Unveiling Connections: Integrating Climate Studies and Cybersecurity Education

MARY TEDESCHI, Pace University

The aim of this paper is to suggest the introduction of a new minor program in climate studies at a major University, emphasizing its interdisciplinary nature and the benefits it offers to students. Future plans include the development of a major in Climate. The primary goal is to emphasize the significance and pertinence of addressing climate change using an interdisciplinary framework, highlighting the potential of incorporating this minor to make optimal use of current course design patterns. By offering a minor in climate, students will have the opportunity to explore the study of climate change, its consequences, and the creation of sustainable solutions. Additionally, it will foster a comprehensive understanding of the intersection between technology and environmental challenges, equipping students with valuable knowledge for the future. Climate change is one of the most pressing issues of our time. The climate change minor gives the students the opportunity to explore climate change from varied disciplinary perspectives while gaining a firm grounding across all academic departments including African American studies, architectural technology, biological science, business, chemistry, computer systems technology (CST), physics, dental hygiene, math, English, Social Sciences, nursing - to name a few. Students from all academic departments can apply for the minor in climate change. One of the goals of the program will be to describe the physical mechanisms that underlie climate change and the drivers of uncertainty in future climate projections. Alexander writes, "There is one timeless way of building. It is thousands of years old, and the same today as it has always been. The great traditional buildings of the past, the villages and tents and temples in which man feels at home have always been made by people who were very close to the center of this way. And as you will see, this way will lead anyone who looks for it to buildings which are themselves as ancient in their form as the trees and hills, and as our faces are." The climate is thousands of years old; Alexanders's principles can guide the design and structure of the proposed minor. This paper will employ Alexander's principles to help create that new course, a minor in climate. The students will relate climate and cybersecurity, which many did not believe had any relationship.[1] The target audience of this paper includes educators seeking to implement innovative curricula, prospective students interested in exploring climate studies, and patterns enthusiasts. Specifically, the main focus of this paper is the computer systems technology department and the introduction of information for a security course. The proposed minor extends its implications to a broader range of academic departments within the college.

Categories and Subject Descriptors: K.3.2 [**Computers and Education**]: Computer and Information Science Education —*Computer science education* General Terms: Patterns, Hybrid Pedagogy

General Terms: Patterns, Collaboration

Additional Key Words and Phrases: Environment, cybersecurity, climate studies, interdisciplinary education, course design, climate change, pedagogical patterns, sustainable solutions

ACM Reference Format:

Tedeschi, M, 2024. Unveiling Connections: Integrating Climate Studies and Cybersecurity Education. HILLSIDE Proc. of Conf. on Pattern Lang. of Prog. 30 (October 2023), 14 pages.

1. INTRODUCTION

Climate and cybersecurity are two distinct but interconnected areas of concern in today's world. While they may seem unrelated at first glance, they intersect and influence each other in several important ways. Although climate change and cyberspace are different phenomena, the risks associated with both of them are anthropogenic and can affect the same critical equities - including key sectors such as water, food and energy infrastructures.

Anthropogenic environment refers to human-induced environmental changes. Examples of anthropogenic environment can be divided into broad categories: pollution, land-use change (including habitat loss and fragmentation), climate change, overexploitation of natural resources, and the introduction of invasive alien species. The integration of climate and cybersecurity is of paramount importance in addressing the pressing challenges of the modern era, as it not only safeguards critical infrastructure against cyber threats, but also enhances resilience in the face of climate change, ensuring

sustainable development and global security. For example, hurricane Sandy hit New York on October 29, 2012, major data centers were affected, leading to internet disruptions. Natural extreme weather events can damage physical infrastructure leaving them vulnerable to attack. Lower Manhattan was without power from 39th street down. The pressing need to confront climate change and the importance of cybersecurity education in our contemporary, highly interconnected world cannot be overstated. Figure 1 illustrates the title as an abstract drawing:

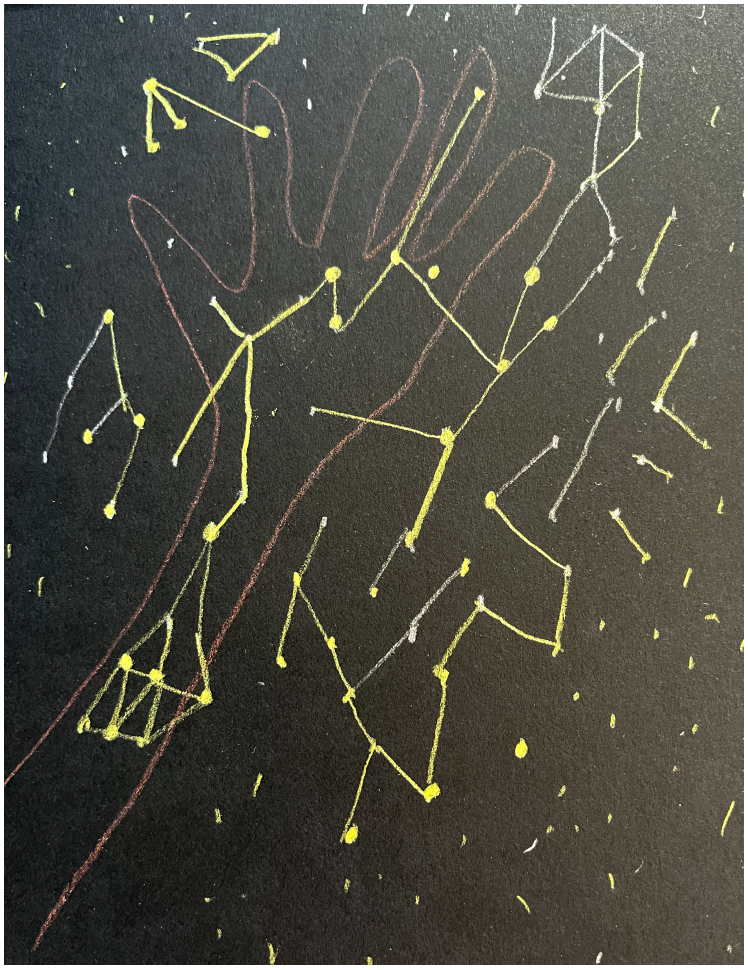

Fig. 1. Original hand drawing by author. Visual depiction representing the title.

- Environmental Impact on Cybersecurity: Climate change and its associated consequences, such as extreme weather events, can have a direct impact on cybersecurity. Disruptions caused by natural disasters like hurricanes, floods, or wildfires can damage critical infrastructure, including data centers and communication networks. Such incidents can lead to service outages, data loss, and even breaches in security, leaving organizations vulnerable to cyberattacks. Environmental disruptions can lead to physical damage, resource scarcity, and increased vulnerabilities in cybersecurity, topics that will be explored in greater detail in the paper.

- Cybersecurity Risks to Climate Infrastructure: As the world becomes more reliant on interconnected systems for managing climate-related infrastructure, such as smart grids, renewable energy networks, and environmental monitoring systems, the risks of cyber threats increase. Unauthorized access, data manipulation, or sabotage of these systems can have far-reaching consequences, disrupting energy supply, impeding climate research, or affecting emergency response capabilities. Disaster management, and sustainable practices to address the

challenges posed by climate change can be taught in a course to the students. We do this now, but we don't emphasize climate. In a region heavily reliant on renewable energy sources like wind and solar power, there is a well-connected and automated energy grid that balances the production and distribution of electricity from various sources. This grid relies on interconnected systems, including smart meters, sensors, and control systems, to optimize energy production and manage demand. A cyberattack on a renewable energy grid where a malicious actor launches a cyberattack targeting this renewable energy grid.

- Data Privacy Concerns: Sensitive data collection in climate research involves the acquisition of information that is confidential, proprietary, or personally identifiable and is subject to stringent ethical, legal, and privacy considerations. Students might need Institutional Review Board, or IRB approval for data collection. Climate-related initiatives often involve the collection and analysis of large volumes of sensitive data, such as personal information, geographic data, or climate modeling data. Protecting this data from unauthorized access or breaches is crucial to maintain privacy and prevent potential misuse. Robust cybersecurity measures are necessary to safeguard this information and maintain public trust in climate-related initiatives.

- Interconnectedness of Global Issues: Climate change is a global challenge that requires international cooperation and information sharing. Similarly, cybersecurity threats know no boundaries and require collaborative efforts to combat them effectively. Addressing both climate change and cybersecurity necessitates cooperation among governments, organizations, and individuals to develop shared strategies, policies, and frameworks. The United Nations works with various countries to create climate change partnerships by drawing upon knowledge and expertise to promote positive, solutions-driven approaches to combat climate change.

Green Technologies and Cybersecurity: The adoption of green technologies, such as renewable energy sources and energy-efficient infrastructure, is vital for mitigating climate change. However, these technologies also introduce new cybersecurity challenges. For instance, the increased use of Internet of Things (IoT) devices and cloud-based systems in smart grids and renewable energy networks can create vulnerabilities that cybercriminals can exploit. Building resilient and secure infrastructure is essential to ensuring the sustainable deployment of green technologies. Green technologies, such as smart grids, introduce vulnerabilities that cybercriminals could exploit to disrupt energy distribution, manipulate grid operations, or compromise critical infrastructure.

This paper employs pedagogical patterns, such as "New Pedagogy for New Paradigms" and "Abstraction Gravity", to design the structure of the proposed minor in Climate Studies. The integration of climate and cybersecurity will be explored, illustrating the unexpected connections between these seemingly unrelated fields. The proposed minor extends its implications to a broader range of academic departments within the college, fostering collaboration and interdisciplinary learning.

In summary, climate change and cybersecurity are interconnected through their impact on critical infrastructure, data privacy concerns, the need for international collaboration, and the challenges posed by emerging green technologies. Addressing these interdependencies is crucial for building a resilient and sustainable future that is both environmentally secure and cyber resilient. I used the Invisible Teacher pattern [2] for active learning to emphasize ACTIVE STUDENT (also a pattern). Usually, the teacher is the central point of a training environment. A discussion forum was created for the students.

2. STUDENT FEEDBACK

Student feedback is a valuable tool for assessing educational experiences, helping institutions improve teaching and learning outcomes. The students in my undergraduate course, Introduction to Information Security, were asked their opinion on adding a minor in climate to the curriculum, and the following feedback was gathered from them. The text concludes with students expressing their interest in learning more about climate change, global warming, and the intersection of IT and climate. Find student feedback in Appendix.

3. SUGGESTIONS FOR COURSE IMPROVEMENT

The cruise ship industry is subject to increasingly stringent environmental regulations to mitigate its impact on climate change, including emissions reduction targets and measures to minimize air and water pollution. To meet these regulations, cruise ships have adopted advanced technologies and interconnected systems, such as emissions control systems, GPS monitoring, and onboard waste management systems. Several years ago, a colleague of mine graduated with his technology degree and obtained a good job on a cruise ship. He was a computer programmer. Now I am aware that every cruise ship contributes to the degradation of vital seagrass that provides manatees' primary course of nutrition. Ships the size of city blocks sail close to shore, disturbing manatees' fragile habitat, churning up sand and sediment pollution and dumping massive quantities of filthy, contaminated wastewater into their feeding grounds. That means manatees die suffocating from the lack of oxygen and withering away from starvation. Without urgent action to stop cruise companies from destroying their habitats, manatee populations could plummet back to the brink of extinction. This could be a topic for a group project in our class.
Also, American companies are beginning to mine seaweed for protein-based HUMAN consumption. Contaminated seaweed curtains that HUMAN supplementals nutrition source (other topic for a class project). Seaweed replaces animal sourced protein because herd animals also affect climate (i.e., methane release, etc.). Seaweed mining, a practice involving the cultivation and harvesting of seaweed for various purposes, is a compelling example that highlights the interconnectedness of climate change, cybersecurity, and the subject matter of environmental sustainability.

3.1 Examine these questions: in order to improve the course

1. Is there a linkage between climate change, environmental threats and cybersecurity, and if so, what is the nature of this linkage?
2.How can the interconnectedness of environmental threats and cybersecurity be identified, managed and regulated, including aspects of governance for cybersecurity and cyber resilience?
3.How can cyberthreats and their related risk assessments be incorporated into regulatory frameworks in order to create proactive rather than reactive law? Which is the best regulatory framework (or possible combination) applicable among different possible areas and levels of regulations?
4.What are the current cyberthreats, for example, in the energy industry and to critical infrastructures (CIs) of the energy system?

3.2 Rationale

This can include but is not limited to the following:

- Wide range of Academic Minors offered at NYCCT as well as other CUNY colleges.
- Can use pre-existing Academic Minors at City Tech as examples, and in time can cite their outcomes.
- Description of the proposed Academic Minor, indicating the subjects involved and whether it focuses on a single discipline or is multidisciplinary.

- Discuss how proposed Academic Minor will give students an opportunity for academic exploration as well as additional depth of focus.
- Discuss how the learning outcomes associated with the Academic Minor ties in with increased post-graduation opportunities.

3.3 Requirements of the Proposed Academic Minor

General Requirements:

All proposed Academic Minors will be designated as a major curriculum change.

Indicate the number of credits required.
12 or more credits; no more than 15 credits are recommended but if more credits are required then provide a sentence indicating how the additional credits are needed in order for students to achieve the learning outcomes of the Academic Minor.

Statement that students must achieve a grade of 2.0 or higher in all courses that contribute towards the Academic Minor in order to be granted a Minor designation on their transcripts.

Required Courses:

An Academic Minor has at least one required foundational or capstone course. For interdisciplinary Minors, there can be a designated group of foundational courses from which to choose.

Foundational Course or Culminating Experience: *This could also come in the form of an Honors Project, Independent Study, Internship or Undergraduate Research project.*

Prerequisites: *Explicitly indicate any prerequisite courses that are needed for entry into the Academic Minor.*

Structure of Administration and Advisement

This shall include but is not limited to the following:

Identification of the Academic Minor Coordinator or Chair.
Description of advisement procedure and strategies for prospective and enrolled students.

The patterns help create the algorithm for new course design.

Prior to the Course: (Patterns) Implement
NEW PEDAGOGY FOR NEW PARADIGMS
ABSTRACTION GRAVITY
REARRANGEMENT
These patterns are from Pedagogical Patterns [2].
Explain how humans interact with climate change. The ABSTRACTION GRAVITY pattern is important to implementing climate linkage throughout the course. At the end of Spring 2023 semester, students did not see a connection between climate and the information security course. After an online discussion, we proved there is a linkage. We want the students to analyze and design to establish a relationship between climate and the CST course.
There are several areas of the current course that could incorporate the climate minor. Computer laws and ethics, risk management, physical security are three broad topics taking 4 weeks of the

course. Specific climate examples can easily be incorporated into the syllabus. We also have a special topics week which can be devoted to climate studies and information security. Students can be made aware of climate as a driver for change.

The learning outcomes for the students - acquire knowledge of key issues and trends in sustainability and climate policy. They will synthesize and evaluate information from the information security perspectives to describe, interpret and critically analyze information about environmental issues, practices and policies in relation to information security. Students will learn to effectively communicate their ideas, both orally, visually, and in writing. The students will work collaboratively. Finally, it is hoped that the knowledge gained will influence student behavior outside the classroom and affect climate imbalances in their real-world living.

NEW PEDAGOGY FOR NEW PARADIGMS, written by Joe Bergin. You are teaching something new to you.

ABSTRACTION GRAVITY. written by Gary L. Craig and revised by Jane Chandler. You are about to start a new topic, which has many levels of abstraction.

REARRANGEMENT, written by Kerstin Voigt and revised by Marianna Sipos. This pattern is based on Big Picture on a Small Scale, written by Kerstin Voigt. You want to teach technologies and concepts which are new and have become essential, and you want the existing material to respect this new progression.

From Design Thinking, the pattern, IT TAKES A VILLAGE, is incorporated as the problem states the breadth of knowledge required to resolve complex problems exceeds that possessed by a single individual, discipline, or specialty [3].

Christopher Alexander's principles can guide the design and structure of the proposed minor. Trying to pull the order of the world from our own being is what the patterns are about. How do the students view the world now and how can they change and improve the climate around them through the use of technology?

Table 1 Based on various UN sources un.org

Causes of Climate Change	Effects of Climate Change
Generating power	Hotter temperatures
Manufacturing goods	More severe storms
Cutting down forests	Increased drought
Using transportation	A warming, rising ocean
Producing food	Loss of species
Powering buildings	Not enough food
Consuming too much	More health risks
Drought	Poverty and displacement

From an information security standpoint, computers become outdated every 18 months according to Moore's Law. What happens to our old equipment? Does it end up in a landfill? Under manufacturing goods, are we causing climate change? One way cybersecurity affects climate change and adds to global warming is through actual computing which entails energy consumption and encourages thermal emissions. Are the climate change crisis and rise of cybersecurity attacks intertwined? There may be no direct causal relationship between climate change and cybersecurity, but climate change may result in more cyber-attacks. Cybercriminals may exploit cyberthreats, instability and disruptions. Table 1 depicts the causes and effects of climate change based on United Nations (UN) findings.

4. DISCUSSION

The most difficult aspect of understanding design and design thinking is not the thinking, it is the mind you think with [4]. It is the worldview: what is known and real, what is valuable and how things are done. You are teaching something new to you. The thing you need to teach has characteristics different from what you are used to, requiring different thinking modes on the part of users.[3] The pattern author, is discussing teaching functional programming. Here, we are incorporating climate as a study. Match the pedagogy to the thinking modes required in the paradigm you are teaching [3]. The potential impact of the proposed minor in climate studies could lead to a major in climate studies. Students will benefit by learning cutting edge technology and life-changing concepts. This minor will contribute to the overall education and development of individuals in many ways. Maybe with less pollution and a better climate we will have less cancer. Design thinking can be employed to bridge the gap between climate studies and cybersecurity education by fostering innovative solutions that address the intersection of these two fields. By applying design thinking principles, educators, researchers, and industry professionals can foster a holistic approach to addressing climate-related challenges while strengthening cybersecurity education, ultimately creating a more resilient and environmentally responsible future.

5. CONCLUSION

How can we distinguish patterns that work? How can we distinguish patterns which work, which are deep and worth copying, from those which are simply pipe dreams, mad imaginings or irrelevant. One test says that a pattern is alive if its individual statements are empirically true. But a pattern is not alive just because its component statements are true, one by one. The fact is that even though its individual component statements are true, the pattern has no empirical reality as a whole. Even the fact that a pattern seems sensible, and has clear reasoning behind it, does not mean at all that the pattern is necessarily capable of generating life. A pattern only works, fully, when it deals with all the forces that are actually present in the situation [1] and alters for the good.

Today, we stand at a critical juncture where the choices we make have profound implications for the world we pass on to future generations. We have a unique opportunity before us - the proposal for a minor program in climate studies. This initiative isn't about adding another line to our academic offerings; it's about preparing ourselves and the generations to come for the challenges of our time. Young people think climate change is a top issue, but when they vote, it is complicated. Over the last decade, climate change has emerged as a top political issue, particularly for younger voters. But polls routinely show climate change lags other items, like traditional pocketbook economic issues, that can motivate voters. Do we care about the climate?

The importance of this proposed minor program cannot be overstated. Climate change is no longer a distant threat; it is happening now, affecting ecosystems, economies, and communities worldwide. To navigate this crisis, we need more than just awareness; we need expertise, solutions, and innovation. The minor is the first step. Imagine a future where graduates from our institution possess a deep understanding of climate science, sustainability, and the intricate connections between climate change and cybersecurity. These future leaders will be equipped to tackle complex issues, find innovative solutions, and shape policies that safeguard our planet.

6. ACKNOWLEDGEMENTS

I want to thank my shepherd Rebecca Rikner, as it is an honor to have you as my shepherd. I would like to thank Reginald Blake, Hamidreza Norouzi, Ivan Guzman Pena, Sean Macdonald, Alexander Aptekar, Robin Michals, Viviana Acquaviva, Daniela Vladutescu of CityTech regarding helpful discussions for climate change research initiative in our school. I would like to thank the students in CST 2410 Spring 2023 who added helpful comments to the discussion board regarding the connection between climate and cybersecurity. Thank you to Sridevi Ayloo for helpful comments while drafting this paper. Thank you to my workshop group: Neil Harrison, Charles J. Danoff, Raymond S. Puzio, Takashi Iba, Hiroaki Tanaka, Sae Adachi, Mizuki Ota, and Urara Tajima. Special thanks to my dear cousin, Richard Karcher for reading this paper and taking the time to correct grammar as only an expert English teacher could.

APPENDIX

PATTERNS MENTIONED

NEW PEDAGOGY FOR NEW PARADIGMS
ABSTRACTION GRAVITY
REARRANGEMENT

Online Appendix to:
Unveiling Connections: Integrating Climate Studies and Cybersecurity Education

A. STUDENT ACTUAL FEEDBACK

A.1. Results

Colleges should strongly consider implementing diligent changes in cybersecurity practices. In today's increasingly interconnected world, the importance of safeguarding sensitive information and digital assets cannot be overstated. Cyber threats, such as data breaches and malicious attacks, continue to evolve in complexity and sophistication. By embracing diligent change, colleges can proactively adapt to these threats, strengthening their security posture and protecting valuable data. Implementing regular updates and patches, enforcing strong password policies, conducting regular vulnerability assessments, and educating staff and students about cybersecurity best practices are crucial steps in mitigating risks. Failure to prioritize diligent change can lead to devastating consequences, including reputational damage, compromised personal and financial information, and disruptions to essential services. Therefore, colleges must recognize the urgency of embracing diligent change in cybersecurity to ensure the integrity and security of their digital infrastructure.

It is hard to imagine the link between climate change and cybersecurity. However, there are several reasons why businesses would benefit from this study. According to the CEO and founder of Global Secure Founders, Chloe Messdaghi, climate change can create more cybersecurity risks on global supply chains, “particularly for industries that rely on raw materials, energy, and transportation.” This would make businesses turn to alternative suppliers and adopt new technologies, in turn, create new vulnerabilities that can be exploited.

I think the idea of implementing climate change in cybersecurity for the next semester is excellent. Educating students on this subject is something very important and necessary since there is a growing concern that climate change could have a significant impact on computer security. One potential consequence of climate change is an increase in natural disasters such as hurricanes, floods, and wildfires. These disasters can damage data centers, disrupt power grids, and leave businesses vulnerable to cyber-attacks. Rising sea levels can also threaten critical infrastructure, including undersea cables and offshore data centers. Additionally, as global temperatures continue to rise, there may be an increased demand for cooling technology, which in turn could lead to higher energy consumption and greenhouse gas emissions. Addressing climate change is therefore not just an environmental issue, but also a critical component of ensuring the long-term security and resilience of our digital infrastructure.

If we are talking about the climate minor in the school, then it is a good topic to talk about because it will give students a strong understanding of the climate and make them want to explore.

This semester when we touched upon the topic of information on climate, we looked into how climate and natural disasters affected information and security. Some suggestions that can possibly be implemented are activities or videos providing more insight on the topic and touching more into how climate can affect cybersecurity as we come out with more technological advancements.

Climate models are computer programs that simulate weather patterns over time. By running these simulations, climate models can estimate the Earth’s average weather patterns—the climate—under different conditions. They are an essential tool for understanding the Earth’s climate and making projections for this century or the next. My suggestion is to talk about the next decade will be defined by climate change and cyber risk and why is the reason for this.

I agree. I believe that it would be interesting to know how climate will affect cyber risks in the near future, taking into consideration that the topic of climate change has always been up for discussion.

To improve your course with information on climate, one thing I would say is:

Incorporate climate change fundamentals: Provide an overview of the basic concepts of climate change, including its causes, impacts, and potential solutions. Cover topics such as greenhouse gases, global warming, climate variability, and climate adaptation/mitigation strategies.
Climate plays a big role in physical security as well as in some cases nonphysical.
We had a chapter that focused on different types of disasters and how they affect physical security.
My suggestion is to focus on the USA climate and focus on how to prepare and what to do after a climate event.
In addition, some technologies only work in certain climates. Maybe there can be some focus on those technologies and how to work around them.
Climate Change is also another topic and what technologies can help and protect us in this scenario
I agree, focusing on the USA climate while relating back to technology with keep the class more engaged and students will be eager to learn more about it.
I agree with you wholeheartedly that climate-related issues are increasingly critical in today's world, influencing various aspects of our lives, including our physical safety and security.
Your suggestion to concentrate specifically on the USA's climate provides an intriguing lens through which we can examine these issues. Considering the country's diverse geography and climate patterns, this focus will enable us to cover a wide array of climate-related challenges and their impact on physical security.
Additionally, your point about certain technologies being climate-dependent is well taken. I believe a section dedicated to these technologies, their limitations, and possible workarounds would add significant depth to our exploration. This could range from simple solutions like using equipment rated for certain environmental conditions to more complex topics like how to operate drones in inclement weather or maintain network stability during natural disasters.
We should put climate topics because the potential future effects of global climate change include more frequent wildfires, longer periods of drought in some regions, and an increase in wind intensity and rainfall from tropical cyclones. Climate change can affect long-term shifts in temperatures and weather patterns. These shifts may be natural, but since the 1800s, human activities have been the main driver of climate change, primarily due to the burning of fossil fuels (like coal, oil, and gas) which produce heat-trapping gases.
We have all heard about the effects of climate change: More frequent and extreme weather events are occurring and will only continue. Climate change increases cyber threats, instability, and disruptions that can be exploited by cybercriminals.
Adoption of green technology -- or adoption of any new technology -- introduces new attack vectors. Attacks on these systems could result in disruptions or loss if not properly secured.
IoT devices, adopted by many organizations to manage and monitor climate risk, come with their own set of security considerations and issues.
I completely agree with your viewpoint that climate change can have a significant impact on computer security. The vulnerabilities that arise from new technologies and the increasing frequency of extreme weather events create new opportunities for cybercriminals to exploit. It is crucial that organizations prioritize the security of these systems to prevent any potential loss or disruption.
Start with these ten actions to help tackle the climate crisis.
Save energy at home. ...
Walk, bike, or take public transport. ...
Eat more vegetables. ...
Consider your travel. ...
Throw away less food. ...
Reduce, reuse, repair & recycle. ...
Change your home's source of energy. ...
Switch to an electric vehicle.

You can do a topic of discussion where how environmental security is threatening internet evolving over the years.
At first instance, you may ask what does climate have to do with information technology or information security and the answer in short is everything as a matter of fact, climate impacts every area of study, every aspect of our daily lives and now more than ever it is everyone's responsibility to take action to reduce their contribution to the adverse effects of the shift in the climate in this time. The carbon emission and the chlorofluorocarbons that are breaking up the ozone layer causing more harmful UV rays to reach the earth's surface resulting in the surface of the earth warming up has negative impacts around the world. Ice caps and glaciers are melting causing sea level to rise, resulting in increased flooding that is affecting places that never flooded before and especially poor countries with poor drainage structures and islands. In islands that experience the dry season and rainy season are getting more rain in the dry season and excessively more rain in the rainy season causing, reduce production in crops and vegetation and overall inflated price for food. The rising temperatures of the earth's surface are causing droughts and shortage in drinking water in Arizona and South Africa for example.
Every person is responsible for reducing their carbon footprint, reducing the use of carbon emitting gases in our daily household usage and we can switch to electric cars or hybrid cars. Carsare responsible for 29% of the greenhouse carbon emission. In New York City there is an efficient public transportation system so more people here can opt to leave their cars at home and travel.
The field of ICT has an enormous impact on climate and the dependability on it is increasing day by day. For example, detection systems are being invented to better predict the weather, detect earthquakes, tsunamis and floods to name a few. We as IT students, have to be privy to this knowledge now because in the next 4-5 years or less we will be active employees and participants in the field and the ideas and knowledge we gained can add to solutions to our current and immediate climate crisis.

Cyber Threats to Climate Data: Examines the cybersecurity risks associated with climate data collection, storage, and analysis. It covers topics like data integrity, privacy concerns, and the protection of sensitive climate-related information.
Cybersecurity for Renewable Energy Systems: Focuses on securing renewable energy systems, such as solar, wind, and hydroelectric power plants, against cyber threats.
Climate Change and Cybersecurity Policy: Examines the policy implications of climate change and cybersecurity, exploring how governments, organizations, and individuals can develop strategies to address both challenges.
Ethical Hacking for Environmental Protection: Ethical hacking techniques with environmental protection efforts. It explores how ethical hackers can contribute to securing environmental systems, identifying vulnerabilities in climate-related infrastructure, and working toward sustainable solutions.
Considering Climate in terms of Computer and Cybersecurity seems to be a good approach. Climate change requires new strategies for dealing with traditional IT and information security risks. It would give us an opportunity for those who are willing to understand and to teach it that way to different students in different ways. It also takes care of risks that would affect climate change. Such Risks are as follows:
-Regulatory risk: Organizations need to adapt to updated and new regulations. Some business leaders are seeking regulatory guidance to better define their responsibilities.
-Supply chain risk: Business leaders should not depend on getting everything they need from traditional sources. Supply chain regulatory mismatches may also come into play, given global supply chain partners.

-Product and technology risk: New issues may arise around the production and use of existing products and technologies.
-Litigation risk: New risks may arise comparable to those in other fields such as tobacco and asbestos.
-Financial risk: Climate change will financially affect consumers, the use of natural resources, and global trade, and will likely require new measures to safeguard the business.
-Reputational risk: The need (or lack thereof) to exhibit a high level of corporate social responsibility in this area can affect reputation, positively and negatively.
I hope this best helps in terms of its implications.
I agree with you that approaching climate change in terms of computers and cybersecurity is a beneficial approach. Climate change poses unique challenges that require new strategies for managing IT and information security risks. By integrating climate considerations into these domains, we can develop innovative solutions and educate students and professionals about the intersection of technology and environmental issues.
Integrating climate change into a course on computer security can be a fascinating, interdisciplinary approach. Here are a few suggestions:
Green Cybersecurity Practices: This could involve studying how to design systems and processes that consume less energy, thus reducing carbon emissions. For example, efficient coding practices, virtualized environments, and effective power management can be part of this module.
Climate Data Security: Cover the importance of securing climate-related data, such as data from weather stations, satellites, and other monitoring systems. Discuss the potential consequences of such data being manipulated or compromised, which could affect everything from daily weather forecasts to long-term climate modeling.
Role of Cybersecurity in Renewable Energy Systems: Discuss the importance of security in renewable energy infrastructures like smart grids, wind turbines, and solar panels. These systems are often connected to the internet and are therefore vulnerable to cyber-attacks. An attack could disrupt the supply of renewable energy, leading to increased use of fossil fuels.
Impact of Climate Change on Cybersecurity: Climate change can have direct and indirect effects on cybersecurity. Direct effects could include damage to infrastructure from extreme weather events, while indirect effects could include increased cybercrime due to social and economic instability.
Environmental Impact of Cryptocurrencies: Cover the environmental impact of cryptocurrencies, which require substantial computing power and hence energy consumption. Discuss the security aspects of cryptocurrencies and blockchain, as well as how to mitigate their environmental impact.
Cybersecurity in Climate Change Mitigation and Adaptation: Discuss the role of cybersecurity in technologies used for climate change mitigation and adaptation. This could include everything from secure communication systems for emergency response to the security of climate research data.
Climate Modeling and AI: Discuss the role of AI in climate modeling and prediction, and the importance of securing these AI systems. A breach could lead to manipulated data and incorrect predictions, which could have wide-ranging consequences.
Climate Change and Ethical Hacking: Introduce the idea of ethical hacking as a means to secure systems and contribute to the fight against climate change. Ethical hackers could help identify vulnerabilities in systems related to climate data collection, renewable energy, and more.
I think a minor in climate would be an interesting venture to explore in an academic setting that would give us a better understanding of ways that we as a growing population affect the natural world as well as give us an insight into the topic that would not really come up in our daily lives.
What would you like covered? What would you like to learn about? Do you have any wonderings?
The climate isn't a topic that I can say I've had great exposure to throughout my studies but the one aspect of it that would consider learning more about would be global warming which is a topic that a lot of us are aware of but doesn't have an in-depth understanding about it. Therefore, I believe that this would be an interesting aspect of global warming to learn more about.

I hold a different perspective and strongly believe that studies in climate hold great relevance for us as IT students. It is my desire to witness a comprehensive exploration of topics that delve deeper into the ways technology can contribute to mitigating our ongoing climate crisis. While I am aware of certain detection systems utilized for earthquake, flooding, and tsunami detection, I am eager to acquire more knowledge about the intersection of IT and climate.

REFERENCES

[1] "The Timeless Way of Building", Christopher Alexander, Oxford University Press, 1979.
[2] Pedagogical Patterns - The Pedagogical Patterns Project January 2012 Edition: Pedagogical Patterns: Advice for Educators Publisher: Joseph Bergin Software ToolsEditor: Bergin J. ISBN: 978-1-4791718-2-8
[3] Design Thinking: The Key to Enterprise Agility, Innovation, and Sustainability, David West, Rebecca Rikner, 2017, 0998477001, 9780998477008
[4] Cassotta, Sandra & Sidortsov, Roman. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. Energy Research & Social Science. 51. 10.1016/j.erss.2019.01.003.

Received May 2023; revised September 2023; accepted February 2024