

A first look at Cybersecurity from an Indigenous Perspective: A case study from Ecuador

Alexander Kopsch
University of Bristol

Etsa Franklin Salvio Sharupi Tapuy
Universidad San Francisco de Quito

Kopo M. Rampokapane
University of Bristol

1 Introduction

According to the World Bank, around 74% of individuals worldwide are using the internet [16]. Technological innovations, such as Starlink, which uses a satellite network to provide high-speed internet, have made it possible for the internet to reach even remote areas [13]. However, the types of risks experienced by users in remote regions, such as Indigenous Peoples, are still poorly understood [2, 15]. Studies show that Indigenous Peoples – referring to those individuals and groups who are descendants of the original populations of a country [5] – face unique cybersecurity issues compared to mainstream users, afforded by the features of security mechanisms that are designed to protect them. Rennie et al. [11] has found that western-centric assumptions inherent to the privacy frameworks of online platforms and mobile devices are at odds with the sociocultural dynamics of Aboriginal Australians, creating privacy risks. In Latin America, indigenous leaders avoid using communication technologies due to a history of state-based surveillance [6]. Without understanding the types of cyber-insecurities introduced by the internet in regions where indigenous users live, we risk designing technologies that introduce rather than alleviate problems, potentially exacerbating inequalities and marginalisation.

Previous studies show that there is little research in Usable Security and Privacy (USP) looking at Indigenous Peoples [12]. Only a handful of articles exist, e.g., on First Nations in Canada [3, 4, 10, 14], Aboriginals in Australia [7, 11], and indigenous people in Namibia [8, 9]. We need more research to investigate the cyber-threats indigenous people experience

and what might make them feel more secure, to design more inclusive protective mechanisms and interventions.

To address this gap, we explored three research questions through a case study in Ecuador: (1) What does cybersecurity mean to indigenous people in Ecuador? (2) Which cyber-threats do indigenous people in Ecuador experience? (3) How do indigenous people in Ecuador recommend addressing these cyber-threats?

2 Methodology

Recruitment: We used purposive sampling and snowball recruitment [1] to reach out to indigenous people interested in talking to us about their experiences of digital technologies and threats. We used the networks of a local assistant (listed as second author) and also reached out to indigenous leaders, asking them to distribute recruitment flyers in their communities. The eligibility of the participants was determined via a screening section in the participant consent form, as well as verbally at the start of the interviews and workshops.

Workshop and Interview Guides: The interview and workshop guides (see Appendix 5.1 and 5.2) were informed by a previous scoping trip to the country. During the scoping trip, we asked indigenous leaders and members of indigenous communities about the cybersecurity topics and issues they would be most interested in exploring. When collecting the data for this study, we were careful not to project our own notions of cybersecurity onto the participants, as the goal was to understand their meanings of and perspectives on cybersecurity. We designed the workshops as open spaces for discussion and framed the questions in the terms used by the participants during the preceding interviews.

Data Collection and Analysis: We conducted 16 semi-structured interviews with people who self-identified as indigenous and held 4 workshops in indigenous communities in Ecuador, which were attended by 73 people. We asked the

participants about their opinions, experiences, and feelings of cybersecurity and cyber-threats. All workshops took place in-person, as well as the majority of the interviews. However, a few interviews were done via Microsoft Teams due to a nation-wide strike happening at the time of data collection. Both interviews and workshops were held in Spanish. The initial findings presented here come from a first round of thematic analysis.

Ethical Considerations: Conducting the study in an ethical manner was a priority for us. This study was reviewed and approved by the Ethics Committee of the Engineering Department at the University of Bristol. We obtained informed consent from the participants through a participant information sheet and a consent form. Because we could not expect all participants to be able to read and write in Spanish, we also confirmed consent verbally. We also consulted with indigenous leaders regarding cultural protocols to follow and asked our local assistant to advise on ethical matters and discussed ongoing findings with him to avoid possible misinterpretations. After the interviews, we sent the anonymised transcripts back to the participants for review. We chose to reciprocate the time and stories the participants shared with us through community meals, as well as through the development of guidelines based on their ideas (currently in progress). This type of reciprocity was a result of the discussions we had with indigenous leaders and our local assistant.

3 Results

Security as being able to trust. When we asked participants what digital security meant to them, a common response was to be able to trust strangers. A participant mentioned that,

“So, that’s security, in other words, not responding to unknown numbers. It’s the security we put [on the workshop sheet]. Not being afraid of false communications. Not being afraid, because it also happened to me that there are some publications, which offer work to you, but first they ask you for money and later say ‘deposit this much money and then we will send you the location you need to go to.’ ”
[Group 3, Workshop 3].

Other participants also mentioned that security for them included the ability to trust online information.

Online Harms: Phishing. The most common online threat that participants experienced was phishing via social media, e.g., *“we also put attempts of threats, sometimes messages on WhatsApp, messages on Facebook, all that”* [Group 1, Workshop 4], leading to the loss of money and personal data.

Physical Harms: Kidnappings. A common physical threat participants mentioned was *“kidnappings through social media”* [Group 2, Workshop 2].

Concerns about Social and Cultural Impact. A particularly often mentioned theme that came up was the social and cultural impact of digital technologies on indigenous culture, especially the internet. Participants said that,

“now, with arrival of the internet, this contact and relations – it’s a threat. It leaves his [the child’s] traditional wisdom, his Waorani cosmovision, it is left to the side.” [P18]

Indigenous ways of relating to nature, such as in the case of this Waorani participant, are under threat with the arrival of the internet. Participants frequently compared the internet to colonisation, eroding indigenous worldviews and values.

Interest in Capacity Building. When we asked the participants how they would like to address the digital threats and concerns mentioned, a common response was to organise workshops about cybersecurity. There was a particular interest in having a *collaboration* between cybersecurity experts and indigenous leaders to work out the needs of the community and deliver a workshop to raise awareness about digital threats. There was a desire to have more *control* in governing the internet, including having *internal regulations* that would align with indigenous forms of community governance.

4 Implications and Future Work

The initial findings of our work have important implications for USP, because the cybersecurity needs and experiences of Indigenous Peoples are still poorly understood. Indigenous people in Ecuador understood security as the ability to trust others and the information found online. This was due to a common experience of threats of phishing and kidnappings when using social media. Another particular concern was the impact of the internet on indigenous cultures. Through the erosion of relationships with nature, the internet acts like a new form of colonisation. The conclusion we can draw from these points is that digital technologies, especially the internet, brings negative outside influences that create a feeling of insecurity for indigenous people in Ecuador.

One way of addressing the cyber-insecurity felt and experienced by indigenous people could be through capacity building workshops. The main emphasis of the participants was to have more control over technology use in a way that is aligned with their ways of living.

Future work could work out how to design these types of culturally-tailored capacity building workshops. Another important line of work could be to work together with indigenous people to establish guidelines for internet regulation.

References

- [1] H. Russell Bernard. *Research Methods in Anthropology: Qualitative and Quantitative Approaches*. Rowman & Littlefield, Lanham, Maryland, sixth edition, 2018.
- [2] Ayako A. Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How WEIRD is usable privacy and security research? In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 3241–3258, 2024. <https://www.usenix.org/system/files/usenixsecurity24-hasegawa.pdf>.
- [3] Laura Huey and Lorna Ferguson. Another digital divide: Cybersecurity in indigenous communities. *Sociology Publications*, 2022. <https://ir.lib.uwo.ca/sociologypub/55>.
- [4] Farrah Huntinghawk, Candace Richard, Sarah Plosker, and Gautam Srivastava. Expanding cybersecurity knowledge through an indigenous lens: A first look. In *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–4, 2020. <https://doi.org/10.1109/CCECE47787.2020.9255753>.
- [5] Kathleen Lowrey and Pauline Turner Strong. Two indigenous americas. In *The SAGE Handbook of Social Anthropology*, pages 465–486. SAGE Publications Ltd, London, United Kingdom, 2012.
- [6] Pascal Lupien. Indigenous movements, collective action, and social media: New opportunities or new threats? *Social Media + Society*, 6(2):1–11, 2020. <https://doi.org/10.1177/2056305120926487>.
- [7] Gavin Morris, Rachel A Groom, Emma Louise Schuberger, Sarah Dowden-Parker, Miriam-Rose Ungunmerr-Baumann, Aaron McTaggart, and Bronwyn Carlson. “i want to video it, so people will respect me”: Nauiyu community, digital platforms and trauma. *Media International Australia*, 183(1):139–157, 2022. <https://doi.org/10.1177/1329878X211038005>.
- [8] Gabriel Tuhafeni Nhinda and Fungai Bhunu Shava. Towards the use of participatory methods in cybersecurity research in rural africa: A grassroots approach. In *3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pages 1–7, 2021. <https://doi.org/10.1109/IMITEC52926.2021.9714649>.
- [9] Gabriel Tuhafeni Nhinda and Fungai Bhunu Shava. Cybersecurity practices of rural underserved communities in africa: A case study from northern namibia. In *International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, pages 1–7, 2023. <https://doi.org/10.1109/icABCD59051.2023.10220449>.
- [10] Sarah Plosker and Gautam Srivastava. Cybersecurity education in rural indigenous canada. In *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6, 2021. <https://doi.org/10.1109/CCECE53047.2021.9569147>.
- [11] Ellie Rennie, Tyson Yunkaporta, and Indigo Holcombe-James. Privacy versus relatedness: Managing device use in australia’s remote aboriginal communities. *International Journal of Communication*, 12:1291–1309, 2018. <https://ijoc.org/index.php/ijoc/article/view/7051>.
- [12] Shruti Sannon and Andrea Forte. Privacy research with marginalized groups: What we know, what’s needed, and what’s next. *Proceedings of the ACM on Human-Computer Interaction*, pages 455:1–455:33, 2022. <https://doi.org/10.1145/3555556>.
- [13] Starlink. Starlink map, 2026. <https://starlink.com/map>.
- [14] Kayleigh Tanner, Sarah Plosker, and Gautam Srivastava. A reflection on cybersecurity indigenous educational experiences. In *IEEE International Conference on Big Data (BigData)*, pages 4819–4825, 2023. <https://doi.org/10.1109/BigData59044.2023.10386338>.
- [15] Aditya Vashistha, Richard Anderson, and Shirang Mare. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS)*, pages 1–14, 2018. <https://doi.org/10.1145/3209811.3209818>.
- [16] World Bank. Individuals using the internet (% of population), 2026. <https://data.worldbank.org/indicator/IT.NET.USER.ZS>.

5 Appendix

5.1 Workshop Guide (English version)

13:00–13:15: Welcome (15 mins)

Welcome and introduction to the workshop.

13:15–13:30: Presentation: Research on cybersecurity capacity building in Ecuador (15 min)

I present the results of my research on cybersecurity capacity building in Ecuador. This is a work in progress.

13:30–13:50: **Workshop question 1:** What does digital security mean to you? (20 mins)

Workshop participants work in groups to reflect on what digital security means to them.

13:50–14:10 **Workshop question 2:** What risks does digital security aim to prevent? (20 mins)

The groups discuss the risks that digital security aims to prevent, in relation to those that they and/or others in their communities experience.

14:10–14:40: **Workshop question 3:** How can these risks be prevented in indigenous communities? (30 mins)

Building on the ideas from questions 1 and 2, the groups will present ideas on how these risks can be prevented in indigenous communities.

14:40–15:00: Presentation of conclusions (20 mins)

The groups briefly present their plans or ideas to one another.

5.2 Interview Guide (English Version)

Table 1: Interview Guide (English)

Questions	Themes
Thank you for accepting to do this interview with me. Today, we will talk about technologies and digital threats and your culture. There are no right or wrong answers. All I am interested in is your experiences and viewpoints. <Verify consent, any questions, and begin the recording>	Start
1. Could you tell me who you are and what you do? Verify: Indigenous Community? Indigenous Nationality? [Build rapport by asking another follow-up question, based on whatever comes up]	Warm-up
2. How has the internet impacted your community? Follow-up: Threats and dangers to communities [if nothing, provide some examples from other participants]	Impact
3. What has been the impact of the internet on your culture? Deeper: What does culture mean to you? Can you explain what cosmovision means?	Culture
4. What kind of threats or dangers have you experienced online? Follow-up: Who? When? What?	Threats
5. How do you react to these kinds of threats? What do you do? Guide: Talking to family members, using certain technologies, etc.	Reactions
6. I know this may be a bit speculative, but how do you think the threats mentioned could be addressed for indigenous communities?	Protection
Thank you very much for participating in this interview. Your input is important in shaping this research. Before we finish, I have one last question: 7. Is there something I should have asked, but didn't?	End