pay a US$4.4 million ransom to DarkSide, a Russia-based criminal group [5]. A very well-known example came

in 2020 when SolarWinds, which provides system management tools for network and infrastructure monitoring, was targeted. Orion, its IT monitoring system, has access to hundreds of thousands of organizations around the world. Over 30,000 public and private organizations use the Orion network management system, making the company an attractive target for hackers and representing a massive scale threat to global security [5]. As climate change worsens, more infrastructures in the energy sector would be required, making the sector even more vulnerable to cyber-attacks. In this context, the consequence of cyber-attacks would be catastrophic, threatening global security and potentially causing economic chaos.

The linkage between climate change and cybercrime extends beyond just infrastructure vulnerability. The second linkage that is significant enough to point out is that climate change contributes to general insecurity and violence in society, which could be manifested as a form of cybercrimes. Increase in the threat to the climate has increased the rates of activism, such as protests and campaigns, and of course online activism as people push for policy reforms. 'Hacktivism' – hacking undertaken for a political or social cause – has become a way to garner more media attention, and as activists become more vocal about their climate fears, it is likely that there would be a significant increase in this type of activity [1]. Globally, climate disasters such as floods and wildfires are becoming more common and highlighting the severity of climate change and the impact that it has on individuals, communities, and businesses. For corporations, climate change strategies should be at the forefront of their business models as physical damage to infrastructure can create opportunities for cyber criminals to hack company data [8]. In this context, the need for robust cybersecurity measures should be implemented as corporations may find themselves vulnerable to digital threats arising from climate change.

The third linkage that exists between climate Change and cybercrimes is that they exacerbate environmental damage. A prime example of this was seen in 2015 when a group of cyber hackers gained access to a German steel company's network through phishing methods. The attack intentionally ruined the system of the company, effectively compromising production control and the blast furnace. As a result, the furnaces could not be shut down and severely damaged the properties and the environment [7]. Similarly, in 2011, Russian hackers compromised computer infrastructure that controls drinking water supply in two U.S. cities. They took control of the pump linked to distributing drinking water and forcibly broke it by repeatedly turning the valves on and off, cutting off the access of thousands of homes to clean and safe drinking water. This incident endangered the lives of many citizens and established cybercrime as a tangible threat to human health and national security. It also led to loss in astronomical amounts of water supply, causing huge damage to the environment [7]. One more infamous incident happened in 2014, where cyber terrorists attacked four NOAA (National Oceanic and Atmospheric Administration) websites. Since the main objective of NOAA is to provide daily weather forecasts, severe storm warning, climate monitoring to fisheries management, coastal restoration, and the supporting of marine commerce, its dysfunction would completely cut off the connection between humans and climate, making it harder for people to carry out tasks that are climate related. Although NOAA successfully triaged the attacks with no significant impact to operations or data, this event brought into focus the cybersecurity challenges that federal agencies face with respect to protecting information technology systems and assets from external and internal threats [7]. Moreover, millions of people worldwide rely on Cloud storage to access information and services, with facilities filled with high-powered CPUs, terabytes of RAM and petabytes of storage. It is therefore no surprise that Cloud storage centers account for 1% of the world's electricity use [6]. As such,

cybercrime against Cloud storage centers has a high potential in indirectly impacting the environment.

Proposed methods and Findings

Adding Climate Change to the Business Security Plan

As mentioned above, this paper explained three main linkages existing between cybercrimes and climate change, which makes it important to solve them collectively when the goal is to mitigate or eliminate the problems caused by these two issues. Businesses and governments need to recognize the interconnectedness of these challenges and to take proactive measures to address them. One of the ways that businesses can improve their readiness for the damage caused by these issues is to ensure that decision makers and IT professionals are working together to incorporate climate change risks into their security plans. For example, if there is a power outage caused by extreme weather conditions, it impacts business operations but also could compromise security — having a plan in place for these events will reduce the burden of these events on the business [1].

Making Smart Investment Decision

Another way for businesses to address climate change and cybercrimes is by making smarter and more sustainable investment decisions, such as channeling capital to the renewable energy sector, and moving away from investments in traditional resources like oil. This provides an opportunity for long-term financial gain as the energy sector is rapidly growing. While the main objective is to support the development of renewable energy and reduce the usage of traditional energy that aggravates climate change, it also reduces the threat from environmental protestors and enhances the company's reputation, making cyber criminals harder to attack [8].

Implementing a More Efficient Energy Management System

Finally, Organizations can use ISO 50001 to gain a better understanding of the way they use energy and to achieve more effective leadership focus on energy policies. The standard helps organizations to reduce their energy usage, save money by managing energy more efficiently, reduce their carbon footprint, increase energy security, and demonstrate a commitment to improved energy performance [6]. This not only helps businesses to address climate change but also to improve their bottom line by reducing their energy costs. Many businesses often find it harder to prepare enough capital to implement better cybersecurity measures and programs. By using better energy guidelines, businesses would be able to gain enough budget to increase their defensive power and resilience against potential cyber-attacks.

Conclusion and Future Scope

The emergence of modern technologies has brought immense benefits to our daily lives. However, just like how there is no such thing as a free lunch, we cannot ignore the fact that we must pay a price for these advancements. Climate change, one that was evident enough for us to realize and prepare earlier yet we did not, threatens people and the ecosystem. Cybercrimes, one that has grown quickly, pose financial and ethical challenges to individuals and firms. Unfortunately, while each issue presents its own set of challenges, the interplay between them has become a stronger burden. As it was discussed above, the linkages between these two issues - infrastructure damage caused by the synthesis of both issues, increase in cybercrimes caused by the climate change and its effect on people, and climate change and cybercrimes negatively affecting the environment – clearly shows that there should be solutions to handle both issues collectively.

Therefore, it is crucial for decision makers and IT professionals to cooperate to incorporate climate change risks when they prepare their own security plans. Considering the causal chains and intersection of two issues would be helpful for them to produce a more robust and resilient plan. On top of that, smarter and more sustainable investment decisions can help reduce the threat from environmental protestors and increase long-term financial gain. Since climate change has enough power to destroy the previous plans the government or the businesses implement only considering cybercrimes, or vice versa, we need to acknowledge the linkages between them and make smarter and more efficient choices. By addressing these issues together, we can better prepare for the challenges ahead and reduce their impact on our society and the environment.

References

[1] *How climate change is impacting cybersecurity: The Renewable Energy Hub*. Button, A. 2022, November 14. The Renewable Energy Hub | Essential articles and recent news events related to the Renewable Energy Industry. Retrieved March 16, 2023, from https://renewableenergyhub.co.uk/blog/how-climate-change-is-impacting-cybersecurity/#:~:text=Between%20school%20and%20work%20closures,people%20at%20risk%20of%20cybercrime.

[2] *Climate change, environmental threats and cybersecurity in the European High North.* Cassotta, S., Sidortsov, R., Pursiainen, C., Pettersson, M., & Goodsite, M. E. 2020, January. isdp.eu.

[3] *Climate change and cyber threats: Acknowledging the links*. Ellen, D. 2014, September 8. The Center for Climate & Security. Retrieved March 16, 2023, from https://climateandsecurity.org/2014/09/climate-change-and-cyber-threats-acknowledging-the-links/

[4] *Environmental risks: cyber security and critical industries.* Environmental Risk Consulting Team. 2020, January. Exton.

[5] *Where do cyber threats and climate change meet?* Hope, B. 2022, February 4. Sustainability Magazine. Retrieved March 16, 2023, from https://sustainabilitymag.com/net-zero/where-security-cyber-threats-and-climate-change-cyberattack-iiot

[6] *Cyber Security's impact on climate change: What can organisations do?* Irwin, L. 2022, March 24. IT Governance UK Blog. Retrieved March 16, 2023, from https://www.itgovernance.co.uk/blog/cyber-securitys-impact-on-climate-change-what-can-organisations-do

[7] *Cybercrime and climate change: Why cybersecurity is critical for all*. McKinney, T. 2022, January 5. IBSS. Retrieved March 16, 2023, from https://www.ibsscorp.com/resources/cybercrime-and-climate-change-why-cybersecurity-is-critical-for-all

[8] *Cyber security and climate change: Cyber security environment*. Nair, M. 2022. Rutherford. Retrieved March 16, 2023, from https://www.rutherfordsearch.com/blog/2021/09/climate-change-and-cyber-security-what-to-expect-in-financial-services

[9] *Climate change: Vital signs of the planet*. NASA. 2023, March 7. NASA. Retrieved March 16, 2023, from https://climate.nasa.gov/

[10] *Cyber crime.* NCA. 2023, February 9. National Crime Agency. Retrieved March 16, 2023, from https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime