BOOK CHAPTER | Two Sides of a Coin

Sustainability of the Cybersecurity and Climate: A Review of the Interconnectivity

Adekanmbi, Toyin Omoriyeba
Canadian Center for Climate Change and Adaptation
University of Prince Edward Island
Prince Edward Island, Canada
E-mail: toadekanmbi@upei.ca
Phone: +19023884970

Abstract

Climate change is a global issue common to the whole world regardless of continent, nationality, tribe, sex, or age. The temperature is rising due to the greenhouse effect as the greenhouse-gas emissions in the atmosphere are increasing. The average global temperature is increasing continuously and is predicted to rise by 2^{o}C until 2100, which would cause substantial economic losses at the global level. Cybersecurity is likewise a global issue common to everyone, just as climate change and its interaction with the physical world phenomena (e.g., weather, climate, water, and oceans) is mostly not found in modern information technology systems. The ability to relate the current climate change impact with the latest cybersecurity scenario, calls for scrutinization and making necessary recommendations. Many aspects of the cyber-security system are not known to relate to climate change and are highly fragmented. The connection between the cybersecurity system and climate change needs to be studied through a multidisciplinary approach to recommend the best way to manage these systems for sustainability, thus making both cyber laws, climate laws, and policy more effective to address any impacts they might pose to humanity. This report presents the relationships between climate change and cybersecurity while identifying their positive and negative impacts, as well as recommending ways to mitigate the impacts.

Keywords: Climate change, Cybersecurity, Sustainability, Cyberattack, Interconnectivity

Introduction

Climate change is a change in the usual weather located in an area. This may be a change in how much rain falls in an area per year or could be a change in an area's regular temperature for a month or season. Climate change is likewise a change in Earth's climate. This may be a change in Earth's regular temperature, a change in the area where rain and snow commonly fall on Earth.

Citation: Adekanmbi, T.O. (2022). Sustainability of the Cybersecurity and Climate: A Review of the Interconnectivity SMART-IEEE-ACity-ICTU-CRACC-ICTU- Series Book Chapter on Web of Deceit. Pp 311-316 www.isteams.net/bookchapter2022. dx.doi.org/10.22624/AIMS/BK2022-P48

Weather can change in only some hours. Climate takes loads or maybe tens of thousands and thousands of years to change [10]. It is a widely accepted fact that the climate is changing. The Fifth Assessment Report of the Intergovernmental Panel on Climate Change stated that the atmospheric concentrations of the greenhouse gases, such as carbon dioxide (CO_2), methane (CH_4), and nitrous oxide (N_2O), have accumulated to a remarkable level in the last 800 000 years [6]. It is unequivocal that human impacts have warmed the atmosphere, ocean, and land. Widespread and fast modifications in the atmosphere, ocean, cryosphere, and biosphere have occurred [5]. The Intergovernmental Panel on Climate Change gave a report, expressing extreme worries about the prospective climate change impacts, now and in the future. Broadly speaking, people around the world agreed that climate change poses an intense danger to nations [8]. Cybersecurity is a process by which the systems, sensors, and wireless communications are protected from digital attacks [9]. Cybersecurity is the frame of technologies, processes, and practices designed to guard networks, gadgets, programs, and data from attack, damage, or unauthorized access. It can also be called information technology security.

Fig 1: Climate Change and Cyber Threats
Source:https://climateandsecurity.org/2014/09/climate-change-and-cyber-threats-acknowledging-the-links/

Cyber protection is vital because the government, military, corporate, monetary, medical, and scientific agencies collect, process, and store quantities of important data on computer systems and different gadgets. A substantial part of that data may be confidential and unauthorized access could have a terrible consequence. Sensitive data are transmitted by organizations through networks and to different gadgets while doing business, and cyber security describes the field devoted to protecting that data and the structures technique used [4]. Apart from the coronavirus pandemic and its associated healthcare and monetary fallout, climate change and cybersecurity to many are the two most pressing issues our planet is facing now and probably in the future, they are separate issues, to be sure. But there are a few areas, however, wherein cybersecurity and climate change overlap, interlock, and affect one another [1].

The Interconnectivity of Cybersecurity and Climate Change

At first instance, it could appear unpersuasive to accept the fact that there is an established link between cybersecurity and climate change; however, climate change can affect, for example, digitally operated physical infrastructures with the high possibility of significantly disrupting their systems, affecting various dimensions of human security [7]. Climate change and cyber threats are security risks that could influence the safety and security of basic resources, which includes water, energy, and infrastructure, generally because of a not unusual place factor: interconnectedness. As humans and as nations, we will always be linked to our environment, because it gives us the necessary resources essential for survival and prosperity. We have additionally turned out to be in detail linked and dependent on our computer-based technologies, with cyberspace and the Internet being a number one conduit [12].

Challenges do now no longer only arise from cyber-attacks on digital infrastructure; they can also arise from climate change–prompted natural catastrophes. For example, natural disasters may also disrupt communication networks and consequently halt digital service, inclusive of health care, education, everyday financing, and so on [7]. Global climate change and cyber threats are the foremost worldwide challenges in terms of law and control. Even though variables affecting climate change, and cyberthreats are different, they gave a comparable characteristic from a regulatory and management perspective as they are associated with dangers of anthropogenic nature affecting important equities, consisting of key sectors of important infrastructures [1].

Many infrastructures affected by climate change, and the infrastructures assisting our cyberspace and the Internet, had been created without considering the security risks climate change and cyber threats, could have. The infrastructures had been in large part constructed in a time when each threat had been non-evident, poorly understood, or ignored. Original service infrastructures are specifically susceptible to climate change. And simply as climate change can influence our access to water and energy, a cyber-attack on computer systems and commercial equipment running water treatment facilities, electric and nuclear energy plants, may have extensive poor consequences. Climate change and cyber-threats often affect the same critical infrastructures [12]. Climate change and threats to cyber protection vis-à-vis critical infrastructures have implications for societal well-being because each can impact the functioning of an electric-grid gadget, water gadget, or energy supply chain [7].

Cybersecurity Impact on Climate Change

Digitization growing rapids has contributed to economic and social improvement and has also helped to improve environmental protection. Meanwhile, it additionally made socio-technical systems and ecosystems greatly liable to cyber-threats. Critical infrastructure (CI) in the energy sector is liable to such threats as remoteness, seasonal darkness, and excessive climate that is turning into much less predictable because of global climate change [3]. To comprehend how climate change and the strategies to counteract its fast ascent will influence cybersecurity, there is a need to study how computing contributes to global warming. Computing includes energy consumption and heat production.

When there is no production of clean energy to fulfill our needs for electricity, the energy consumed through computing—and protection inside it—will maintain to contribute to global warming. Some fields in computing and cybersecurity guzzle up large quantities of electricity and bring the heat as a by-product, for instance, supercomputers, blockchain mining, data centers, and the Internet as a whole [1]. The threat of cyber influence or hacking, and control and possession over information and intelligence is frequently the first imagined threat to cyber security. This places the state, its infrastructure, and its establishments at the center of such threats however fail to bear in mind the effect of cyber security on the people and their communities [7].

Climate Change Impact on Cybersecurity

Conversely to the contribution of cybersecurity to climate change, global warming and its consequences on the climate, environment, and economic system do have an instantaneous effect on our ordinary lives, and that transcends down to cybersecurity. Some of the projected risks include flooding, the extension of the wildfire season, disease spread, cost of the economy, and scarcity of sparkling water. Climate change and its effects will act as a destabilizing factor on society. When livelihoods are in danger, this can initiate a lack of confidence and drive useful resource competition. This does not only have implications for physical security, however, in present-day society, this additionally influences cybersecurity and its related threats. From in worst-case-state of affairs perspective, climate change could cause profound worldwide conflicts, which move together with cyberwar. Furthermore, people that haven't any means of providing their households could flip to cybercrime, which is regularly visible as a low-danger way with a probably huge gain. But on a smaller scale, we're already seeing the influences of climate change on cybersecurity, either through social engineering scare processes embraced by hazard actors or disruptions to Internet-related domestic heating and cooling gadgets intended to track energy consumption [1].

Comparison of Climate Change to Cybersecurity

Climate change is a systemic issue, born out of many poor decisions, wrong turns, and compromises that we've together made over decades. Consequently, the effects can only be tackled collectively via addressing the systemic forces that create them. There is a need to collectively work together to recognize the systemic elements that create those threats after which we seek ways to deal with them at their core. Likewise in cybersecurity, in which the threats and vulnerabilities we address on a day by day certainly have their origin in huge scale systemic and structural forces that exists ways past our reach, we need to begin by appreciating that the emergent cyber-threat panorama is the characteristic of machine forces and are seeking to recognize the forces and their impact, in preference to focussing on the signs we see [11].

The cybersecurity framework will become more comprehensive through the utilization of human security techniques comprehensive. Instead of targeting the technical infrastructure, a complete cybersecurity technique should focus on safeguarding human wellbeing.

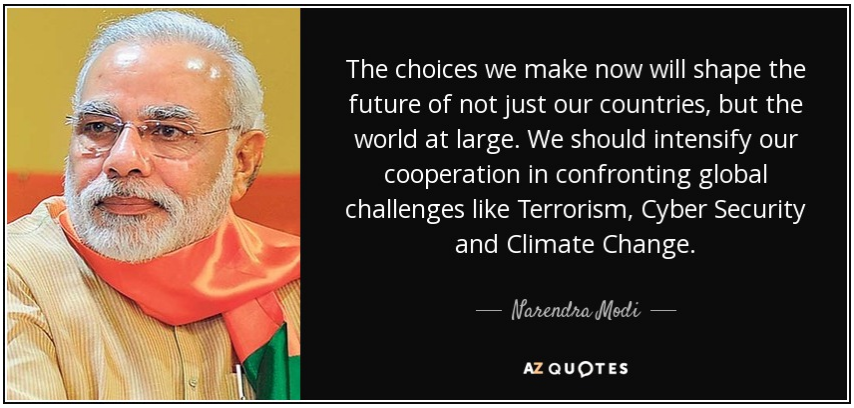

Fig 2: Climate Change and Cybersecurity Quotes
Source: https://www.azquotes.com/quote/1304282

Such a human-targeted cybersecurity technique can be applied as a tool that allows the creation of meaningful and targeted policies that addresses both the effective and terrible influences, while at the same time there is the flexibility to consider the regional peculiarities [2]. There are possibilities for those in security and computing to gradually slow the progression of climate change. But there are also possibilities for those in cybercrime to take advantage of the destabilization due to climate change, as few have already got through related scams and malware campaigns. If we do not drop the reduce or stop in the attempt to counteract global warming, we will be capable of defending against several the greater superior threats coming down the pike. But at the same time as we nevertheless can, let's rein in our carbon footprint, enhance computing efficiency, and consider our cybersecurity training when criminals come calling [1]. Vital infrastructures need to be resilient both in meeting physical climactic threats and improved human vulnerability considering cyber insecurities inclusive of cyber-attacks [7].

Conclusion

Cyberspace and global climate appear to exist separately, independently but there are many shared similarities. Though the variables that affect cyberspace is different from the one affecting climate, the risks associated with both are anthropogenic, can affect the same equities, which include our water, food, and energy infrastructures. Developing a risk mitigation technique that acknowledges these similarities is required, and inspiring cross-pollination among those key sectors, are consequently crucial first steps for making sure a climate and cyber-stable future. The society should be well informed of both menace.

In conclusion, there is a need for policymakers, managers, and treaty makers existing at international, regional, and national levels, operating in the climate and cybersecurity area, to be better informed about the transition towards sustainable "climate" and "cybersecurity" behavior that is currently taking place. One way to better understand the complexity of the system, in terms of the regulatory challenges facing most countries, is to try to find solutions within existing similar systems. Further multidisciplinary review of the research area is recommended.

References

[1] Arntz, P. (2020). The effects of climate change on cybersecurity. Malwarebytes Labs. https://blog.malwarebytes.com/awareness/2020/03/the-effects-of-climate-change-on-cybersecurity/

[2] Cassotta, S., & Pettersson, M. (2019). Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example. Beijing Law Review, 10(03), 616–642. https://doi.org/10.4236/blr.2019.103035

[3] Cassotta, S., & Sidortsov, R. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. Energy Research and Social Science, 51, 129–133. https://doi.org/10.1016/j.erss.2019.01.003

[4] de Groot, J. (2022). What is Cyber Security? Definition, Best Practices & Examples | Digital Guardian. Digital Guardian. https://digitalguardian.com/blog/what-cyber-security

[5] IPCC. (2021). The Physical Science Basis Summary for Policymakers Working Group contribution to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change.

[6] Karimi, V., Karami, E., & Keshavarz, M. (2018). Climate change and agriculture: Impacts and adaptive responses in Iran. In Journal of Integrative Agriculture (Vol. 17, Issue 1, pp. 1–15). Chinese Academy of Agricultural Sciences. https://doi.org/10.1016/S2095-3119(17)61794-5

[7] Klein, J., & Hossain, K. (2020). Conceptualizing Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change. Arctic Review on Law and Politics, 11(0), 1–18. https://doi.org/10.23865/arctic.v11.1936

[8] Pew Research Center. (2019). Climate Change Still Seen as the Top Global Threat but Cyberattacks a Rising Concern (Vol. 10). www.pewresearch.org.

[9] Salam, A. (2020). Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. In Internet of Things (pp. 299–327). Springer. https://doi.org/10.1007/978-3-030-35291-2_10

[10] Stillman, D. (2014). What Is Climate Change? NASA. https://www.nasa.gov/audience/forstudents/k-4/stories/nasa-knows/what-is-climate-change-k4.html

[11] van der Walt, C. (2020). Climate change in cybersecurity - Global. Orange Cyberdefense. https://orangecyberdefense.com/global/blog/cybersecurity/climate-change-in-cybersecurity/

[12] Werrell Caitlin, & Femia Francesco. (2014). Climate Change and Cyber Threats: Acknowledging the Links. The Center for Climate & Security. https://climateandsecurity.org/2014/09/climate-change-and-cyber-threats-acknowledging-the-links/

Web Reference

1. https://www.azquotes.com/quote/1304282
2. https://climateandsecurity.org/2014/09/climate-change-and-cyber-threats-acknowledging-the-links/