Laidlaw Scholars Program, Leadership in Action (LiA), Professional Experience Reflection

Anna Lysenko

Abstract. My unforgettable LiA practical experience illuminated the essence of leadership: the ability to maintain unwavering flexibility and resilience in the face of unexpected and dynamic circumstances. Moreover, LiA presented me with a refreshing perspective on the interplay between expectations and reality, highlighting that while they may not always align, both harbour the potential for profound growth and unforeseen possibilities.

My initial anticipation was to engage intensively with the CyberPeace Foundation (CPF) in a dynamic in-person capacity, situated in the vibrant locale of South San Francisco. Yet, serendipity had other plans, steering me towards six weeks of remote work from a cozy inn with lacklustre WiFi and various coffee havens in an idyllic, sunny city. Unperturbed by the unexpected turn, I embarked on the endeavour to create an impactful, insightful "Cyber x Democracy" workshop. This project interwove foundational cybersecurity concepts with my research exploring the seismic impact of cyberattacks on American democracy. The culminating act saw me presenting this workshop to a global audience of dedicated CPF volunteers based in India. This journey was marked by a steadfast positive attitude in navigating challenges, ultimately rendering my LiA experience an extraordinary educational odyssey.

The Genesis. The true value of acquired and created knowledge lies in its meaningful integration into the real world. With this guiding principle, I embarked on the planning of my LiA summer almost immediately after initiating my original Laidlaw Scholars application in 2022. My research,

aimed at dissecting the extent to which cyberattacks erode American trust in government, could be implemented through three captivating opportunities within the LiA framework. These were implementing research, collaborating with a Non-Governmental Organization (NGO) for practical impact, or engaging in centrally coordinated projects. My 6-week research escapade during the summer of 2022 unveiled a disconcerting thesis – cyberattacks destabilize public trust by sowing seeds of doubt in the government's capacity to safeguard critical infrastructure, food security, and individual privacy from external malevolent forces. The most fitting response to this conclusion emerged as a twofold mission: augmenting cybersecurity awareness in the US to empower individuals against cyber threats and elucidating the intricate nexus between cyberattacks and the erosion of trust in democratic institutions.

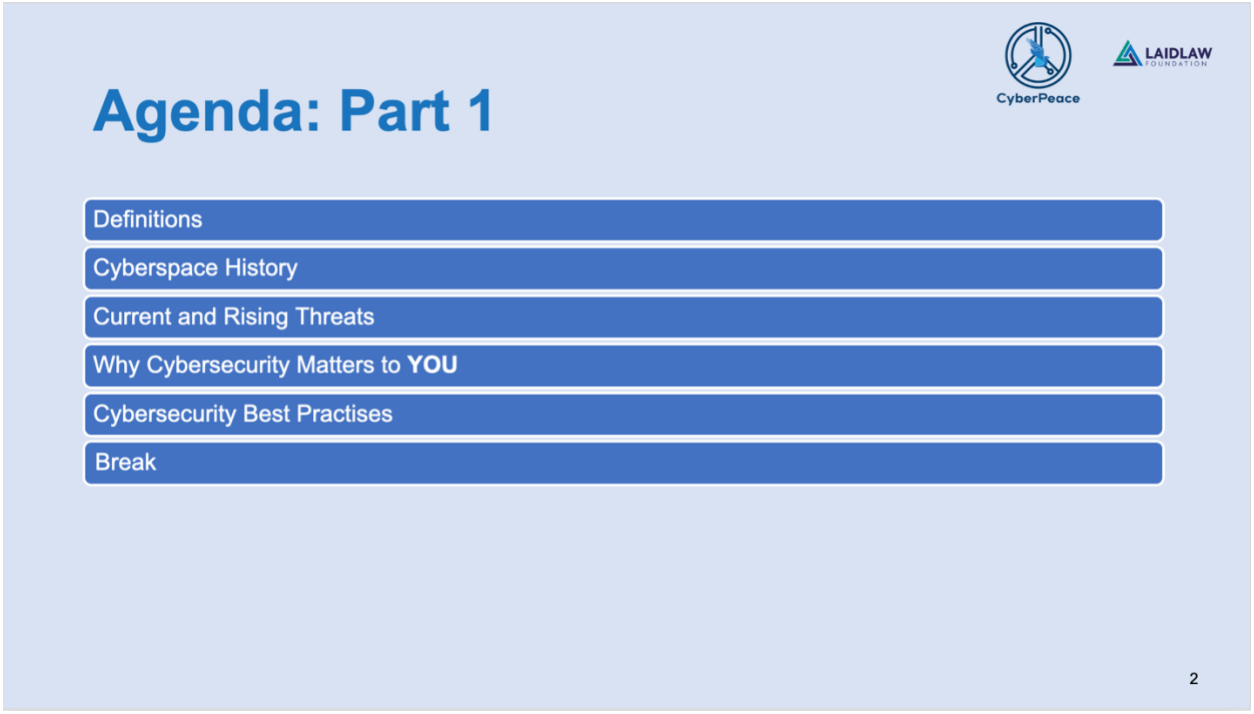
Initially, my inclination leaned towards orchestrating an in-person workshop series within the United States, capitalizing on the power of physical interactions to project my important yet seemingly abstract message. However, further reflection led me to seek collaboration with an NGO, drawn by the allure of its established network and specialized expertise. A thorough exploration of pertinent NGOs, intertwined with the realms of cybersecurity and democracy-strengthening, guided me to the CyberPeace Foundation (CPF). An alignment of values and purpose was palpable as I delved into the pages of CPF’s web presence, unveiling a shared commitment to cybersecurity advocacy. The foundation's resolute focus on awareness, education, training, and collaboration resonated deeply with the essence of my research. My aspirations found a home within the CPF's dynamic sphere, marked by a resounding harmony of purpose. A mentoring partnership with Abhishek, one of the CPF’s prominent team members, materialized, solidifying my trajectory. A transcontinental engagement with the CPF’s operations spanning

India, Africa, and the US encapsulated my aspiration for an international dimension to my research. The realization that one of the CPF's offices was nestled in the vibrant South San Francisco propelled me into an exhilarating realm of novel possibilities.

Embarking on the Journey. The landscape of San Francisco unfurled before me on May 22nd, a canvas of unexplored potential and professional camaraderie. My mind was primed for immersive engagement within a bustling professional office environment, brimming with stimulating encounters. Yet, the symphony of expectation and reality played an unexpected tune. Swiftly, it became evident that my vision of in-person collaboration was thwarted; the under-construction status of CPF's San Francisco office relegated the entire team to remote operations. This unexpected twist tested the limits of my resilience. A veil of disappointment briefly clouded my enthusiasm, an understandable response to the shift in course. However, resilience swiftly prevailed, steering me towards a transformed narrative. The verdant expanse of the Californian landscape became my workspace, as I forged ahead in the creation and presentation of the "Cyber x Democracy" workshop. The CPF's steadfast support served as a beacon, guiding my efforts as I navigated the uncharted terrain of remote engagement.

Planning the Presentation. My workshop's composition emerged as the culmination of meticulous efforts, weaving foundational cybersecurity principles with the intricate tapestry of my research findings. The workshop assumed a tripartite structure, deftly designed to engage and educate. The initial segment orchestrated an introduction to cybersecurity's essence, outlined through slides titled Agenda, Definitions, Cyberspace History, Current and Emerging Cyber Trends, Why Cybersecurity Matters to YOU, and Cybersecurity Best Practices (Slides 1 - 11).

These carefully crafted slides established a vital foundation, easing the uninitiated into the realm of cybersecurity while seamlessly paving the way for deeper insights.



Agenda: Part 2

- The Colonial Pipeline Attack
- The JBS US Meatpacking Facility Attack
- The SolarWinds Data Breach
- 3 Case Studies, Shared Implications
- Cyberspace and Democracy
- Women in Cybersecurity and Democracy
- Leaders in International Cybersecurity
- Looking Forward
- Conclusion

3

Definitions: Part 1

- **Cyberspace:** The interconnected digital realm where information is stored, transmitted, and accessed through computer networks, encompassing websites, social media platforms, online databases, and communication systems
- **Democracy:** A system of government in which power is vested in the people, who exercise it directly or through elected representatives, ensuring political equality, participation, and protection of individual rights
- **Cybersecurity:** The practice of protecting computers, servers, networks, and digital information from unauthorized access, use, disclosure, disruption, or destruction, ensuring the confidentiality, integrity, and availability of digital systems
- **Critical Infrastructure:** The physical and virtual systems, networks, and assets that are vital for the functioning of a society, economy, or nation-state
- **Malware:** Short for malicious software, malware refers to any software or code designed to harm, exploit, or gain unauthorized access to computer systems or networks

4

Definitions: Part 2

- **Data Breach:** An incident where unauthorized individuals gain access to sensitive or confidential data, typically stored in databases or computer systems, resulting in potential exposure or compromise of personal or organizational information
- **Phishing:** A type of cyber attack where attackers impersonate a trustworthy entity, such as a well-known company or organization, to trick individuals into revealing sensitive information like usernames, passwords, or credit card details
- **Social Engineering:** A technique used by attackers to manipulate or deceive individuals into divulging sensitive information or performing certain actions that may compromise security
- **Disinformation:** False or misleading information spread deliberately with the intention to deceive, manipulate public opinion, or undermine trust in democratic institutions, often propagated through social media and online channels
- **Digital Rights:** The fundamental rights and freedoms of individuals in cyberspace, including the right to privacy, freedom of expression, access to information, and protection against online censorship or surveillance

5

Brief History of Cyberspace

- **1960s:** Development of the Advanced Research Projects Agency Network (ARPANET), a precursor to the internet, by the U.S. Department of Defense
- **1990s:** Commercialization of the internet and the introduction of the World Wide Web, leading to a surge in online communities and e-commerce
- **Early 2000s:** Rise of social media platforms like Facebook and Twitter, transforming cyberspace into a hub for social interaction

6

Brief History of Cyberspace

- **Growing concerns about cybersecurity and privacy** emerged as cyber attacks and data breaches become increasingly prevalent; governments begin considering and creating national cybersecurity measures to protect networks and users from evolving cyber threats

- **Today:** There is ongoing evolution with emerging technologies, such as Artificial Intelligence, blockchain, and the Internet of Things (IoT), shaping the present and future of cyberspace. Cyberattacks continue to pose significant challenges, requiring constant vigilance

7

The Current Threat Landscape

- From 2011 to 2021, the number of internet users has grown from 2.1 billion to **4.9 billion**
- According to SonicWall's 2022 Cyber Threat Report, there were **623.2 million global ransomware attacks** in 2021, representing a 105% increase since 2020
- As of 2023, the most prevalent cyberattacks are:

1) Malware	6) Code Injection Attacks
2) Denial of Service (DoS) Attacks	7) Supply Chain Attacks
3) Phishing	8) Insider Threats
4) Spoofing	9) DNS Tunneling
5) Identity-Based Attacks	10) IoT-Based Attacks

8

Why Cybersecurity Matters to YOU

- **Preventing Fraud:** Strong cybersecurity measures prevent identity theft, keeping your online identity secure and reducing the risk of **identity theft**
- **Protecting Your Digital Possessions:** Cybersecurity is essential for safeguarding your digital belongings, such as important files, creative works, and valuable information, from unauthorized access or theft
- **Respecting Your Privacy:** Effective cybersecurity ensures that your online activities, messages, and personal data remain private, shielding them from unauthorized spying or intrusion
- **Building Trust in Online Services:** Cybersecurity is crucial for establishing trust in digital platforms like online shopping, banking, and government services, **creating a secure, dependable, and thriving online environment for everyone to enjoy**

9

Top 5 Cybersecurity Best Practises

1) **Strong Passwords:** Use unique, complex passwords for each online account: remember to update passwords at least once every few months to maintain security
2) **Multi-Factor Authentication (MFA):** Enable MFA whenever available, adding an extra layer of protection by requiring multiple forms of verification, such as a push notification or a unique code being sent to your phone
3) **Regular Software Updates:** Keep your operating systems, applications, and antivirus software up to date with the latest security patches and fixes
4) **Phishing Awareness:** Be cautious of suspicious emails, messages, or websites that attempt to trick you into revealing personal information. Verify the authenticity of requests before providing any sensitive data
5) **Data Backup:** Regularly back up your important files and data to an external storage device or a cloud-based service

10

The subsequent phase unfurled my research's quintessence from the first Laidlaw summer, encapsulated in slides titled The Colonial Pipeline Attack, the JBS US Meatpacking Facility Attack, the SolarWinds Data Breach, and 3 Case Studies: Shared Implications (Slides 12 – 16). Distilling intricate research into concise, accessible narratives was an exhilarating yet demanding endeavour, necessitating the distillation of a comprehensive 20-page report into succinct, impactful paragraphs.

The Colonial Pipeline Attack

- The CP is the **largest refined oil pipeline system** in America
- On April 29th, 2021, hackers gained access to the digital pipeline system due to a **single compromised password**
- The breach was noticed by an employee on May 7th after a **ransom note** demanding **cryptocurrency** appeared on a computer screen. The pipeline was shut down within an hour
- On May 8th, Colonial announced it would pay the 4.4 million USD ransom, but operations would take a few days to restore
- This led to **nationwide consumer panic and gas prices rising**
- President Biden made an announcement lifting all limits on amounts of domestic gas transportation to lower gas prices and calm the public
- In the aftermath of the attack, it was reported that around **100 gigabytes of employee data were stolen**

12

The JBS US Meatpacking Facility Attack

- JBS SA is one of the four **largest meat companies in the world**
- On May 30th, workers in JBS factories across the world got a **ransom note** on their devices, demanding **cryptocurrency** payment in exchange for control of various beef and pork slaughterhouses in America, Canada, and Australia
- The hackers did not damage equipment but warned they **could damage delicate systems** if the ransom would not be paid promptly
- JBS shut down all slaughterhouse, meatpacking, and shipping systems, leading to the **number of cattle slaughtered in America dropping by 22% for a week**, and the **price of American beef rising around 1%**
- On June 9th, a JBS spokesperson stated that JBS would pay the 11 million USD ransom to get back system control
- There were no reports of data being stolen

13

The SolarWinds Data Breach

- The SolarWinds data breach **targeted** vast parts of the American government and private sector. The attack began as early as March 2020, with hacker actions being traced back to as early as September 2019
- Malicious code was **distributed through a routine software update** package of Orion, a popular network-monitoring application
- Nearly **18,000 users** installed the malicious update, including actors in **key federal agencies**, from the Department of Homeland Security to the the Department of Energy, the agency that oversees America's nuclear weapons arsenal
- The **Russian** group CozyBear was suspected to be behind the attack, with the likely motive being **cyberespionage** for the Russian government
- While affected actors did their best to restore protection by reupdating systems and changing passwords, experts are **still uncertain** about whether the hackers have some **access to systems through digital backdoors**

14

3 Case Studies, Shared Implications

- **All three cases demonstrate the cyberattack's versatility and damage to trust in the government**
- In the CP case, rising oil prices created **national anxiety**, and questions about **government competence** in protecting Americans from cyberattacks
- Similarly, in the JBS case, the meat industry realized its **vulnerability** to cyberattacks and had to consider how the government could **confront the attackers responsible**
- Finally, the government itself was one of the targets of the SolarWinds breach, leading to **direct questions about the government's cybersecurity posture**, and plans to improve cybersecurity
- In all three cases, Americans witnessed their government's lackluster cybersecurity approach and questioned whether they could trust their government to protect them from **future cyberattacks** and **mitigate other rising security threats**

15

The culmination unveiled the insights garnered during my tenure as a CPF scholar, encapsulated through slides christened Women in Cybersecurity and Democracy, Leaders in International Cybersecurity: CPF, Looking Forward: Solutions, YOUR Involvement, and Conclusion (Slides 17 - 23). The LiA program's guiding principle of engaging with communities and serving underrepresented groups served as a guiding force. One of my original motivations for travelling to San Francisco was rooted in the prospect of engaging with a new community abroad. However, my project's inherent nature within the realm of cyberspace led me to an invaluable realization: confining 'community' within the boundaries of physical spaces is a limitation. Not only does it counter the essence of my work, but it also contradicts the contemporary landscape, where technology increasingly mediates both personal and professional interactions.

In this digital age, the parameters of “community” have expanded, presenting a fertile ground for innovation in outreach and engagement. As I delved into crafting my workshop, I was acutely

aware of the transformative potential that technology holds for bridging geographical divides. The realization that meaningful community engagement transcends physical limitations became a cornerstone of my journey. While in-person interactions possess unique value, the digital realm unveils an expansive canvas for connectivity, enabling individuals from diverse corners of the world to congregate, share insights, and collaborate seamlessly.

Indeed, a fundamental requirement of the LiA project was to ensure a lasting impact that extended beyond the duration of my trip. While I don't lay claim to my workshop being a world-altering force, I take pride in its accomplishments in several modest yet meaningful ways. First and foremost, the workshop found an eager audience among the CPF's newly inaugurated "CyberCorps" volunteers – individuals at the threshold of their journeys in advancing Cyber Peace. I hold the hope that my workshop left a lasting impression on them, influencing their future endeavours with the core messages I conveyed. The level of engagement exhibited by the audience, marked by their active questioning throughout the presentation, strongly indicates the effectiveness of this dissemination.

Moreover, my workshop presentation, complete script, and a recording of the session found a home within the CPF's repository – a testament to our shared commitment. As part of the organization's ongoing training and educational resources, these materials were incorporated into a shared folder, accessible to both current and incoming experts and volunteers. The realization of this dissemination strategy, as I had originally envisioned and promised, brought about a sense of gratification and further fueled my dedication to advancing the cause of sustainable improvements in cyberpolitics.

In this context, my workshop found its perfect platform, seamlessly uniting a global audience of like-minded individuals passionate about the intersections of cybersecurity and democracy. This virtual congregation catalyzed the very partnership that bound me with the CPF, underscoring the potential and relevance of technology as an enabler for community engagement. Notably, this alignment extends beyond the virtual realm; it echoes the philosophy and practices of both the Laidlaw Foundation and the CPF.

Similarly, both institutions share a commitment to diversity – a commitment that reverberates through the design of my workshop and its thematic exploration of the nexus between women, cybersecurity, and democracy. The CPF stands as an embodiment of this dedication, explicitly prioritizing diversity through workshops tailored for women and a steadfast acknowledgement of the integral role women play in cybersecurity. This resonant harmony between my journey and the principles of the Laidlaw Foundation and the CPF elevates the significance of my insights, amplifying their impact within a broader narrative of community empowerment.

Within this evolving narrative, a poignant realization kindled the inclusion of a slide spotlighting the intricate synergy of women, cybersecurity, and democracy. As a woman navigating these domains, I found myself situated at the juncture of underrepresented groups, exemplifying the very essence of the LiA's commitment to diversity. This segment extended further, illuminating the pivotal role of CPF’s incoming volunteers, the esteemed CyberCorps, in propelling the organization’s mission forward. The resonant alignment of these insights with my journey

introduced a layer of profundity, bridging my personal leadership trajectory with the broader narrative of community connections and empowerment.

Women in Cybersecurity and Democracy

CyberPeace

LAIDLAW FOUNDATION

- **Women in Cybersecurity:** Despite making up around ½ of the world's population, women represent **only 24%** of cybersecurity professionals. Promoting cybersecurity training for women enhances their ability to protect personal information and contribute diverse perspectives to cybersecurity measures

- **Women in Digital Democracies: Women are also valuable democratic participants.** Cybersecurity training empowers women to participate fully in democratic processes, safeguard their rights, and express their opinions without fear of cyberattacks undermining them. Women strengthen the overall security and resilience of democratic systems

17

International Cyberspace Leaders

CyberPeace

LAIDLAW FOUNDATION

CyberPeace is an award-winning global civil society organization, think tank of cybersecurity and policy experts with the vision of pioneering CyberPeace Initiatives to build collective resilience against cyber crimes & global threats of cyber warfare

CyberPeace Corps (CPC) is a volunteer-driven, crowdsourcing initiative which works on the concept that 'security is everyone's responsibility.' Through the crowdsourcing model of the CyberPeace Corps, the idea of a truly global Internet that is trustworthy, secure, inclusive, and sustainable, is furthered by bringing together a large talent pool of individuals & organisations. Thereby sourcing enormous array of skills, resources, and expertise contributing to the urgent cause of raising awareness about cybercrimes and promoting peace and trust in cyberspace

18

Looking Forward: Solutions

- Improving cybersecurity and public trust in government requires governments to undergo a **paradigm shift** in its understanding of cybersecurity; the world still approaches cybersecurity as a slow, growing threat that awaits culmination, but cybersecurity presents **dynamic, ongoing, ground-level challenges**
- Governmental **bureaucracy** must be adjusted for increased **cross-departmental communication**
- Governments should be upfront about previous weaknesses with the public and **collaborate with the private sector** for improvement
- The government should also take on a **sterner geopolitical approach** to malicious actors behind cyberattacks. **Public cyberattack attribution**, paired with **sanctions and diplomacy** would serve as effective deterrents

19

YOUR Involvement

- **Regardless of your technical background or expertise, your contribution is invaluable.** At the CyberPeace, we believe that every individual has a role to play in ensuring cyber peace, regardless of their technical proficiency. Whether you're a cybersecurity expert or someone with limited technical knowledge, your involvement is crucial!
- As a volunteer, there are many activities you may get involved with:

1) **Awareness and Education:** Volunteers educate people about cybersecurity and online safety to promote a culture of responsible digital behavior
2) **Incident Response and Support:** Volunteers help identify and report cybercrimes, offering support to victims and facilitating timely intervention and resolution
3) **Advocacy and Policy Development:** Volunteers advocate for robust cybersecurity policies and international cooperation to ensure a safer and more peaceful cyberspace
4) **Research & Innovation:** Volunteers to connect with high level research networks established in CyberPeace Centers of Excellence.

20

Conclusion

Embrace the opportunity to **join the CyberPeace Corps** and actively contribute to our noble mission of promoting **Peace, Trust, and Stability** in the vast realm of Cyberspace. By becoming a member of our dedicated community, you will play an integral role in safeguarding digital harmony and fostering a secure online environment for all

To embark on this remarkable journey, we invite you to register and be part of the **CyberPeace Corps** movement

Take the first step towards creating a safer cyber landscape by visiting our official website at https://www.cyberpeacecorps.in

By registering with us, you will unlock a wealth of resources, connect with like-minded individuals, and gain access to impactful initiatives that aim to reshape the future of cybersecurity

21

Any Questions?

22

As the slides found their harmonious rhythm, so did the script that would underpin the presentation. The workshop, aptly titled "Cyber x Democracy," emerged as a holistic exploration, artfully bridging foundational cybersecurity principles with contemporary challenges to democratic ideals. However, a pivotal juncture awaited – the engagement of an audience receptive to the workshop's insights. The original plan to engage an in-person cohort necessitated adaptation; guided by the CPF, a decision emerged to present the workshop to new CPF "CyberCorps" volunteers. This cohort, diverse in their academic backgrounds yet united by a shared commitment to CPF's ethos, offered a receptive canvas.

The Unforeseen Technological Challenge to My Digital Destination. As the presentation's designated hour loomed, an unexpected technological hurdle emerged, underscoring the significance of adaptability and resilience in the leadership journey. A consistent challenge surfaced throughout my tenure – the mercurial nature of the WiFi at my lodging. It oscillated between periods of seamless functionality and frustrating lapses. The presentation was scheduled

for July 16th at 4:30 AM San Francisco time, which corresponded to 5:00 PM New Delhi time, forming an optimal bridge between time zones to thoughtfully accommodate a global audience. Armed with preparation and brimming anticipation, I stood poised to surmount the final hurdle – the delivery of the workshop.

Dawn on July 16th unveiled an unforeseen conundrum. Eager to commence my preparation, I found myself entangled in a WiFi vortex, my attempts to connect rendered futile. The anticipated hour of the workshop passed, the unrelenting WiFi woes casting a shadow of frustration. A subsequent inquiry unveiled an exasperating reality – the WiFi's early morning upgrade routine rendered it inoperable. This unforeseen twist threatened to derail the culmination of weeks of diligent effort. Yet, amidst the frustration, the indomitable spirit of resilience surged forth. Swift communication with the CPF mentor followed, revealing a gracious willingness to reschedule the presentation.

June 19th heralded a new dawn, both metaphorically and literally. On this day, as I prepared to embark on my journey back to Toronto, the alarm declared 4 AM, a resolute affirmation of my commitment. The WiFi conundrum was circumvented with a determined walk to the nearby 24/7 Dunkin' Donuts, affording a stable connection. Against this backdrop, the first notes of the "Cyber x Democracy" workshop resonated. The attendance, a heartening mix of twenty engaged participants, validated the journey's worth.

A Reflective Conclusion. Contemplating this experiential expedition unveils a synthesis of leadership, adaptability, and the ability to discern opportunities within challenges. The LiA voyage bore testimony to the symbiotic relationship between resilience and determination, underpinning

the essence of leadership. The juncture where expectation met reality, marked by the pivot from in-person to remote engagement, symbolized a valuable lesson – while life may chart its course unpredictably, the resultant journey abounds with untold prospects.

The six weeks in South San Francisco unfolded as an intricate dance, an interplay between expectations and the unanticipated. While my vision was attuned to immersive in-person interactions, the reality beckoned me to forge connections amidst the virtual realm. The journey revealed an inner reservoir of adaptability and optimism, qualities that thrived and surged amidst professional challenges. As eloquently articulated by my University of Toronto counsellor, Shraddha Prasad, “We thrive better with support, but we do not thrive without it.” The support I initially envisaged drawing upon was traditionally rooted in in-person interactions. However, the unfolding of my LiA journey unveiled a unique and fortuitous twist – while the expected in-person support transformed into a remote embrace, I found myself amply fortified by the virtual network provided by the CPF. This shift in the form of support not only reaffirmed the essence of Shraddha's insight but also underscored the adaptive and resilient nature of effective leadership in a dynamic world. This experience attested to my capacity to navigate professional headwinds while harnessing the power of resilience and positivity.

Surveying the culmination of my efforts, I stand proud of the tapestry woven within the environs of South San Francisco. The “Cyber x Democracy” workshop emerges as an accomplishment – a successful convergence of cybersecurity and democratic ideals that resonated with an eager audience. The importance of this experience has stoked a burgeoning fire within me, a desire to delve deeper into the realm of cyberpolitics. My collaboration with the CPF, the creation of the

workshop, and the culminating presentation coalesce to underline the significance of nurturing cybersecurity awareness within democratic discourse. As I bid goodbye to sunny California, windy South Francisco, and dear South San Francisco, the Industrial City, I carry with me a treasury of insights and lessons, bound by an unwavering commitment to continue my contributions to the burgeoning realms of cyberspace, both in the tangible world and across digital horizons.