EPIC2022 ETHNOGRAPHIC PRAXIS IN INDUSTRY CONFERENCE PROCEEDINGS

Cybersecurity in the Icelandic Multiverse

MEGHAN MCGRATH, *IBM*

> "Security in cyber space should be one of the main cornerstones of economic prosperity in Iceland, resting on a foundation of sophisticated awareness of security issues and legislation."
>
> —Icelandic National Cyber Security Strategy

Iceland makes a unique case study for cybersecurity in that it ranks among the world's most connected nations as well as among the highest for social trust. Data that elsewhere is considered sensitive is shared freely by individuals and businesses. As a result, technology built in places with different cybersecurity paradigms may not function as intended in an Icelandic context. This work, undertaken with undergraduate and graduate students from the University of Iceland's Computer Science department, employed ethnographic methods in a classroom setting to build cybersecurity awareness with a special emphasis on culture and to engage the broader community in conversations about security from local perspectives. This work lends itself well to multinational enterprise settings, where systems may be built with the expectation of security behaviors that do not actually reflect local or regional norms. Of special interest to the EPIC community may also be this case study's exploration of ethnography as a defensive grassroots tool in cyberwarfare. In the so-called "wild west" of cybercrime where so often those with the most resources and imperialist drive win the day, we suggest that ethnographic skills are an undertapped resource that communities can employ in active striving for resilience.

Keywords: cybersecurity, cyberwarfare, ethnography, anticipatory ethnography, futures thinking, storytelling

BACKGROUND

"þetta reddast," widely regarded as the national slogan of Iceland, roughly translates to, "it'll all work out just fine." A 2017 report by Oxford University (Bada and Weisser 2017), commissioned by the Icelandic government, noted that this trust that "it will all work out" could make government initiatives surprisingly effective in Iceland—and at the same time opened up the country to acute security risks. A prevailing belief that attackers will ignore Icelandic targets is common in industry and is reflected in the lack of security positions available. All of this is compounded by the fact that for much of Iceland's history, national defense has been provided by other nation states and geographic isolation has rendered most threats relatively harmless. The shared memory of a generations-long peacetime is strong.

What happens then, when one of the world's most trusting nation states (Vilhelmsdóttir 2020) is also one of the most connected? In addition to ranking among the most trusting countries in the world, Iceland is also one of the highest in terms of internet saturation, with 99% of businesses and individuals online (BBC News, 2018).

Such connectedness marks a significant change for this country with no geographic neighbors. As Milton Mueller notes in his "Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace," the internet that we know today, with its roots in Web 1.0 idealism, was architected to fundamentally ignore nation state boundaries (Mueller, 2017). The result is deep layers of mutual access between geographic regions that may not have been connected before. And while the connection goes both ways, it is rarely true that both

parties are equal in terms of resources, computing power, cyber skill, and willingness to attack. What this means for Iceland is that its "digital borders" are far more permeable than its geographic borders have historically been. In other words, the ocean isn't enough to keep other nation states out anymore.

Although the above premise was a major driver in the case study presented here, it was thrown into high relief in March, 2022, with the invasion of Kiev, Ukraine, through a mixture of on-the-ground and cyber attacks. As Russian forces hinted at further-reaching cyberwarfare against Ukrainian allies, the security posture of NATO's smallest and most undefended state was urgently felt. This is discussed in more detail in the "Reflections" section of this paper.

This project took the form of a semester course in the University of Iceland's Computer Science department, attended by undergraduate and graduate students hailing from a variety of fields. The work was sponsored by the Icelandic Fulbright Commission as part of a National Science Foundation Fulbright grant in Critical Cyberinfrastructure. It was inspired in part by the work of the previous year's grant recipient, whose students connected local disinterest in cybersecurity with the concept of "þetta reddast" (echoing the 2017 Oxford report). This work began with a hypothesis that ethnographic methodologies could contribute to a more robust Icelandic cybersecurity posture by: building up a general awareness of cybersecurity, by focusing the entire topic on the students' home turf and the sites of their everyday lives and work, and by focusing on local, emic storytelling of cybersecurity realities to inform the secure management and consumption of data.

PROJECT OVERVIEW

Initial Context-Setting

The germination of this project began during my work leading design research for IBM Pervasive Encryption for the z14 mainframe, where my team saw firsthand how profoundly human cybersecurity can be. Spending time with clients across the world in the sites where they worked, we encountered a range of ways security incidents were anticipated or escalated, saw critical information conveyed through informal modes like stories or humor, and experienced the impacts of regional norms on overall cybersecurity expectations and how a product was actually used.

This work is in conversation with others at the quietly bustling intersection of cybersecurity and ethnography. Susan Squires and Molly Shade's 2015 EPIC case study, asking: "People, the Weak Link in Cyber-security: Can Ethnography Bridge the Gap?" is one especially resonant example; in the accompanying article, the authors note that "users and their actions do not exist in a vacuum, and their perceptions and subsequent behaviors regarding security risk are shaped by a vast array of beliefs, social relations and workplace practices." (Squires and Shade, 2015) Much has been explored regarding the way privacy threats are recognized and defended against by communities, and these echo our lens here of communities-as-actors within a security landscape. (Ahmad, et al., 2022; Cordio, et al., 2012; Dourish and Anderson, 2006) Laura McNamara, working with Los Alamos and Sandia National Laboratories in the United States, has also extensively studied the impact of geopolitical shifts on security posture and in-house security knowledge (McNamara, 2016), which is relevant to our examination of resilience amid shifting international cyber threats.

Methodologically, there are a wealth of resources (within EPIC and otherwise) exploring how ethnographic fieldwork can complement speculative fiction, futures design, and the creation of science-fictional artifacts as a mode of storytelling (Anderson and McGonigal, 2004; Attari et al, 2021; Cuciurean-Zapan, 2017; Greenmail and Smith, 2006). Underlying these we find the anticipatory anthropology work of Robert Textor and collaborators such as Margaret Mead (Textor 1995; Mead and Textor, 2005).

The "Cybersecurity Capacity Review for the Republic of Iceland" assembled by the Global Cyber Security Capacity Centre at the University of Oxford and described above (Bada and Weisser 2017), provided important background on the cybersecurity landscape of Iceland. For additional context, conversations with both Dr. Matthias Book, department head of Computer Science at the University of Iceland, and with the previous recipient of the NSF-Fulbright grant, Dr. Gregory Falco (Johns Hopkins University), were invaluable.

Dr. Falco's findings have been covered in a publicly-available presentation that can be found (as of September 2022) on the Fulbright Iceland YouTube channel (Falco, 2021). Key points from that work can be summed up as follows:

- Iceland's high level of social trust has had many positive effects but also can result in a more compromised cybersecurity position
- Actual cyberattacks that do affect national infrastructure tend to be underreported in the Icelandic press, further contributing to the low public awareness of cyber risk
- Young technologists who are interested in growing their skills in this area do not have a lot of outlets, whether at the university or in employment after graduation (this is tied to the belief of many organizations that "we do not have security problems")

At present, Iceland's version of the national identification number, the *kennitala*, is publicly available on a national database along with identifying information such as address, phone number, and birthdate. Although identity theft in Iceland is rare, exploiting these public databases is not difficult. In one recording made by Dr. Falco's class, a student called one of Iceland's largest telecom companies using the kennitala of a Laki Power employee, and was able to obtain critical private information quickly and without any apparent issue.

Dr. Falco also notes in his presentation that a significant number of his students "had never heard of security before" taking the course, as there are few opportunities to do so, and that low cybersecurity awareness in industry could translate to fewer opportunities for the students to grow those skills as they go on to become the builders and maintainers of the country's technological infrastructure (Falco, 2021).

The follow-on course described in this paper, titled "Ethnographic Approaches to Cybersecurity," was informed by Dr. Falco's experience, by the aforementioned 2017 report, and other supporting research. It was not sufficient to teach the students new cybersecurity skills; they needed to be able to tell a compelling story within their communities to justify their interest and any further work they might do. It was also important that these perspectives be defined by local realities: what holds true for cybersecurity in Silicon Valley, where social trust is comparably lower and information such as passwords and national identity numbers are assumed secrets, may not function as intended in an Icelandic context. Security solutions that would genuinely protect the community should ideally be built with the community's perspectives, values, and practices in mind.

The underlying question at this stage was: could ethnography be used to help Icelandic technologists tell their own, locally-informed stories about security, as opposed to having those stories told to them? And could those stories engage the community in broader cybersecurity conversations?

The goal of this project was to take the previous grantee's class and compare the students' security awareness after technological coursework to a curriculum centered on ethnographic approaches. Success, in this case, would be the students defining in their own words what security could look like in Iceland in the future, in the places that were most meaningful to them. Achieving a level of community engagement was also a secondary goal of the project. Therefore, success would be measured by the content of the final class projects (which would center on that community-oriented storytelling), as well as through benchmark surveys before, during, and after the course to gauge/track learning.

The course was designed in three parts:

1. Establishing a shared vocabulary
2. Fieldwork
3. Storytelling

Course content was subject to iteration as feedback was received from the students (discussed below), but maintained its core structure throughout the semester.

Establishing a Shared Vocabulary

As described above, the previous grantee found that students did not tend to have a strong knowledge of cybersecurity concepts nor a drive to learn them; they did not see the purpose in a society that felt inherently safe. This was reflected in the broader industry contexts as well, with hospital and energy companies indicating to researchers that security was not a significant concern (Falco, 2021).

At the beginning of the course described in this case study, students widely reported an unfamiliarity with cybersecurity concepts, with only one student stating that they were "very familiar" with the topic. This was addressed in part by introducing basic cybersecurity concepts into the curriculum, which students had a chance to apply each week in homework assignments, and was reinforced through storytelling with our guest speakers. In the latter instance, invited speakers (professionals working in cybersecurity today) were invited first to share stories of their experiences and then to answer questions from students and in some cases offer feedback on current work.

One memorable guest speaker described a social engineering attack in which the owner of a high-value Instagram account was bombarded with unpaid pizza orders until they surrendered their handle (this individual was located in Manhattan, within delivery range of seemingly endless pizza shops.) In a class that focused on helping students identify non-technical security attacks, the "pizza attack" story became a recurring reference point, one that the students could attach certain concepts to and remember them. In fact, throughout the rest of the semester and into the final projects, students were referencing not just the pizza attack but other stories from the guest speakers' visits as well.

What Worked Well

Running through assignments together in first half of the course and then applying that knowledge in the second worked well, providing a needed introduction as well as an embodied experience working with these skills and processes.

The course was also set up such that small increments of work were completed each week, and the students' final projects were largely finished by the end of the semester, giving them a chance to use the time to critically assess and iterate on their own work rather than creating it from scratch. Students were also asked to turn in their final projects two weeks before the end of the class in order to receive feedback, reflect, and make one more iteration of their work before the grading period. Students were also welcome to resubmit work at any time during the semester for re-grading. While these details are largely pedagogical, they were also intended to reinforce core concepts of cybersecurity and information management: that it is more useful to think of the work as constantly improving than to think of it as finished, that it is crucial to reserve time for sensemaking and reflection, and that big changes can be made through a series of small, manageable actions.

Areas to Improve

One of the most interesting outcomes of the work came from sharing a model used by my team for years to reframe user experiences in security contexts: user and "anti-user" personas[1]. The "anti-user" persona developed out of a need to articulate not just the needs, motivations, actions, and tools, etc., of a user in the system, but also someone not anticipated at all by the system's architecture, be it an outside attacker, malicious insider, or the inadvertent error of someone accidentally given the wrong level of access. Students quickly understood the concept of an "anti-user" persona, but their first passes tended to be more generalized and less nuanced than their user personas. While the user personas often had quirks (a love of Dolly Parton, for example, or a pet chihuahua), the anti-users tended to be described with a small set of tropes, and given no more specific a role than "hacker" (in some cases, not even a name.) In Iceland as in the United States and elsewhere, the classic stock image for "hacker" (and indeed, often for cybersecurity in general) is a faceless individual in a hooded sweatshirt, sitting before an open laptop in the blue light of a windowless room. This image haunted the first drafts of anti-user personas, whose love of sweatshirts was only rivaled by their love of money, and who lived and worked most frequently from their home basement[2]. We pivoted by bringing ethical hackers into the classroom to share stories, answer questions, and in one case comment on a MURAL board of the students' project topics, giving additional details and questions to consider. This was followed by a lecture on what makes a financially-motivated criminal syndicate differ in tools, goals, and attack vectors from a state sponsored group, or a FIG-motivated (Fun, Ideology, or Grudge) individual attacker, as well as which types of attackers or attack groups are most likely to target which industries. Having learned about "anti-users" at a deeper level of specificity, students were asked to assess in future work what types of attackers and attacks were most likely for the sites they were exploring.

Even with the changes made, there is room to improve the experience of how students imagine the "anti-user" user experience and to more systematically consider which processes will slow down or better enable those "anti-users". Particularly if a lessening of pandemic risk allowed for more in-person interaction with guest visitors to the classroom, having face

time with white, grey, or black hat hackers[3] during a social engineering engagement or other piece of security work might enrich the students' understanding of the "anti-user" experience and how it fits into the functioning of technical systems that they may in their future careers be responsible for protecting.

In addition to the above, one particular session needed to be made virtual due to the pandemic, and this is one of the missed opportunities that could be worth trying in future iterations of the course. Originally, the students were scheduled to participate in a hands-on activity where they would breach the perimeter of an "office" and collect vulnerable data, such as a password prominently written near a laptop and sensitive documents in the trash bin. The intent was to give the class a visceral experience of information vulnerability, one they could remember in future contexts where they might be building technology solutions and could consider security requirements beyond immediate technical ones like encryption. While not possible during the week scheduled due to pandemic restrictions, this might be a worthwhile experience to provide, reinforcing an embodied understanding that systems can be broken into, in order to hold more informed conversations about how to protect those systems.

FIELDWORK

The approach taken in this course was to first expose students to different security ethnography techniques through a mixture of lectures, videos, speakers, podcasts, and case studies. Then, after selecting a field site of interest to them, each student carried out fieldwork at those places over the course of a semester, taking notes and often diagrams or pictures, and recording their own observations.

Sites

First, each student chose a local site; they were encouraged to chose a place that was interesting and engaging to them, but also relatively easy to access (so as to limit obstacles to their getting coursework done on time.) The idea was for them to, at the end of the day, tell a story about their community. Projects were mostly centered in Reykjavík, but a few remote students were elsewhere in Iceland and one Swiss student focused on the Swiss-Iceland expat tax experience.

Students were required to spend time in their chosen sites in person. Although by this time the pandemic risks in Iceland were comparatively low, as a safety precaution the students were able to chose an online "location" and spend time in those online spaces if they preferred or to conduct an auto-ethnography on their home offices[4]. Other chosen sites included the local pool, a hospital cafeteria, the Icelandic Patent Office, a horse paddock where horses were microchipped, a local technology services company, the domestic airport, the international airport, a gym requiring biometric entry, the National Library, and more.

Student Fieldwork Requirements

For the fieldwork component of this course, students were asked to spend time in/with their chosen sites. They were given templates to note behavior and draw maps that included spatial data from the larger environment and interconnected systems. Almost every student included photographs in their field notes as well, with the intent to capture security-sensitive

aspects of the sites that they hoped to learn more about through their observations during the semester. (fig. 1-2)

Figure 1. Section of student notes from visit to Icelandic patent office. Photograph © Ragna Dúa Þórsdóttir, used with permission.

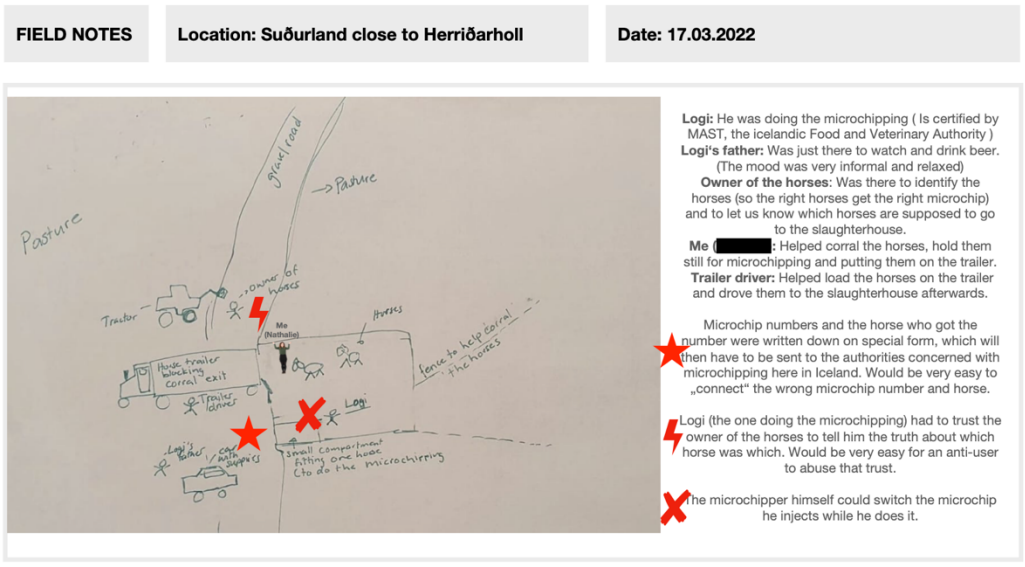

Figure 2. Section of student notes from visit to horse paddock for microchipping. (Original names redacted) Photograph © Nathalie Monika Moser, used with permission.

One key way that security ethnographic work differs from what has historically been practiced in ethnography is its special emphasis on shortcuts, workarounds, human error, and any occasion where a disconnect appears between the worldview assumed by a system and the worldview experienced and/or enacted by a human user. Oftentimes, in this context, understanding how a system works is not nearly as interesting or useful as understanding how it doesn't. Students built up an understanding of the security landscape in their chosen site, considered how those elements worked together, and identified points in the system with the potential to lead to unintended consequences—and particularly, to security incidents. The ethnographic skills of observing complex human-influenced systems, synthesizing data, deriving critical insights, and telling a story about that were all important here.

All ethnographic work undertaken in this course was framed as the beginning of future conversations, with room for expansion and further understanding. Sensemaking activities were accompanied by a documentation of assumptions and outstanding questions. The goal was for students to have a piece of work that they could conceivably bring to an employer or graduate advisor to say, "here is what I have discovered and observed so far; I would like to do *x* work in order to further an understanding of *y*, and this is what would need to happen to accomplish that."

Overall, the students' fieldwork experiences helped to underscore that they as technologists were empowered to observe and identify the security elements within a system (that this could be part of their process), as well as to share those observations with their peers. Compared to the initial example sites that were used by all the students when learning the introductory material, the sites students chose individually seemed to elicit a stronger enthusiasm and sense of ownership, with students adding additional visits and questions to their research unprompted. Situating their experiences within known sites also seemed to add a level of concreteness to the sometimes nebulous and difficult-to-visualize topic of cybersecurity—the floating blue fields of 1's and 0's in cybersecurity journalism replaced by a poorly-secured router in the local gym that is easier both to envision and to address.

STORYTELLING

After initial sensemaking based on their ethnographic observations, the students worked on telling stories about how cybersecurity might develop in these local places via a methodology called Artifacts from the Future (which Lindley, et al. describe as "intentional design fictions").

Students collected signals of change related to the sites they were studying, and assessed those signals according to which were most likely to persist over the next ten years and which were most likely to impact the everyday realities of their site. They then explored the implications of key signals using the Futures Wheel tool, (Glenn, 1972) (fig. 3) and generated a list of questions and ideas related to that space. From this, they imagined and created an object that might exist in the security landscape of Iceland in 2032, along with stories about the item's purpose and use. These stories took the form of chat conversations (using 2032 slang), breaking news articles, minutes from a professional organization, straightforward narrative, and other formats. They were peppered with details from the students' field work and their perspectives on how those elements of the site experience would develop in the forthcoming ten years.

Figure 3. Futures Wheel example template, partially filled. This is a modification of Jerome Glenn's 1972 Futures Wheel method, and uses a ring of user/stakeholders to frame the changes from specific user perspectives. In the case of this class, "anti-user" personas were also included here. © Meghan McGrath.

Together, the class created a multifaceted and thoughtful picture of Iceland's cybersecurity future, with objects that could be picked up, handled, and considered. These objects presented *multiple* versions of the future, whether hopeful or dystopian or somewhere in between, and formed a sort of multiverse of Icelandic security futures when taken together. This framing is especially useful at putting participants in an empowered position of deciding which of the many futures proposed they would like to work towards or away from—rather than simply waiting to inherit whichever single future arrives for them. For a security culture that had been expressing throughout 2021 a sentiment of "it will be fine,"

but which suddenly found itself in the potential attack line of a global superpower, this conversation found an unexpected relevance and usefulness for the community.

The students' multiverse was on display in an exhibit that is detailed below in the "Deliverables" section. It engaged in a public conversation far beyond the initial classroom constraints, and generated conversations in some cases at a national level.

What Worked Well

Using the Artifacts from the Future technique proved useful not just in helping students apply the insights of their field work into concrete, sharable forms, but also to engage the broader community with the work the students were doing. The class developed a set of imaginative and engaging artifacts, and throughout the month of their exhibit I received messages from visitors expressing interest and appreciation. In the world of security, this is no small feat.

Security professionals, like user researchers and industry ethnographers, are familiar with the concept that in order to do the job well, one must sometimes be the "canary in the coal mine," the bringer of bad news who alerts the community that something is amiss. This can be a difficult position. Unexpected issues require unexpected work and changes that organizations may or may not have budgeted for. Resistance to the bad news is more common in many places than a willingness to fix the vulnerability. Storytelling, then, is crucial for *making the security work happen*. A compelling story can open doors and resources that will help a system be built smarter, stronger, and protect its users' data more successfully. A story that is *memorable* will follow audience members outside of the conference room and engage them longer, invite them to brainstorm possible solutions longer, and will be easier to share through word-of-mouth with other colleagues who may have resources or knowledge that would prove essential to the project.

Areas to Improve

There is room to improve this process in the stages between when students explore the implications of key changes using the Futures Wheel and when they first begin to brainstorm their object. In some cases, students struggled to imagine what objects might characterize daily life of 2032, rather than an object that could exist in 2022 but didn't. There are a number of practices in Futures Design today that might be experimented with to frame this transition more clearly and in an easier-to-follow way.

OUTCOMES

Exhibit

The class ended with a public exhibit designed to provoke discussion in the broader community. The exhibit, named "Spoiler Alert" by the class and subtitled, "What Cybersecurity in 2032 Might Look, Feel, and Smell Like", ran through April, 2022, in the Gróska Innovation Center of the University of Iceland. This site was chosen for its proximity to downtown Reykjavík, its public accessibility, and the fact that the building was shared with or adjacent to many of the country's biggest technology companies. Walking

distance to Parliament, the site was also frequented by policymakers and diplomats throughout the capitol.

Figure 4. Entrance to "Spoiler Alert" exhibit, April 2022. Photograph © Meghan McGrath.

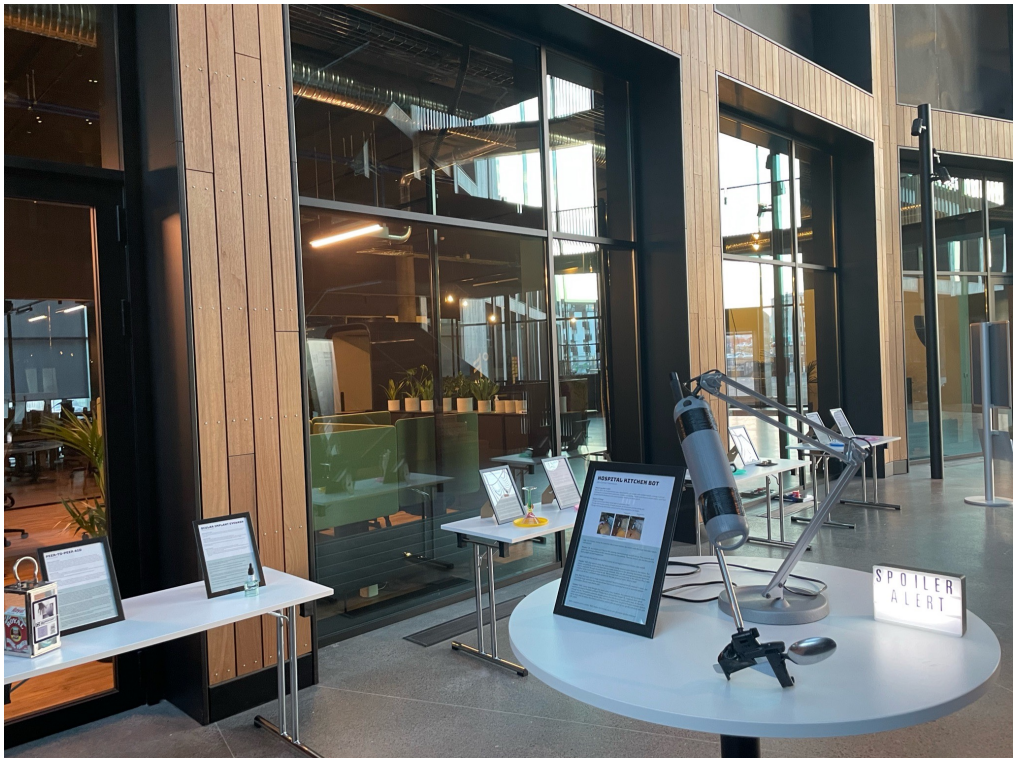

Figure 5. Student projects in "Spoiler Alert" exhibit. Artifact on the right is a movable "hospital kitchen bot" intended to portion and spoon out cafeteria food in a hospital. Student story describes how kitchen bot was not designed with security in mind, allowing attackers to access the hospital network with which it is connected. Photograph © Meghan McGrath.

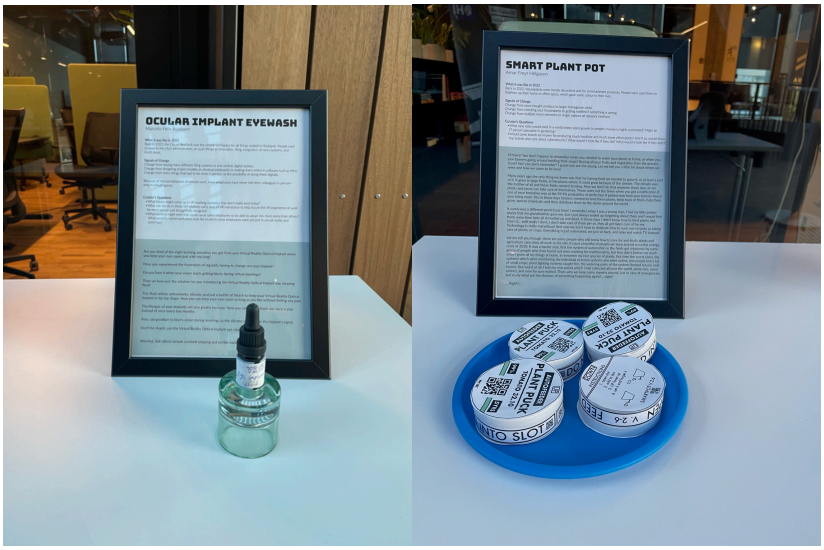

Figure 6. Student projects in "Spoiler Alert" exhibit. Artifact on the left is "ocular implant eyewash," intended to accompany a VR-enabled artificial eye. Artifacts on the right are smart plant cartridges for a personal plant with third party software. In this story, the plant has just been transported to a work site, compromising the owner's company's intranet. Photograph © Meghan McGrath.

Figure 7. Student projects in "Spoiler Alert" exhibit. Artifact on the left is a designer-branded adversarial scent, intended to give the wearer control over how their biometric scent signature was read in public places. Artifact on the right is a "service bots on the premises" sign, created by a warehouse employee for a world in which organizations with voice- and facial-recognition-enabled service bots would be obligated to notify anyone on the premises that they were opting in to having their data collected. Photograph © Meghan McGrath.

The exhibit featured table displays of the objects made by each student, along with the stories/scenarios they had written and a series of prompt questions for the viewer. Rather than booking a conference room, the displays were placed along a wide but busy corridor with heavy foot traffic. They received visitors from the building's tour groups and patrons of the local gym in addition to the expected neighboring technology companies (such as Alvotech, a biologics firm, and CCP Games, creator of Eve Online.) We were also honored by the attendance of Icelandic writer Bergur Ebbi, whose recent collection of essays on culture and technology entitled *Screenshot* had informed this coursework and accompanying research (Ebbi, 2020). Noted folklorist and ethnologist Valdimar Hafstein visited the exhibit and encouraged the University of Iceland's folklore students to visit as well. One emeritus professor of medicine wrote days later to say he enjoyed the work and was still thinking about it.

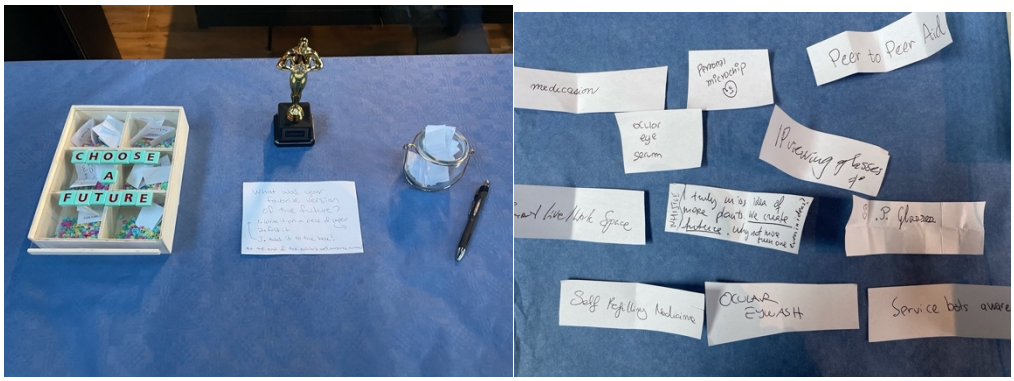

Figure 8. Voting area in "Spoiler Alert" exhibit. Visitors were invited to vote on whichever version of the future was most compelling to them, or introduced the most interesting questions. Photograph © Meghan McGrath.

Members of the National Security Council also attended or heard about the exhibit, and this led to follow-up engagements and conversations about the human aspects of cybersecurity that might impact Iceland's security posture, including conversations about the forthcoming National Security Policy that was in the process of being re-written.

What Worked Well

Showcasing the work of the students added a layer of meaning to their experience with security and ethnography during the semester, and many brought friends, family, and significant others to see the work. Since the goal of this project from the start had been tied to fostering community resilience through a connection to cybersecurity knowledge, this was an ideal outcome.

Areas to Improve

The availability of our exhibit site was somewhat limited and complicated to obtain permissions for; though we succeeded, we had no choice but to launch the exhibit in the height of the Easter holidays when many had left early for vacations or were attending confirmation parties (which are extremely popular in Reykjavík during that time.)

Fortunately, the exhibit space was reserved for the entire month, and in fact did experience a wave of new interest when students, faculty, and tech employees began returning to the building after the holidays ended.

Reusable Templates

The other key deliverable besides the exhibit was a set of reusable templates that could be shared with potential employers or graduate advisors. The idea was for students to leave the class with a portfolio of work showing their process and how they imagined security from an Icelandic lens. In this sense, it was meant to support emic storytelling—crucial in a security landscape where so much of technology is consumed in the form of imports and a better understanding of Iceland-specific security requirements is much needed.

In the class itself, the students had already "reused" the reusable templates when we applied them a second time in the student project section of the class, so students had experience interacting with these documents *as* templates in order to help them repeat what they had previously done.

If one intent of the exhibit was to create a memorable experience in which the students could see and remember themselves as cybersecurity experts for the community, in a sense, then the reusable templates might help to accompany them on that journey after the class to whatever extent and whatever context they chose to take it.

What Worked Well

Student adapted well to the templates, and each section seemed "manageable" enough that almost every student finished every assignment—astonishing in an Icelandic context where education is free and college courses can be taken and dropped or failed without significant cost or and with comparatively lower stigma than in the United States.

Areas to Improve

Although the students' final portfolios were turned in early for feedback and a final iteration, in a future version of this course it would be interesting to have guest tech professionals provide feedback and hold conversations with students about the work. This would give the students further experience with the nuances of applied security ethnography and what forms that can take in industry or public settings, as well as connecting them with professionals already doing similar work today.

REFLECTION

This case study had promising results in the case of the class itself, with students who had experienced the ethnographic approach reporting a significantly increased security consciousness—including regular conversations with friends and colleagues about what security means to them. In the sense of engaging the larger community in conversation about security, the approach of hosting an exhibit of student work also worked well.

It should be stated in reflection of the case study presented here, that it is in many ways a project informed and impacted by crisis and events without precedent in the near past. The course's curriculum was modified at times in response to local pandemic levels, and student fieldwork was undertaken with health protocols in mind. What does it mean for a student

doing contextual inquiry for the first time to be aware of their research participant's sniffle as a potential health risk, or to simply not be able to see the mouths of the people around them? Crisis too informed the class's methodological trajectory in some ways, as our Artifacts from the Future activity was seeing a surge in industry practice due to a prevalent sense of generally uncertain conditions (sometimes described as VUCA or "Volatile, Uncertain, Complex, and Ambiguous"). The disruptive nature and profound strangeness of a global pandemic renewed interest in futures thinking among governments and private organizations around the world, echoed in our 2021 EPIC theme of "Anticipation" (English-Lueck, et al., 2021). Finally, the invasion of Ukraine in early 2022 reframed much of the class's perception of the course material and brought that course material into conversations with national policymakers and with staff of the Icelandic Prime Minister.

The attack happened halfway through the winter semester, just two weeks after the class had had a lecture on e-governance in Estonia. We were exploring ways that culture can inform technical infrastructure, and Estonia's long shared cultural memories of invasion were a strong driver behind the desire to create a government that has no geographic borders—essentially, one that can can persist even if its physical land were to be invaded. Our discussion of cyber warfare and kinetic invasion was still fresh on the students' minds in the wake of the Kiev attacks, and reframed the work of this course in significant and unexpected ways.

What began as an exercise in emically building up structural security hygiene within the sociological context of "everything will be fine" took on extra valences as a way for that community to bolster its grassroots defense in the event of a large-scale cyberattack. This is in part because while expensive tools and methods can be used to increase a country's security posture, the human element should not be overstated (fig. 8). While financially-motivated attacks may favor ransomware or infected code, politically-motivated attacks overwhelmingly hinge on social engineering and exploiting poor security awareness. Growing the community's familiarity with non-technical attacks can be critical in achieving resilience in not just infrastructure but many everyday technologies and services.

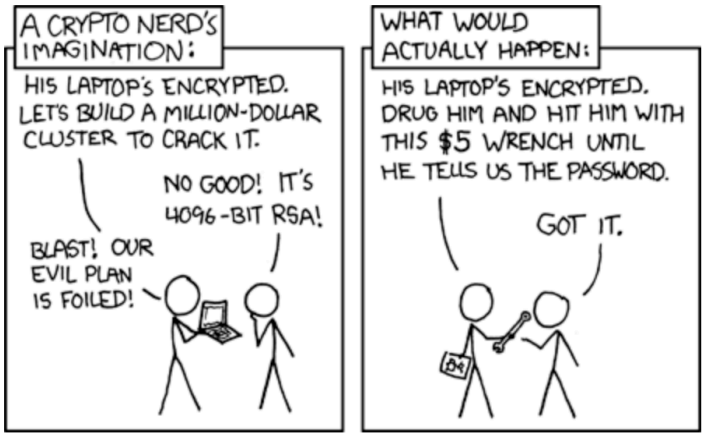

Fig. 9. "Cybersecurity" by Randall Munroe is licensed under CC BY-NC 2.5.

Ethnographic approaches to local sites, as seen in the student work shared here, centers attention on ways that human behaviors and processes can differ from what a technical system's architecture expects. This is especially useful in countries where technology is consumed as an import, a set of tools that were built and imagined elsewhere. In Iceland, those doing cybersecurity assessments are often foreign consultants brought in from other countries. The need for stories told from a local perspective may be essential in helping energy companies, hospitals, social services and more continue to function safely into the future.

Icelandic systems not only have specific needs tied to the way the *kennitala* is used, but also need to make use of special characters like the thorn (þ) or eth (ð) that can break systems not developed with those characters' existence in mind. Due to the relatively smaller footprint of the Icelandic language (spoken by 0.004% of the world's population, as opposed to the roughly 17% that speak English), the Icelandic internet is also significantly less catalogued, and so less searchable, than the Anglophone internet (Rögnvaldsson 2012). This can create moments of vulnerability or resilience, depending how a system is designed and the assumptions about the world built into it.

Beyond this Icelandic case study, there is a need for more culturally alert cybersecurity work to provide resilience for communities and the infrastructure that supports them. While this project represents one instance of using anticipatory ethnographic approaches to grow cybersecurity skills and support broader conversations, there is much more work left to be done and more cybersecurity contexts (beyond the Silicon Valley model and other well-known models, and beyond even the high-trust, high-networked model of Iceland) to be brought into the discussion. For large-scale enterprises that handle user data located in, coming from, and traversing across a massively diverse range of cultural contexts, a lack of understanding of regional expectations around security and privacy remains a blind spot.

In a hyperconnected world, cyberwarfare and vulnerability may in many ways be a matter of brute strength—of who has the greatest computing resources, the greatest processing power. What does it mean for a community to be a fellow node in that web, with the full breadth of its citizen data, its hospital and healthcare networks, its energy infrastructure, water systems, governance, etc. living in online spaces? What might be at risk, and what does resilience look like? Although this case study does not claim to have an answer to that question, it suggests that further inquiry into the strategic use of ethnographic tools towards community resilience is justified.

Additional questions for our community include: how do we ensure that all users are receiving a baseline of security coverage when designing for a product with global reach and multicultural consumption patterns? How might we usefully measure and track that? How might we measure the implications of *not* doing that well? How can we be smarter about imagining the shifts in environmental influence (be they geopolitical, climate-driven, technological, etc., or even, as in our earlier example, tied to the availability of a critical mass of pizza parlors) that will morph these patterns in ways unlike what we see today? How can local knowledge holders inform all of the above conversations? Further examination of these questions could help communities better leverage ethnographically-informed security work in the service of sensemaking with regards to their own security posture, as well as actionable strategies towards resilient and sustainable future approaches.

Meghan McGrath is the Future Demands Lead for IBM Systems. She led the design and ethnography work on IBM Pervasive Encryption, which work has been featured in Fast Company and in a HBS case study. She represented IBM at the 3Ai Institute from 2019-2020. Connect at meghanmcgrath@us.ibm

NOTES

Many thanks to the Háskóli Íslands students of HBV604M, the faculty (especially the guidance and support of Matthias Book), and to the Fulbright Commission Iceland and National Science Foundation for funding this work.

1. It is worth noting that the term "anti-user" carries a level of imprecision in today's industry use, ranging from the intentionally/unintentionally malicious user (as described by this case study) to the wholly absent user who is *out of scope* for a project being designed. For my team and for the purposes of this class, "anti-user" has been sufficient to connote the former user—one who is present in a system that was not designed for their presence.

2. What makes this trope so misleading and so problematic a mental model for computer science students is its persistent suggestion that malicious attackers can fit into a single hoodie. In today's cyber landscape, security incidents are far more likely to be perpetrated by sophisticated syndicate organizations or state actors with enterprise-grade resources and computing power than by an individual working alone. (Klimburg, 2017; Buchanan, 2020; Verizon 2021)

3. The following summary from *Wired* will work for our purposes: "White hats disclose vulnerabilities to software vendors so they can be fixed; black hats use or sell them to other criminals to conduct crimes; gray hats disclose or sell them to governments to be used for hacks against adversaries and criminal suspects." (https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/ Accessed Sept. 2, 2022)

4. Students looking at online spaces were particularly directed towards the field of digital anthropology/ethnography for examples of what this practice has looked like from the 1990s up until today.

REFERENCES CITED

Ahmad, Norita, et al. "A Cybersecurity Educated Community." *IEEE Transactions on Emerging Topics in Computing*, Vol. 10, No. 3, p. 1456-1463. 2022.

Anderson, Ken, and Jane McGonigal. "Place storming: performing new technologies in context." Third Nordic Conference on Human-Computer Interaction (NordiCHI) Proceedings. Association for Computing Machinery, 2004.

Attari, S., Scull, C. and Harandi, M. "Leveraging Speculative Design to Re-Imagine Product Roadmaps." Ethnographic Praxis in Industry Conference Proceedings, 2021.

Bada, Maria, and Carolin Weisser. "Cybersecurity Capacity Review for the Republic of Iceland." Global Cyber Security Capacity Centre at the University of Oxford, 2017. Digital.

"Iceland profile." *BBC News*, October 3, 2018. Accessed September 2, 2022. https://www.bbc.com/news/world-europe-17386737

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, 2020. Print.

Cordio, Sherley, et al. "Identifying Community Factors of Privacy." International Conference on Privacy, Security, Risk and Trust and International Conference on Social Computing, 2012.

Cuciurean-Zapan, M. "Situated: Reconsidering Context in the Creation and Interpretation of Design Fictions." Ethnographic Praxis in Industry Conference Proceedings, 2017. https://www.epicpeople.org/situated-reconsidering-context-design-fictions/

Dourish, Paul and Ken Anderson. "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena." *Human-Computer Interaction*, Vol. 21, No. 3, p. 319–342. 2006.

Ebbi, Bergur. *Screenshot*. Mál og Menning, 2020. Print.

English-Lueck, Jan, et al. "Little Dramas Everywhere: Using Ethnography to Anticipate the Future." Ethnographic Praxis in Industry Conference, 2021. https://www.epicpeople.org/little-dramas-everywhere/

Falco, Gregory. 2021. "A Cybersecurity Clinic for Critical Infrastructure." *Fulbright Iceland* YouTube channel, May 10. Accessed September 2, 2022. https://www.youtube.com/watch?v=YTJMfaXZLuY

Glenn, Jerome C. "Futurizing Teaching vs Futures Course," *Social Science Record*. Syracuse University, Vol. 9, No. 3 Spring 1972.

Greenman, A., and Scott Smith. "Embed: Mapping the Future of Work and Play: A Case for 'Embedding' Non-Ethnographers in the Field." Ethnographic Praxis in Industry Conference Proceedings, 2006.

Klimburg, Alexander. *The Darkening Web*. Prentice Hall, 2017. Print.

Lindley, Joseph, et al. "Operationalizing Design Fiction with Anticipatory Ethnography," Ethnographic Praxis in Industry Proceedings, 2015.

McNamara, Laura A. "Interdisciplinary Research in the National Laboratories." *Anthropologists in the Securityscape: Ethics, Practice, and Professional Identity*, edited by Robert Albro, p. 87-101. Routledge, 2016. Print.

Mead Margaret and Robert B Textor. *The World Ahead : An Anthropologist Anticipates the Future*. New York: Berghahn Books, 2005. Print.

Mueller, Milton. *Will the Internet Fragment?* Polity Press, 2017. Print.

Noyes, Dorothy. *Humble Theory: Folklore's Grasp on Social Life*. Indiana University Press, 2016. Print.

Rögnvaldsson, Eiríkur, et al. *The Icelandic Language in the Digital Age*. Springer, 2012. Print.

Squires, Susan and Molly Shade. "People, the Weak Link in Cyber-security: Can Ethnography Bridge the Gap?" Ethnographic Praxis in Industry Conference Proceedings, 2015.

https://www.epicpeople.org/people-the-weak-link-in-cyber-security-can-ethnography-bridge-the-gap/

Textor, Robert B. "The ethnographic futures research method: An application to Thailand." *Futures*, Vol. 27, No. 4, p. 461-471. 1995.

Verizon. *Verizon 2021 Data Breach Investigations Report*. New York, NY. Verizon, 2021. Accessed September 2, 2022. https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

Vilhelmsdóttir, Sjöfn. *Political Trust in Iceland: Determinants and trends, 1983 to 2018*. PhD diss. University of Iceland, 2020.

Wash, Rick. "Folk Models of Home Computer Security." Sixth Symposium on Usable Privacy and Security Proccedings. Association for Computing Machinery, 2010.