A Visual Exploration of Cybersecurity Concepts

Miriam Sturdee
m.sturdee@lancaster.ac.uk
Lancaster University
UK

Lauren Thornton
l.thornton2@lancaster.ac.uk
Lancaster University
UK

Bhagya Wimasaliri
b.m.wimalasiri@sheffield.ac.uk
University of Sheffield
UK

Sameer Patil
patil@indiana.edu
Indiana University Bloomington
USA

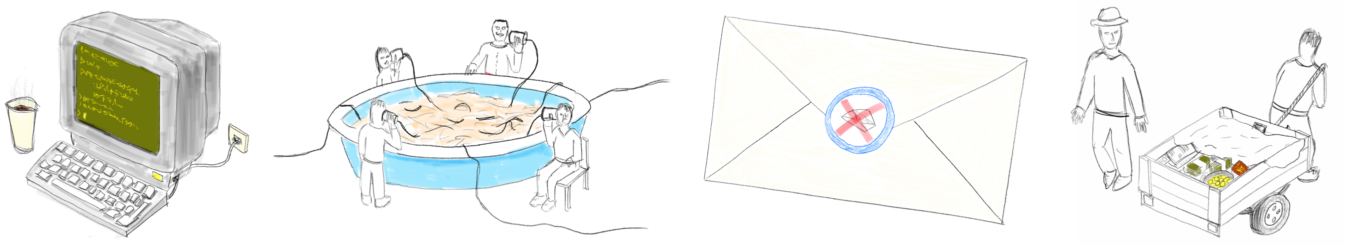

Figure 1: Example participant sketches: Left–Cybersecurity; Middle left–Privacy; Middle right–Trust; Right–Risk.

ABSTRACT

Cybersecurity-related concepts can be difficult to explain or summarise. The complexity associated with these concepts is compounded by the impact of rapid technological changes and the contextual nature of the meaning ascribed to the various themes. Since visual imagery is often employed in articulation and explanation, we conducted a study in which we asked participants to sketch their understanding of cybersecurity concepts. Based on an analysis of these sketches and subsequent discussions with participants, we make the case for the use of sketching and visuals as a tool for cybersecurity research. Our collection of sketches and icons can further serve as the seed for a visual vocabulary for cybersecurity-related interfaces and communication.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**; • **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

sketching, imagery, icons, risk, privacy, trust, cybersecurity, visualisation

C&C '21, June 22–23, 2021, Virtual Event, Italy
© 2021 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8376-9/21/06.
https://doi.org/10.1145/3450741.3465252

ACM Reference Format:
Miriam Sturdee, Lauren Thornton, Bhagya Wimasaliri, and Sameer Patil. 2021. A Visual Exploration of Cybersecurity Concepts. In *Creativity and Cognition (C&C '21), June 22–23, 2021, Virtual Event, Italy.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3450741.3465252

1 INTRODUCTION

Cybersecurity is a continually evolving and challenging interdisciplinary field. Cybersecurity deals with technology and people who are the gatekeepers to the private information connected with people's online practices. As the volume of sensitive data stored online expands, external threats to the data repositories grow, requiring users to be cautious about unwanted incursions. Cyberattacks are one of the top sources of global-scale risk [3, 55]. Yet, for the vast majority of the population, 'cybersecurity' represents an unknown. Most people are unaware of the meaning and implication of the terms we use to describe basic cybersecurity concepts. Cybersecurity and cybercrime coverage in the popular media is typically full of buzzwords and jargon unintelligible to the average person.

Although textual definitions and descriptions of terms can help facilitate understanding, reading these can be overly specific, dense, and time-consuming, limiting their utility. In contrast, visual techniques offer an effective means to deliver information at-a-glance. For instance, visuals can be applied to construct dashboards to portray results of incursions [41, 61], show icons to depict security ratings (e.g., DuckDuckGo Privacy Essentials[1]), present educational material to inform vulnerable groups such as children [63], and display data about threats such as phishing attacks [64].

It has been argued that we need to find a happy medium between complexity and visualisation by rethinking how we visualise cybersecurity and risk [23]. Yet, there are no standard techniques for

[1] https://addons.mozilla.org/en-US/firefox/addon/duckduckgo-for-firefox/

the development and use of imagery used to convey cybersecurity concepts. With the notable exceptions of a few depictions, such as the "hooded hacker" [37], that have become ingrained, there is no current consensus on cybersecurity imagery, with each application typically creating its own visuals. Moreover, stereotypical images used by the popular press neither foster a correct understanding of cybersecurity concepts nor facilitate safe online practices.

We fill this gap by studying how cybersecurity domain experts and non-experts sketch the core cybersecurity concepts of *risk*, *trust*, and *privacy*. Such sketches have the potential to translate difficult-to-articulate concepts into visual representations, map understanding of cybersecurity across people, and consolidate themes into tangible visual libraries for user education, system implementation, and research. Specifically, we address the following two research questions:

RQ1: How do experts and non-experts visualise their perceptions of core cybersecurity concepts?

RQ2: How can user-produced imagery serve as the basis for a consolidated 'visual mapping' to help users, system developers, and researchers?

Based on an analysis of participant-produced sketches and related discussions, we make the following contributions: i. demonstrating the utility of the sketching technique to surface people's understanding of cybersecurity concepts; ii. discussing the methodological utility of sketching for research in usable cybersecurity; and iii. providing a collection of expert and non-expert images as a seed for the development of a common visual vocabulary for core cybersecurity concepts.

2 RELATED WORK

Visual imagery in cybersecurity is connected to its use in the media, applications, and research and its role for surfacing end-user mental models related to cybersecurity matters.

2.1 Visuals in Cybersecurity Communication, Applications, and Education

Cybersecurity coverage in the media spans a diverse range of incidents, from leaks via social media and suspicious third party apps [10, 20] to breaches of large companies and government entities [12] to terrorist attacks and cyberwarfare [14, 29]. Such news articles are often accompanied by stereotypical images including but not limited to: binary numbers, circuits, imagined 'AI' faces, glowing screens with pale hands at a keyboard, etc. These stereotypes can be portrayed as evidence that artists and photographers have achieved a "visual standard" [18] for the coverage of cyberthreats, led by the ubiquitous hooded hacker, a basement-dwelling malevolent white male [37]. The use of these images in the press has become so staid that the Hewlett Foundation (a nonpartisan, private charitable foundation) challenged this status quo in a recent article [54] and teamed up with the open innovation platform openIdeo to put out a competitive design call for reimagining the current "sensationalized" cybersecurity imagery [47]. In comparison, our research solicits imagery from end users, rather than relying solely on the judgements of professional designers.

Visualisation in cybersecurity-related publications encompasses imagery (i.e., artistic, illustrative, and icon-based work) alongside *information visualisation* (i.e., depictions of data in the form of graphs, dashboards, etc.). The former is used largely for educational or communications purposes [40, 43, 63] as part of commercial applications where icons can indicate security ratings or inform other users of their virus protection status [30]. Between largely *informal* visual imagery and formal visualisation, we can find user-focused informational imagery used for a variety of purposes, such as conveying security and privacy ratings [61], enabling secure sign-in using pictorial passwords [1, 5], promoting the creation of safe passwords using image-based education [62], utilising 3D glyphs [35], etc. The more academic imagery in cybersecurity research is often connected to visualisations such as tables of results in papers or grids of risk analysis. Similarly, researchers have explored the design of visualisation-based dashboards for security analysts [4]. Such visualisations support security professionals in their decision making via techniques such as visual depictions of data provenance [19], visual cues for detecting malicious logins (such as for enterprise networks [50]), etc. The explorations of McKenna et al. [42] and Staheli et al. [51] provide a comprehensive background to user-centred visualisation research in cybersecurity, and a recent survey by Zhao et al. [65] maps additional examples. Hall et al. [23] suggest that we should rethink how we visualise cybersecurity and risk, rooting our investigation in historical visualisations as well as modern gamified resources. The IEEE Symposium on Visualization for Cyber Security (VizSec) is targeted toward new visual design techniques and analyses, underscoring the increasing attention visuals are receiving from cybersecurity researchers and practitioners.

2.2 Mental Models of Cybersecurity Concepts

Mental models are personal internal representations of external reality that people use to interact with the world [31]. Mental models guide user perceptions, adoption decisions, and interaction practices [60]. As such, mental models have the potential to provide insight into personal understandings of processes. Additionally, mental models can be utilised to improve cybersecurity design and communication with end users about online security [7, 8, 15, 16, 31, 45, 49]. Furthering our understanding of the mental models of end users, especially those who lack domain expertise, can improve communication efforts that are currently designed and implemented by domain experts [2]. Design based on the assumptions that users possess the correct expert mental model will not induce the desired behaviour if non-experts make choices according to some other mental models [58]. Consequently, many commercial security products suffer from usability problems, lacking necessary attention to the design of alerts and information presented to end users [27]. Research comparing experts and non-experts is especially helpful in exploring the ways in which people think about concepts in cybersecurity. Notably, Ion et al. [28] compared the practices and attitudes of experts and non-experts for tailoring security advice. With regards to mental models in particular, Kang et al. [32] compared expert and non-expert mental models of the Internet, finding that non-experts have simpler mental models. Kang et al. [32] found additional distinctions between the two user groups; those with technical knowledge are more likely to mention hackers having access to data, with others relying on reputations and branding of technology companies [32].

2.3 Visual Methods for Usable Cybersecurity

Oates et al. [45] examined metaphors, themes, symbols, and mental models from visual drawings related to privacy, finding that privacy is perceived as highly individualised. Experts are more likely to depict privacy for data and information (e.g., financial and health) in comparison to non-experts who were more likely to draw privacy in a physical context (e.g., bathroom). Friedman et al. [15] reached similar conclusions via semi-structured interviews. Ray et al. [48] combined semi-structured interviews with diagrammatical sketching to look at mental models of privacy. Oates et al. [45] and Ray et al. [48] looked only at privacy, whereas our research covers cybersecurity more broadly. Unlike our study, drawings used by Oates et al. [45] were not sketched by the participants in their study but taken from an online database of existing unstructured privacy imagery. In contrast, our visuals were sketched by the participants within a systematic study. Sketching as a method of elicitation is effective at capturing mental models and complex ideas that are hard to explain with words [6, 52, 53], enabling participants in our study a space for expression and reflection that may not be possible in words and allowing us to capture tacit knowledge and meaning [11, 21, 26, 31, 48].

People's perceptions of visuals in relation to cybersecurity are a rich source of data [30]. In contrast, sketching as an informational source remains on the outskirts of visual research in cybersecurity, despite having a persistent presence. For example, McKenna et al. [42] utilised "data sketches" of designers to inform the design of a new dashboard. Sketched perceptions of complex cybersecurity tools such as Tor have offered insight into expert and non-expert conceptualisation and demonstrated the efficacy of sketching as a method for generating information [17].

3 METHOD

We designed a study to elicit sketches regarding cybersecurity concepts from experts and non-experts. For both groups, we followed an identical protocol with two exceptions: i. experts participated in an in-person study session whereas non-experts completed the study online; and ii. experts engaged in in-person group discussion with the other expert participants and researchers after completing the individual sketching activity, while annotation and discussion regarding non-expert sketches was carried out by the first three authors of this paper. As reward for participation, experts received lunch and a £10 Amazon gift certificate and non-experts received a £5 Amazon gift certificate. The online questionnaire allowed non-experts to upload images of the sketches they produced. All study procedures were approved by Lancaster University's ethics board.

3.1 Study Protocol

Potential participants read detailed information regarding the study procedures and data handling before providing participation consent. Next, we asked for basic demographics and cybersecurity knowledge based on the literature [32]. We then provided instructions to generate sketches depicting the themes of *risk*, *privacy*, *trust*, and *cybersecurity* based on individual understanding of these concepts in regard to information technology. We informed participants that sketches could depict figures (i.e., contain recognisable objects/beings), contain artistic expression (i.e., use colour and shape to express emotion or feeling), tell a story, explain a process, use icons, or employ a combination of any of these. We instructed participants to try not to use text in the sketches unless absolutely necessary. Participants produced their sketches alone without consulting anyone else. We chose the themes of *risk*, *privacy*, and *trust* to reflect current practices and research within cybersecurity where these terms occur frequently within the literature and media discourse. Moreover, these terms are understandable to a general audience, ensuring that non-expert participants would be able to apply their understanding of the base concepts to the larger topic of cybersecurity.

3.2 Discussion of Expert Sketches

We conducted a group sketch analysis by laying all expert sketches on a large table to view as a group. Then, the expert participants generated keywords and phrases *as a team* using Post-It notes. Next, they discussed these keywords/phrases with the researchers and fellow participants and merged them where appropriate. Following the group discussion, the experts sketched specific icons to go with each keyword/phrase. In cases where there were multiple icons for a keyword, the group voted on the most appropriate image. Finally, a single icon was chosen to represent the overarching topic. The icon-generation exercise was based on the technique developed by Lewis[2] [38, 39]. The exercise was followed by a group discussion about visualisation and imagery on cybersecurity, during which the researchers took detailed notes. The insight from the analysis of the expert session in turn informed the analysis of the data generated by the non-expert participants.

3.3 Discussion of Non-Expert Sketches

The first three authors of this paper analysed the sketches collected online from non-experts. Each researcher initially annotated each image independently (similar to the technique used by Sturdee et al. [53]), generating corresponding keywords and phrases. The image annotation tagged items such as reoccurring themes, figures, animals, objects, computational devices, threat depictions, and so forth. Next, the researchers individually generated summaries of their comments on Post-It notes and placed the Post-It notes on a wall. The three researchers as a group further distilled the corresponding keywords and phrases were using affinity diagramming [24] and theme generation (similar to the method used by Ray et al. [48]). The group discussion among the three researchers resulted in the generated summaries and keywords being sorted into themes and sub-themes. The approach helped eliminate bias during the initial stages of discovery and allowed duplicate (and therefore strong or repetitive) themes emerging from the imagery to be identified and discussed. The three researchers then organised the final keywords and phrases relating to each topic until top-level categories emerged, which were further compared between topics.

[2] https://www.makaylalewis.com

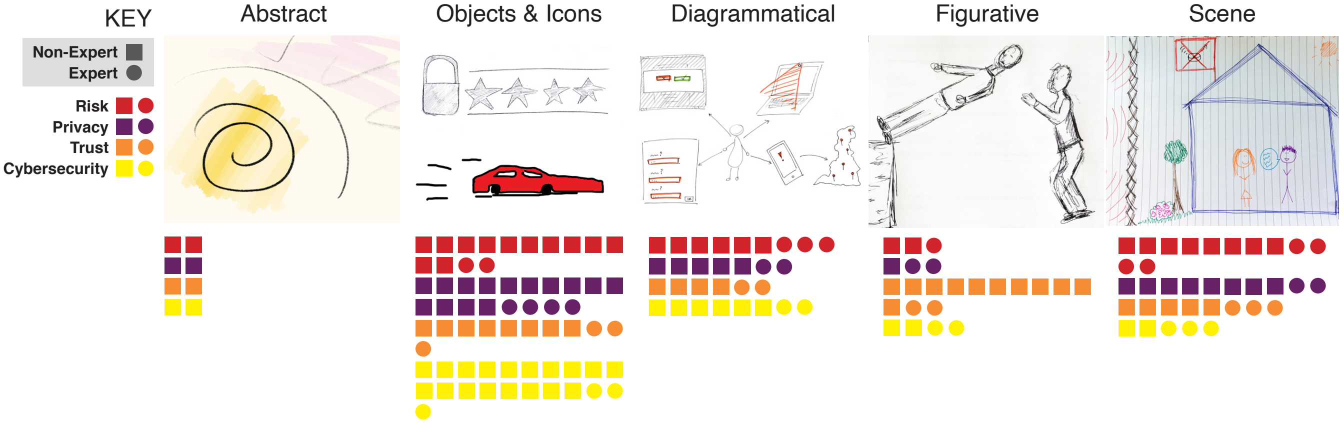

Figure 2: Distribution of all 160 sketches (120 sketches from 30 Non-experts & 40 sketches from 10 Experts) across levels of abstraction (based on Walny et al. [57]). *Abstract* refers to non-identifiable imagery; *Objects & Icons* refers to objects and icons without context or presence of people; *Diagrammatical* refers to conglomerate images containing objects, icons, arrows, or other diagram elements and basic icons representing people; *Figurative* refers human imagery with little or no context; *Scene* refers to images made up of multiple components with or without people which form a tableau or still-life.

3.4 Sample

We recruited expert and non-expert participants via Lancaster University mailing lists, social media (e.g., Facebook, Twitter), and flyers at and near Lancaster University. When soliciting non-experts, the advertisement explicitly stated that the participants must not be working in the cybersecurity field. Ten cybersecurity experts between the ages of 21 to 40 (4 women and 6 men) participated in the in-person study session. These participants were either students at the end of a two-year cybersecurity Master's program who had already secured industry employment or professors in cybersecurity at Lancaster University. Overall, the average score of the expert sample on the cybersecurity knowledge test [32] was 4.63 on 5-point scale, with 5 corresponding to most knowledgeable. In the non-expert component, 30 non-expert participants aged between 17-57 (12 women, 17 men, and 1 non-binary) completed the online sketching study. Of these, 13 studied or worked in the field of computer science, but not within cybersecurity. The other participants worked in industry and had no relationship with Lancaster University. The non-expert sample averaged 3.53 on the 5-point cybersecurity knowledge test, confirming a notably lower domain knowledge of cybersecurity compared to the expert sample.

4 FINDINGS

We addressed RQ1 by collecting 160 images drawn by 40 individuals (30 non-experts and 10 experts).[3] We first discuss the results from the study session with experts followed by an analysis of the sketches and associated participant data for experts and non-experts combined. After considering the set of images as a whole, we address RQ2 by narrowing the focus to our four primary themes (i.e., *risk*, *privacy*, *trust*, and *cybersecurity*) and exploring the implications of our findings.

4.1 In-Person Expert Session

The initial in-person expert session served to validate the data collection technique, provide initial insight, and inform approaches for the subsequent online data collection from non-experts. At the end of the icon-generation exercise (see Section 3), experts collectively chose a single icon to represent each overarching theme. As expected, these icons mapped directly to the preceding individual expert sketches, but also presented new ideas that did not initially come up (e.g., plane, ghost, government, sheep). This is notable as it shows potential for the development of imagery after initial ideation and sketching. Some icons reflected the media status-quo (e.g., hoodie, shields), whereas others linked to subsequently-collected non-expert sketches (e.g., fishing rods, handshakes indicating trusted agreements). The emergence of novel themes in the collective development of the icons suggests that group discussion is useful for augmenting and enhancing individually-produced sketches.

Discussion Points. The research team took detailed notes during the semi-structured discussion to capture thoughts on the current status of visuals and visualisation in cybersecurity and associated topics. Analysis of the group discussion suggests that the use of imagery within cybersecurity research typically involves simple tables, graphs, and network diagrams, with highly visual content seen to be an educational or informational tool for non-experts. When asked about the usefulness of the imagery generated during the sessions, expert participants were unsure about applications in "pure" research, but agreed that imagery in cybersecurity has room for improvement and felt that it would be beneficial to utilise visualisations for these purposes. Experts argued that "higher level" users of cybersecurity software/hardware rarely need visualisations or images because their training diminishes such a need. However, the group agreed that signs and symbols taken from outside the digital sphere are useful for communication. For example, experts felt that

[3] The visual dataset is available at: https://osf.io/8a4un/

Table 1: Top-level categories and counts for all themes, with overlaps between themes matched by column.

Risk	Privacy	Trust	Cybersecurity
Computational Hardware (3)	Computational Hardware (7)	Computational Hardware (6)	Computational Hardware (9)
Computational Software (8)	Computational Software (7)	Computational Software (6)	Computational Software (9)
Conceptual (14)	Conceptual (13)	Conceptual (9)	Conceptual (21)
Human (4)	Human (9)	Human (12)	Human (4)
Objects (18)	Objects (14)	Objects (10)	Objects (14)
Feelings (6)	Data (11)	Actions (6)	Data (2)
Actions: Negative (11)	The Bad Guys (6)	The Bad Guys (8)	Negative Imagery (14)
Actions: Neutral (7)	Surveillance (7)	Positive Imagery (9)	Positive Imagery (11)
Actions: Positive (1)	Home (9)	Processes: Transactions (2)	Symbols (6)
Risk Management (8)		Processes: Assessment (5)	
		Processes: Agreements (3)	

risk perception could be improved by presenting images of *physical* hazard signs to warn users of *digital* threats. We observed that one of the challenges for utilising imagery within cybersecurity is a lack of agreement on the meaning of the concept: "…one person's amber is another person's red". Experts mentioned that they usually place information within a simplistic grid for ease of comprehension rather than depicting them using more sophisticated – but accurate – visualisations because of the large number of variables used to illustrate concepts such as risk. This suggests that more accurate and complex visual representations of risk and confidence percentages may inadvertently introduce ambiguity, rather than indicate uncertainty. Similarly, experts suggested caution regarding the possibility of a false sense of security if imagery and signposting is open to interpretation and used incorrectly. In relation to the image analysis, experts overwhelmingly felt that symbols are contextual and culturally dependent and suggested that symbols for general use must be explicit in order to avoid having to explain meanings. However, experts agreed that visualisation is especially valuable in a context that requires explanations, especially when something is hard to imagine or measure.

4.2 Combined Analysis of Expert & Non-expert Sketches

We collected data from non-experts by administering the same individual sketching activities via an online questionnaire. Since there was no in-person meeting of the non-expert participants, we combined the sketches collected online with those gathered from experts and analysed them as a whole, guided by the discussion and analyses that occurred during the in-person expert session.

Levels of Abstraction. Figure 2 shows a breakdown of expert and non-expert sketches based on levels of abstraction [57]. Over a third of the responses (64/160) included depictions of objects and icons (hardware or items such as shields, padlocks, etc.), without figurative or human imagery, especially for the *cybersecurity* theme. However, *trust* appeared to rely more heavily on depictions of people (figurative) compared to the other themes. Abstract sketches were present only in the drawings of the same two participants. For the experts, distribution of levels of abstraction was fairly even across all levels of abstraction, with the exception of abstract imagery. Due to the uneven numbers participant groups, we cannot make direct comparisons, but can note general trends.

Gauging Efficacy of Current Communications. During the study, we asked participants if current communication about online safety and security in their daily lives was sufficient. Over half of the participants (23/40) felt it was not, and nearly a fourth (9/40) were unsure. Experts felt that such communication was poor or incomplete, jargon-heavy, confusing, or contradictory. Similarly, non-experts found it hard to follow the communication owing to complexity of the information and recommended solutions. Many non-experts reported seeking advice or information only after being victimised. Further, several participants felt that stronger language could be used, and the risk and consequences of the threat ought to be more explicit, perhaps with illustrative examples: "It's difficult to communicate a complex subject like online security in easy to understand terms" – NE27.

General Sketch Analysis. Despite being instructed that sketches should relate to digital technology, participants relied heavily on sketches of physical items and offline situations to explain online phenomena and constructs. This may be due to the ethereal nature of online items; we cannot always *see* the data, but we know it exists. To depict such items, participants resorted to imagery they understood. Even though we requested participants to use little to no text in their representations, many felt the need to caption their sketches, most likely because they felt that their sketching skills were not adequate to communicate their ideas without the supporting textual annotations or because some items have text in them as a matter of course (e.g., browser windows, credit cards). Additionally, some participants used words as part of comics-style communication (i.e., thought or speech bubbles), and two participants used each concept as a panel in a comic strip such that their sketches taken together told a story spanning all four themes we asked them to draw.

Cross-cutting Imagery. Some visual imagery appeared across all themes. For example, padlocks were featured in 29/160 images, although the expert group did not use them for *cybersecurity* and *risk*. Similarly, real-world brand names and apps, such as Facebook, Apple, etc., were present across all themes (19/160). A high proportion of participants used images of hardware, such as desktop computers, laptops, mobile phones, or tablets (56/160). However, the most frequently-occurring images were those of humans (75/160), depicting one or more persons. Diagrammatic images frequently contained one or more depictions of people, and the theme of *trust* included the most human imagery, such as depictions of two people hugging, individuals shaking hands, parents with children, or trust falls.[4] Visual depictions of *trust* and *risk* stood out for the use of physical dangers, including sharks, water traps, falls, and monsters. Physical dangers did not appear in the images of *privacy* at all and appeared only twice in the expert sketches for *cybersecurity*.

4.3 Risk

In the online environment, expectations of potentially damaging outcomes have a direct effect on high-risk actions and behaviours [9]. Feelings of distrust and high risk are related and can be characterised as suspicion, wariness, and fear rooted in the desire for protection from harm [9]. Risk is seen in opposition to trust [3]. We found that participant sketches reflected this connection between (dis)trust and risk. Participants drew specific threats to life (e.g., being eaten by a shark or falling off a cliff or a tightrope). In comparison to *trust*, drawings for *risk* contained solitary figures; there is no one to catch the falling individual. Contrary to *trust*, sketches for *risk* showed many negative actions (e.g., identity theft, financial loss, stabbing). Experts drew digital risk with reference to infrastructure hacking, black-box algorithms, unpatched systems, access permissions, unknown programs, spam, and lack of industry investment in protection because it is not "profitable".

Offline/Online Imagery. The sketches showed a divergence between online and offline risk. A majority of non-experts drew *risk* in offline environments with links to fear and potential harm. Of those who drew *risk* in online environments (including most expert participants), risks were similar (e.g., malicious pop-ups or spam). However, consequences were considered less frequently, and if drawn, focused on individual and localised concerns (e.g., financial or identity theft). Few participants noted broader consequences, such as system infection or network disruption. The portrayal of *risk* as individually harmful with low consideration of wider consequences suggests that it is important to educate and inform users regarding the larger impacts of their online actions.

4.4 Privacy

Participants depicted *privacy* as an attempt to protect themselves online (e.g., blocking social media websites/applications, using incognito mode). Many drew Internet of Things (IoT) devices as these devices have become commonplace. Some participants captured recent media stories of webcams used to spy on people and microphones used to eavesdrop. For experts and non-experts alike, privacy in online environments centred around *action*, e.g., using incognito mode, VPN, and other means to protect spaces (e.g., covering webcams, not using specific IoT devices). Participants represented *privacy*, or lack thereof, as a process of *physically* passing along personal information and data to others or physically removing devices from spaces. Control was important to several participants, who sketched objects implying individual and localised control, such as locks [2]. Interestingly, control measures drawn by experts were often sarcastic or cynical, e.g., unplugging CCTV cameras. For instance, a sketch by E6 included the text: "Privacy is becoming an obsolete concept in a world that is constantly connected by tech giants that inherently surveil."

Offline/Online Imagery. Of the participants who drew *privacy* in offline environments, the home and the family were central. Images included locked doors, home safety systems, and closed curtains. The drawings reflect people's feeling that homes are private places, which they can, and should be able to, control. Privacy in the home is treated as sacrosanct. Interestingly, participants depicted firmly-shut front doors, without explicit indication that privacy can be altered by opening the doors. When comparing offline and online depictions of *privacy*, the sketches predominantly featured the door remaining shut or privacy being maintained, with only a small number of sketches showing privacy as being under threat or breached.

Data & Surveillance. Experts and non-experts were similar in their depictions of *privacy*. We identified 'surveillance' as a prominent category, focusing on violations of consent and invasions of privacy by "listening in" and "spying on". Those surveilling were often websites and apps (especially social media), "the government", and those who want to make money by selling personal information to third parties. 'Data' was identified as a category that covered personal data and information. Sketches captured the feeling that a person's data *is* the person and should belong to the person. Sketches of *privacy* echo the literature that people are more concerned about unauthorised *disclosure* of information than about unauthorised modification or destruction of information or disruption of access to, or use of, information or systems [16].

4.5 Trust

There is a clear overlap in the literature between cybersecurity, privacy, and trust [7, 13, 22]. Most characterisations of trust are based upon interpersonal considerations, with few connected specifically to the digital realm. Therefore, we sought to seek sketches that uncover the ways in which trust is conceptualized in the online sphere. People place or refuse trust based upon judgement or assessment [46]. Therefore, trust is *active* in that it can be updated based on available information and also an *action* in that it relies on 'doing'. Participants depicted *trust* by sketching verbs: thinking, looking, listening, using, falling, and jumping. In these cases, *trust* was drawn literally to describe what we do and how we feel when trusting (although four non-experts drew abstract forms). We further identified that these sketches contained the themes of balance, gradualness, naturalness, fluidity, connectivity, and illumination. As with *privacy*, defining *trust* is difficult because of its complex, context-specific nature, especially in an online context [34, 36, 46]. The overall diversity of sketches of *trust* reflected this multivalent nature of trust.

[4] A trust fall is a team building exercise in which an individual falls backwards with eyes closed, relying on a colleague/acquaintance to break the fall.

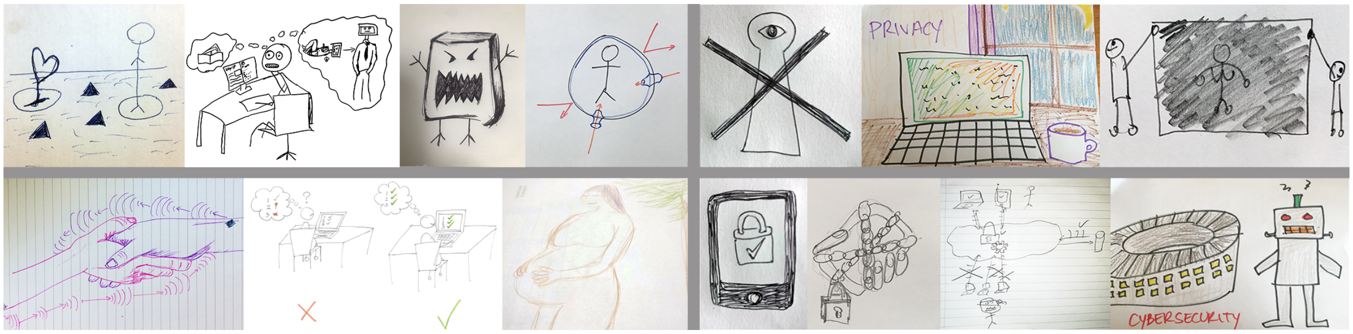

Figure 3: Sketches for *risk* (top left); *privacy* (top right); *trust* (bottom left); and *cybersecurity* (bottom right).

Offline/Online Imagery. While all participants had experienced digital trust, when characterising *trust* in an online context they could not completely separate it from 'traditional' offline trust. Although the instructions explicitly asked participants to draw "digital trust", a number of non-experts (19) and experts (3) sketched trust with no elements of technology. Additionally, some participants depicted digital trust as human connection incorporated into the digital realm (e.g., stick figures using social media or shopping online). *Digital* trust was sketched explicitly by only a third of the non-experts, reflecting generic practices such as using technology for interpersonal communication, paying for online purchases, finding trustworthy online information sources, etc. Conversely, the experts were more focused on depicting *digital* trust, drawing representations of *trust* as the protection of personal data and included IoT devices. Expert and non-expert participants alike depicted digital *trust* in reference to mechanisms encountered in online activities (e.g., trust ratings, badges, and certificates) [16, 44]. For instance, expert P2 sketched digital trust showing secure channels (i.e., HTTPS), trustworthy brands, and International Organization for Standardization (ISO) standards. Overall, digital trust is built and maintained using cues such as industry standards and reputation and questioned when it cannot be taken for granted.

Affect. Conceptually, *trust* was depicted positively, e.g., a person in the middle of a trust fall, neither having being caught nor having fallen. However, some negative consequences were identified as well. One non-expert drew an unsuccessful trust fall, and two experts drew potential pitfalls: personal information floating away and a house being blown-up. Overall, *trust* was associated with positive connotations in comparison to *risk*. Our analysis of trust sketches identified nine positive abstract themes: togetherness, familiarity, comfort, calm, love, happiness, safety, protection, and sense of security. In comparison to other concepts, we identified fewer negative themes for *trust*.

4.6 Cybersecurity

Similar to Oates et al. [45], we found that security and privacy are closely related in people's minds. As with *privacy*, physical items, such as padlocks (13) and protective shields (6), were prevalent in the non-expert sketches. Some non-experts (6) presented the idea of a "force field" or a "shield", possibly alluding to a sense of containment within cyberspace. In contrast, expert sketches showed a general sense of cynicism and uncertainty regarding cybersecurity. Depictions of experts included: network of rabbit holes, mystery, myth, and snake oil. Literal depictions included phishing (4), the EU General Data Protection Regulation (GDPR) (2), and the stereotypical hooded hacker. Interestingly, the 'hoodie' was chosen as the overarching image for *cybersecurity* during the group analysis, despite appearing only once in the expert sketches.

Cybersecurity as a Losing Battle. Some experts felt that cybersecurity is a mere marketing strategy and that defense efforts are futile. One expert point out the simplicity of cyberattacks compared to physical attacks. There were indications of similar thoughts even amongst non-experts (4). Some non-expert sketches contained imagery of camera-based surveillance and showed information escaping a protective shield. Further, some non-experts associated *cybersecurity* with games, with one even portraying a game of Battleship between hackers and end-users. Another non-expert sketched *cybersecurity* as blindfolded hide-and-seek, where the 'seeker' is at a significant disadvantage.

Lack of Awareness of Cybersecurity. Several non-expert sketches (16) contained symbols typically associated with digital security (e.g., shield, padlock). In contrast to concepts such as trust, where actions denoting the concept of trust were often portrayed, it appears that the understanding of cybersecurity amongst the public consists mostly of what common entities within cyberspace show or sell (e.g., antivirus protection, encryption). People generally have an understanding of concepts such as trust and privacy from their everyday lives, giving them a baseline to interpret these concepts within cyberspace. However, the concept of cybersecurity appears to remain foreign and elusive. The observations from the drawings are further substantiated by questionnaire responses of the non-expert participants, where nearly half qualified the sketches they submitted by saying they did not know anything about *cybersecurity*. Ironically, the professed ignorance ties back to the cynicism expressed by the experts in their sketches of *cybersecurity*, where most depicted it as a mystery, myth, or uncertainty. Further, cybersecurity measures are seen as a "hard sell" to those who feel that the threat is unreal until after it ends up affecting them negatively.

5 DISCUSSION AND IMPLICATIONS

Sketching as an investigative method of eliciting visuals for cybersecurity themes provided an interesting set of data and raised questions regarding public and practice-based perceptions of the field. Visualisation within cybersecurity underpins the understanding and dissemination of data in the field. Despite over a decade of VizSec symposia [51], the potential for visuals is not yet fully realised. Using sketching, we were able to surface content that may not otherwise have emerged and to generate rich, personal, and evocative views that were sometimes surprising. In the course of sketching cybersecurity-related themes, participants were able to recognise their own understanding or lack thereof. The physical security metal model [8] was the most prevalent, containing descriptions of locks and keys with individual and localised control [2, 45]. It may not be necessary to settle on a single image or definition of risk, privacy, trust, or cybersecurity, as people have different interpretations in different contexts. No mental model is ever “correct” or “right”, and models change constantly with changes in context and background information [31, 33, 59]. Yet, our findings show that some mental models are shared widely, which can be useful when communicating with users regarding cybersecurity.

Expert participants deemed visualisations suitable mostly for educating or communicating with non-experts regarding the complexities of cybersecurity. We might argue that the very definition of ‘expert’ may require re-imagining as there was a feeling that knowledge was missing even amongst experts [32]. Since cybersecurity experts must often work with non-experts, effective visualisation could help improve collaboration and communication in groups with diverse expertise. Moreover, our findings demonstrate that visual depictions can be useful for purposes beyond enhancing communication. For example, widely relatable, recurrent themes in user-generated sketches could be used in the design of cybersecurity-related user experiences [56, 61]. Cybersecurity practitioners could further benefit from sketching as a means to understand their own motivations and opinions.

The Hooded Hacker stereotype is pervasive in media depiction of cybersecurity [18, 37]. So ingrained is this depiction that it has become synonymous with incursions and data breaches. Surprisingly, even cybersecurity experts perpetuated this stereotype in their sketches, despite knowing its inaccuracy. Media stereotypes were evident in expert and non-expert depictions of hacking. If familiar media language is becoming *universal* then we may need to challenge it: our investigation indicates that the visual language of cybersecurity is a *social construct.* Although *openIdeo* [47] ran their competition for media perceptions in cybersecurity, the results of that task fall outside of the interpretation and usage in the field because it was a design-based exercise rather than empirical research. There are, however, comparisons to be made with our findings. For example, the top 25 submissions to the competition portrayed themes to similar to the sketches we collected (e.g., hide-and-seek, monsters, sharks). These commonalities can perhaps be taken as representative of public opinion and may have implications for the development and evolution of a visual language for cybersecurity.

We expressly asked participants to draw concepts relating to the *online* realm. Yet, many participants chose to draw the offline world (e.g., padlocks, shields, windows), similar to icons in the Noun Project[5] which include physical objects. It may be that the mental models used by participants cannot be cleanly separated into online and offline modes. The mixing of the offline world with online concepts is surprising given that Camp [8] has argued that the differences between online and offline worlds make it difficult to leverage mental models based on physical security concepts. It is possible that the images drawn by participants are metaphors, indicating that the underlying concept is abstract or difficult to envisage. These difficulties suggest that cybersecurity communication could benefit from making relevant connections to familiar objects and concepts from the offline world. Metaphors from the offline world may serve as an effective bridge for the gap between known real-world experiences and unknown digital operations [25].

Currently, no visual standards for cybersecurity exist, despite the range of work in this area [42, 51] and public interest in its depictions [37, 47, 54]. Our findings serve as the initial step for a larger library of visual materials for the depiction of cybersecurity. User-generated sketching can be used to generate local and culturally-specific icons and imagery, harnessing the flexibility and creativity of diverse users rather than treating the typical set of images dominated by the Western cultural context as globally applicable. Although the Noun Project and the recent openIdeo finalists depicted some themes similar to ours [47], there are notable differences between designer-produced imagery and that generated by the public and cybersecurity experts. Our work points to the promise of employing user sketches for enhancing cybersecurity communication and user experiences. For instance, images from a library of cybersecurity visuals could be used to populate security dashboards and create visuals for specific applications and/or locales. Further, end users could sketch and use their own images in cybersecurity user interfaces.

Our findings highlight that sketching as a method can be useful in cybersecurity research in at least two ways. First, the addition of a sketching component in cybersecurity research can be a powerful addition that helps surface user mental models not uncovered via written and verbal articulation. To that end, it would be interesting to employ sketching to dig deeper into various cybersecurity concepts. For instance, user-generated visuals of specific cyberattacks (e.g., ransomware, man-in-the-middle) can help reveal the extent to which non-expert mental models map to real-world threats and, in turn, leverage that mapping to help improve training and protection. Second, sketching can make cybersecurity user research more inclusive by allowing expression for those who may find written and verbal articulation difficult.

6 CONCLUSION

We demonstrated that sketching can be effective for gauging understanding of cybersecurity. Experts and non-experts alike create meaningful, recurring imagery and complex scenes that depict salient facets of *risk*, *privacy*, *trust*, and *cybersecurity*. Notably, user-generated sketches emphasise the *human* embedded within the complexity of cybersecurity, showing presence and interaction alongside technical objects and infrastructure, such as hardware and cloud processes. Next steps for the development and utilisation of imagery in the field could include expanding the investigative

[5] https://thenounproject.com/

focus to explore additional topics or to standardise icons and images across cultures and fields. Our work highlights the utility of sketching as a research method and facilitates the development of a visual language for communicating with end users about matters related to cybersecurity.

ACKNOWLEDGMENTS

This research was funded by the UK EPSRC under grant EP/N028228/1 (PACTMAN).

REFERENCES

[1] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-Based Authentication Schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 316–322. https://doi.org/10.1145/2785830.2785882

[2] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. Mental Models of Security Risks. In *Financial Cryptography and Data Security*, Sven Dietrich and Rachna Dhamija (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 367–377. https://doi.org/10.1007/978-3-540-77366-5_34

[3] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? (2019). arXiv:1901.02672 [cs.CR]

[4] Georgios Bakirtzis, Brandon J. Simon, Cody H. Fleming, and Carl R. Elks. 2018. Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis. In *2018 IEEE Symposium on Visualization for Cyber Security (VizSec '18)*. 1–8. https://doi.org/10.1109/VIZSEC.2018.8709187

[5] Robert Biddle, Sonia Chiasson, and P. C. Van Oorschot. 2012. Graphical Passwords: Learning from the First Twelve Years. *ACM Comput. Surv.* 44, 4, Article 19 (Sept. 2012), 41 pages. https://doi.org/10.1145/2333112.2333114

[6] Flora Bowden, Dan Lockton, Rama Gheerawo, and Clare Brass. 2015. *Drawing energy: Exploring perceptions of the invisible.* Royal College of Art, London, UK.

[7] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security Privacy* 9, 2 (2011), 18–26. https://doi.org/10.1109/MSP.2010.198

[8] L. Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and Society Magazine* 28, 3 (2009), 37–46. https://doi.org/10.1109/MTS.2009.934142

[9] Yong-Sheng Chang and Shyh-Rong Fang. 2013. Antecedents and distinctions between online trust and distrust: Predicting high-and low-risk internet behaviors. *Journal of Electronic Commerce Research* 14, 2 (2013), 149–166.

[10] Nabie Y. Conteh and Paul J. Schmick. 2016. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research* 6, 23 (2016), 31. https://doi.org/10.19101/IJACR.2016.623006

[11] Andrew Cox and Melanie Benson. 2017. Visual methods and quality in information behaviour research: The cases of photovoice and mental mapping. *Information Research* 22, 2 (Jun 2017), n2.

[12] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3173575

[13] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401. https://doi.org/10.1007/s00779-004-0308-5

[14] Cyrus Farivar. 2009. A brief examination of media coverage of cyberattacks (2007–Present). In *The virtual battlefield: Perspectives on cyber warfare*, Christian Czosseck and Kenneth Geers (Eds.). Vol. 3. IOS Press, 182–188.

[15] Batya Friedman, David Hurley, Daniel C. Howe, Helen Nissenbaum, and Edward Felten. 2002. Users' Conceptions of Risks and Harms on the Web: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems* (Minneapolis, Minnesota, USA) *(CHI EA '02)*. Association for Computing Machinery, New York, NY, USA, 614–615. https://doi.org/10.1145/506443.506510

[16] Susanne Furman, Mary Frances Theofanos, Yee-Yin Choong, and Brian Stanton. 2012. Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy* 10, 2 (2012), 40–49. https://doi.org/10.1109/MSP.2011.180

[17] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 385–398. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher

[18] Nicole Gallucci. 2017. *We need to talk about all these absurd stock photos of hackers.* https://mashable.com/2017/05/15/horrible-hacker-stock-photos/ Accessed: 2021-05-28.

[19] Jeffery Garae and Ryan K. L. Ko. 2017. Visualization and Data Provenance Trends in Decision Support for Cybersecurity. In *Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications*, Iván Palomares Carrascosa, Harsha Kumara Kalutarage, and Yan Huang (Eds.). Springer International Publishing, Cham, 243–270. https://doi.org/10.1007/978-3-319-59439-2_9

[20] Deborah Gonzalez. 2014. *Managing online risk: Apps, mobile, and social media security.* Butterworth-Heinemann.

[21] Devon Greyson, Heather O'Brien, and Saguna Shankar. 2020. Visual analysis of information world maps: An exploration of four methods. *Journal of Information Science* 46, 3 (2020), 361–377. https://doi.org/10.1177/0165551519837174

[22] Joshua B. Gross and Mary Beth Rosson. 2007. Looking for Trouble: Understanding End-User Security Management. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '07)*. Association for Computing Machinery, New York, NY, USA, 10–es. https://doi.org/10.1145/1234772.1234786

[23] Peter Hall, Claude Heath, and Lizzie Coles-Kemp. 2015. Critical visualization: a case for rethinking how we visualize risk and security. *Journal of Cybersecurity* 1, 1 (12 2015), 93–108. https://doi.org/10.1093/cybsec/tyv004

[24] Gunnar Harboe and Elaine M. Huang. 2015. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 95–104. https://doi.org/10.1145/2702123.2702561

[25] Jenna Hartel. 2017. Adventures in visual analysis. *Visual Methodologies* 5, 1 (2017), 80–91. https://doi.org/10.7331/vm.v5i1.106

[26] Jenna Hartel, Rebecca Noone, Christie Oh, Stephanie Power, Pavel Danzanov, and Bridgette Kelly. 2018. The iSquare protocol: Combining research, art, and pedagogy through the draw-and-write technique. *Qualitative Research* 18, 4 (2018), 433–450. https://doi.org/10.1177/1468794117722193

[27] Tarik Ibrahim, Steven M. Furnell, Maria Papadaki, and Nathan L. Clarke. 2010. Assessing the Usability of End-User Security Software. In *Trust, Privacy and Security in Digital Business*, Sokratis Katsikas, Javier Lopez, and Miguel Soriano (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 177–189. https://doi.org/10.1007/978-3-642-15152-1_16

[28] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[29] Lee Jarvis, Stuart Macdonald, and Andrew Whiting. 2015. Constructing Cyberterrorism as a Security Threat: A Study of International News Media Coverage. *Perspectives on Terrorism* 9, 1 (2015), 60–75. http://www.jstor.org/stable/26297327

[30] Rebecca Jeong. 2019. *Children and Adults' Perception of Signal Colours, Symbols, and Words in the Context of Cybersecurity Warnings.* Master's thesis. Carleton University, Ottawa, Canada. https://doi.org/10.22215/etd/2019-13469

[31] Natalie A. Jones, Helen Ross, Timothy Lynam, Pascal Perez, and Anne Leitch. 2011. Mental Models: An Interdisciplinary Synthesis of Theory and Methods. *Ecology and Society* 16, 1 (2011), 13 pages. http://www.jstor.org/stable/26268859

[32] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 39–52. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

[33] Frank C. Keil. 2010. The Feasibility of Folk Science. *Cognitive Science* 34, 5 (2010), 826–862. https://doi.org/10.1111/j.1551-6709.2010.01108.x

[34] Bran Knowles. 2016. Emerging Trust Implications of Data-Rich Systems. *IEEE Pervasive Computing* 15, 4 (2016), 76–84. https://doi.org/10.1109/MPRV.2016.68

[35] Anita Komlodi, Penny Rheingans, Utkarsha Ayachit, John R. Goodall, and Amit Joshi. 2005. A user-centered look at glyph-based security visualization. In *IEEE Workshop on Visualization for Computer Security (VizSEC 05)*. 21–28. https://doi.org/10.1109/VIZSEC.2005.1532062

[36] Meriem Laifa, Samir Akrouf, and Ramdane Maamri. 2015. Online Social Trust: An Overview. In *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication* (Batna, Algeria) *(IPAC '15)*. Association for Computing Machinery, New York, NY, USA, Article 9, 6 pages. https://doi.org/10.1145/2816839.2816912

[37] Selena Larson. 2017. *Why do hackers always wear hoodies? Behind the stereotype.* https://money.cnn.com/2017/05/26/technology/hacker-hoodie-stereotype-hacking/index.html Accessed: 2021-05-28.

[38] Makayla Lewis and Lizzie Coles-Kemp. 2014. A tactile visual library to support user experience storytelling. In *Proceedings of NordDesign 2014* (Espoo, Finland). 386–395.

[39] Makayla Lewis, Miriam Sturdee, and Nicolai Marquardt. 2018. Applied Sketching in HCI: Hands-on Course of Sketching Techniques. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC,

Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3170427.3170649

[40] Makayla M. Lewis and Lizzie Coles-Kemp. 2014. Who Says Personas Can't Dance? The Use of Comic Strips to Design Information Security Personas. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI EA '14)*. Association for Computing Machinery, New York, NY, USA, 2485–2490. https://doi.org/10.1145/2559206.2581323

[41] Sean McKenna, Diane Staheli, Cody Fulcher, and Miriah Meyer. 2016. BubbleNet: A Cyber Security Dashboard for Visualizing Patterns. *Computer Graphics Forum* 35, 3 (2016), 281–290. https://doi.org/10.1111/cgf.12904

[42] Sean Mckenna, Diane Staheli, and Miriah Meyer. 2015. Unlocking user-centered design methods for building cyber security visualizations. In *2015 IEEE Symposium on Visualization for Cyber Security (VizSec '15)*. 1–8. https://doi.org/10.1109/VIZSEC.2015.7312771

[43] Christine Mekhail, Leah Zhang-Kennedy, and Sonia Chiasson. 2014. Visualizations to teach about mobile online privacy. In *Adjunct Proceedings of the International Conference on Persuasive Technology (PERSUASIVE 2014)*. 3 pages.

[44] Jason R. C. Nurse, Sadie Creese, Michael Goldsmith, and Koen Lamberts. 2011. Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. 60–68. https://doi.org/10.1109/STAST.2011.6059257

[45] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (2018), 5–32.

[46] Onora O'neill. 2002. *A question of trust: The BBC Reith Lectures 2002*. Cambridge University Press.

[47] openIDEO. 2019. *How might we reimagine a more compelling and relatable visual language for cybersecurity?* https://www.openideo.com/challenge-briefs/cybersecurity-visuals Accessed: 2021-05-28.

[48] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2019. "Woe is Me": Examining Older Adults' Perceptions of Privacy. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3290607.3312770

[49] Delanie Ricketts and Dan Lockton. 2019. Mental Landscapes: Externalizing Mental Models through Metaphors. *Interactions* 26, 2 (Feb. 2019), 86–90. https://doi.org/10.1145/3301653

[50] Hossein Siadati, Bahador Saket, and Nasir Memon. 2016. Detecting malicious logins in enterprise networks using visualization. In *2016 IEEE Symposium on Visualization for Cyber Security (VizSec '16)*. 1–8. https://doi.org/10.1109/VIZSEC.2016.7739582

[51] Diane Staheli, Tamara Yu, R. Jordan Crouser, Suresh Damodaran, Kevin Nam, David O'Gwynn, Sean McKenna, and Lane Harrison. 2014. Visualization Evaluation for Cyber Security: Trends and Future Directions. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security* (Paris, France) *(VizSec '14)*. Association for Computing Machinery, New York, NY, USA, 49–56. https://doi.org/10.1145/2671491.2671492

[52] Miriam Sturdee, Paul Coulton, Joseph G. Lindley, Mike Stead, Haider Ali, and Andy Hudson-Smith. 2016. Design Fiction: How to Build a Voight-Kampff Machine. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 375–386. https://doi.org/10.1145/2851581.2892574

[53] Miriam Sturdee, Aluna Everitt, Joseph Lindley, Paul Coulton, and Jason Alexander. 2019. Visual Methods for the Design of Shape-Changing Interfaces. In *Human-Computer Interaction – INTERACT 2019*, David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris (Eds.). Springer International Publishing, Cham, 337–358. https://doi.org/10.1007/978-3-030-29387-1_19

[54] Eli Sugarman and Heath Wickline. 2017. *The Sorry State of Cybersecurity Imagery*. https://www.lawfareblog.com/sorry-state-cybersecurity-imagery Accessed: 2021-05-28.

[55] Mariarosaria Taddeo, Tom McCutcheon, and Luciano Floridi. 2019. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence* 1, 12 (2019), 557–560. https://doi.org/10.1038/s42256-019-0109-1

[56] Bernardo Malta Leite Telles, Shapor Naghibzadeh, and Carey Stover Nachenberg. 2021. User interfaces for presenting cybersecurity data. United States Patent 10958534.

[57] J. Walny, S. Huron, and S. Carpendale. 2015. An Exploratory Study of Data Sketching for Visual Representation. *Computer Graphics Forum* 34, 3 (2015), 231–240. https://doi.org/10.1111/cgf.12635

[58] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. https://doi.org/10.1145/1837110.1837125

[59] Rick Wash and Emilee Rader. 2011. Influencing Mental Models of Security: A Research Agenda. In *Proceedings of the 2011 New Security Paradigms Workshop* (Marin County, California, USA) *(NSPW '11)*. Association for Computing Machinery, New York, NY, USA, 57–66. https://doi.org/10.1145/2073276.2073283

[60] Justin Wu and Daniel Zappala. 2018. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 395–409. https://www.usenix.org/conference/soups2018/presentation/wu

[61] Yifan Yang, John Collomosse, Arthi Kanchana Manohar, Jo Briggs, and Jamie Steane. 2018. TAPESTRY: Visualizing Interwoven Identities for Trust Provenance. In *2018 IEEE Symposium on Visualization for Cyber Security (VizSec '18)*. 1–4. https://doi.org/10.1109/VIZSEC.2018.8709236

[62] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2013. Password advice shouldn't be boring: Visualizing password guessing attacks. In *2013 APWG eCrime Researchers Summit*. 1–11. https://doi.org/10.1109/eCRS.2013.6805770

[63] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2016. The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity. *International Journal of Human–Computer Interaction* 32, 3 (2016), 215–257. https://doi.org/10.1080/10447318.2016.1136177

[64] Leah Zhang-Kennedy, Elias Fares, Sonia Chiasson, and Robert Biddle. 2016. Geo-Phisher: The design and evaluation of information visualizations about Internet phishing trends. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*. 1–12. https://doi.org/10.1109/ECRIME.2016.7487941

[65] Haisheng Zhao, Wenzhong Tang, Xiaoxiang Zou, Yanyang Wang, and Yueran Zu. 2019. Analysis of Visualization Systems for Cyber Security. In *Recent Developments in Intelligent Computing, Communication and Devices*, Srikanta Patnaik and Vipul Jain (Eds.). Springer Singapore, Singapore, 1051–1061. https://doi.org/10.1007/978-981-10-8944-2_122