A Critical Look at the Visual Representation of Cybersecurity

By Paromita Bathija, Padmini Ray Murray, and Saumyaa Naidu

Edited by Karan Saini

Illustrations by - Paul Anthony George, and Roshan Shakeel

The Centre for Internet and Society and design collective Design Beku came together on the 15th of November for a workshop on Illustrations and Visual Representations of Cybersecurity. Images in the public sphere such as visuals in the media, Wikipedia commons, and stock images - play a vital role in the public's perception of cybercrime and cybersecurity. The existing imagery comprises of largely stereotypical images of silhouettes of men in hoodies, binary codes, locks, shields; all in dark tones of blue and green. The workshop aimed at identifying the concerns with these existing images and ideating on creating visuals that capture the nuanced concepts within cybersecurity as well as to contextualise them for the Global South. It began with a discussion on the various concepts within cybersecurity including disinformation, surveillance in the name of security, security researchers, regulation of big technology companies, gender and cybersecurity, etc. This was followed by a mapping of different visual elements in the existing cybersecurity imagery to infer the biases in them. Further, an ideation session was conducted to create alternate visualisations that counter these biases. A detailed report of the workshop can be read here.

The participants began by discussing the concerning impacts of present visualisations – there is a lack of representation and context of the global south. Misrepresentation of cybersecurity leads people to be susceptible to disinformation, treats cybercrime as an abstract concept that does not have a direct impact, and oversimplifies the problem and its solutions. The ecosystem in which this imagery exists also presented a larger issue. A majority of the images are created as clickbait alongside media articles. Media houses thus benefit from the oversimplification and mystification of cybersecurity in such images.

Through the mapping of existing images present online, several concerns were identified. The vague elements and unclear representation add to the mystification of cybersecurity as a concept. In present depictions, the use of technological devices and objects, leads to the lack of a human element, distancing the threat from any real impact to people using these devices. The metaphor of a physical threat is often used to depict cybersecurity using elements such as a lock and key. Recurring use of these elements gives a false idea of what is being secured or breached and how. Representations rely on tropes regarding the identity of hackers, and fail to capture the vulnerability of the system. The imagery gives the impression that systems which are breached are immensely secure to begin with and are compromised only as a result of sophisticated attacks carried out by malicious actors. The identity of hackers is commonly associated with cyber attacks and breaches, and the existing imagery reinforces this. Visuals showing a masked man or a silhouette of a man in dark background are the usual markers of a malicious hacker in conventional cybersecurity imagery. While there is a lack of representation of women in stock cybersecurity images, another trope found was that of a cheerful woman coder. There were also images of faceless women with laptops[1]. The

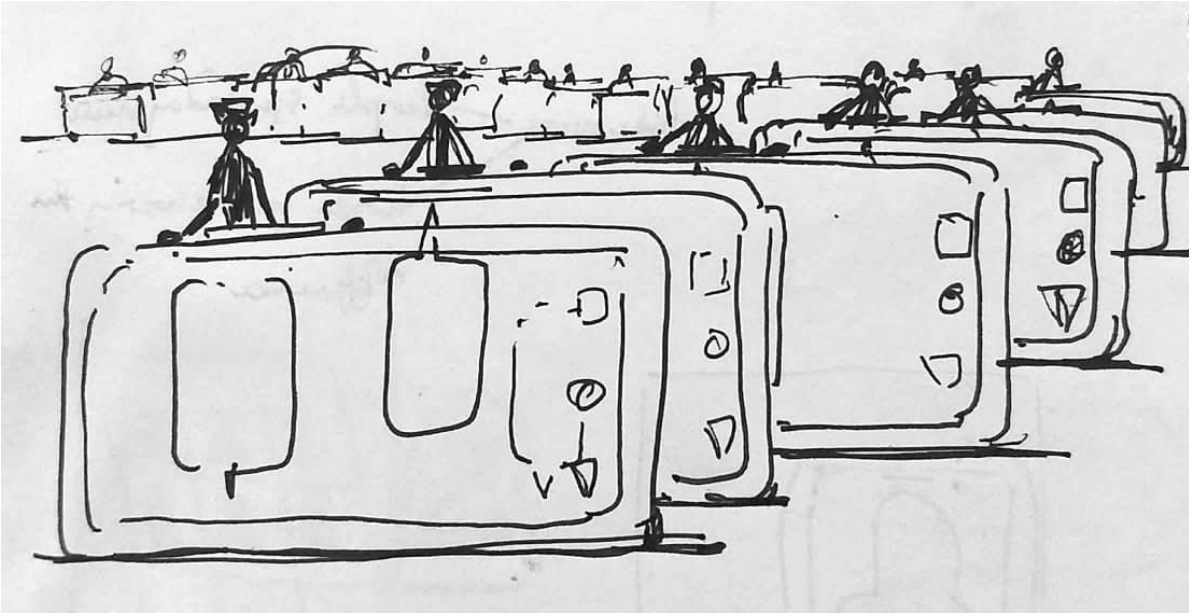
[1] https://www.independent.co.uk/life-style/gadgets-and-tech/features/women-in-tech-its-time-to-drop-the-old-stereotypes-7608794.html

reductive nature of these images point to deeper concerns around gender representation in cybersecurity.

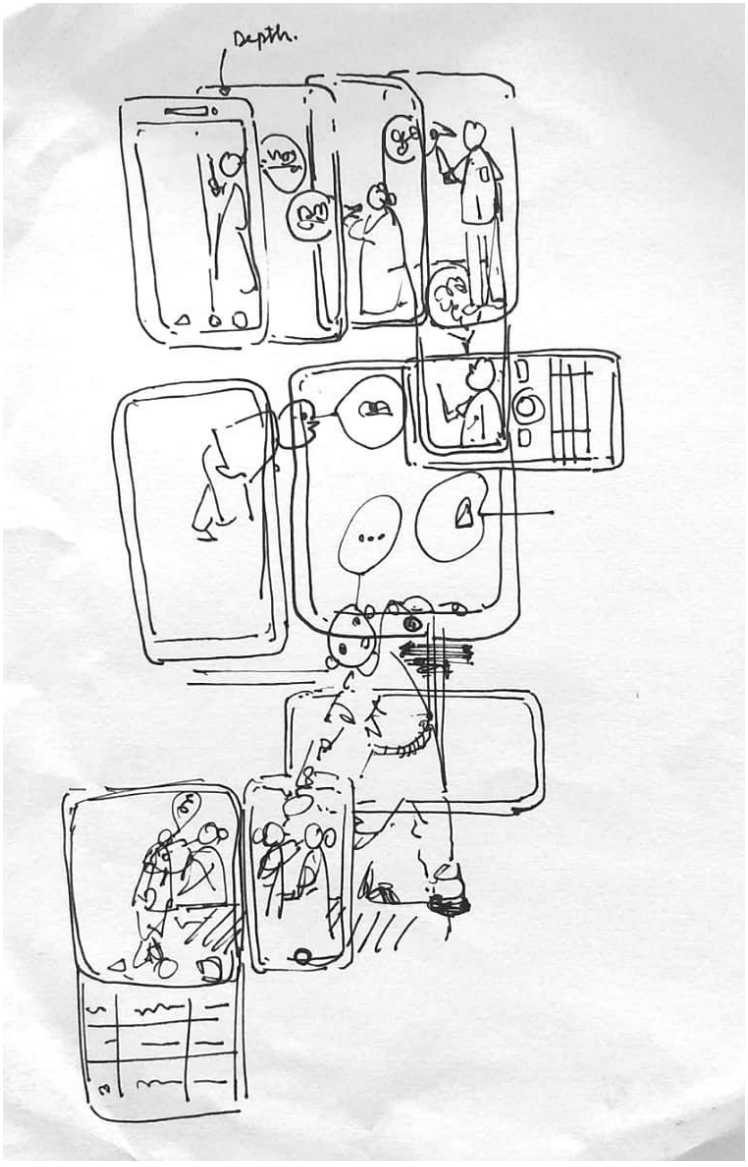
The participants examined what the implications of such visual representation would be, and why there is a need to change the imagery. How can visual depictions be more representative? Can they avoid subscribing to a homogenised idea of an Indian context – specific without being reductive? Can better depiction broaden understanding of cybercrime and emphasize the proximity of those threats? With technology, concepts are often understood through metaphors – how data is explained impacts how people perceive it. Visual imagery can play a critical role in demystifying concepts when done well; illustrations can change the discourse. They must begin to incorporate intersecting aspects of gender, privacy, susceptibility of vulnerable populations, generational and cultural gaps, as well as manifestations of the described crimes to make technological laypersons more aware of the threat.

Potential new imagery would need to address aspects such as disinformation, the importance of privacy and who has a right to it, change representation of hackers, depict the cybersecurity community, explain specific concepts to both – the general user and to the people part of cybersecurity efforts in the country, the implications of cybercrime on vulnerable populations, and more in an attempt to deconstruct and disseminate what cybersecurity looks like today.

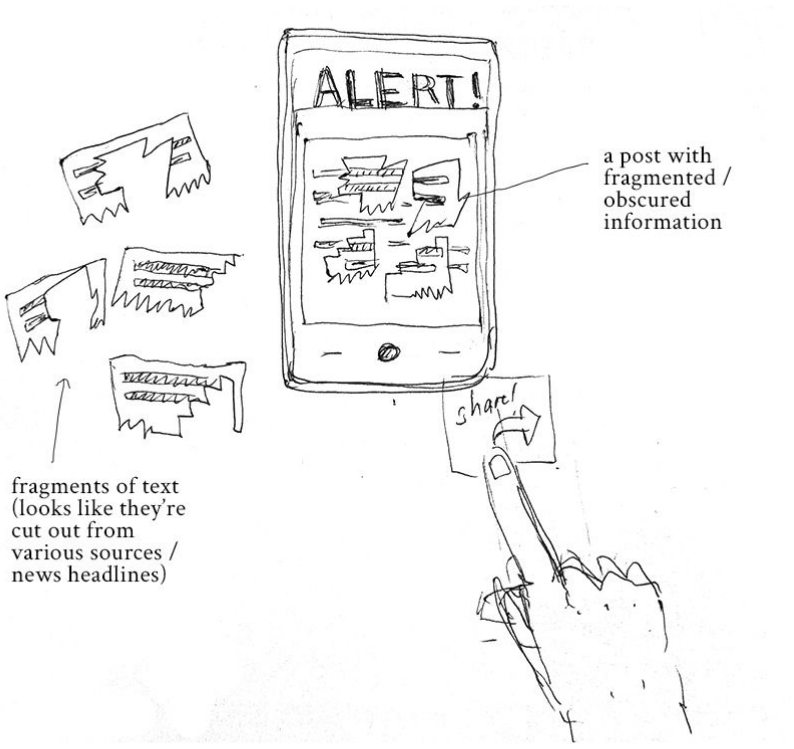
The ideation session involved rethinking specific concepts such as disinformation, and ethical hacking to create alternate imagery. For instance, disinformation was visually imagined as a distortion of an already distorted message being perceived by the viewer. In order to bring attention to the impact of devices, a phone was thought of as a central object to which different concepts of cybersecurity can be connected.

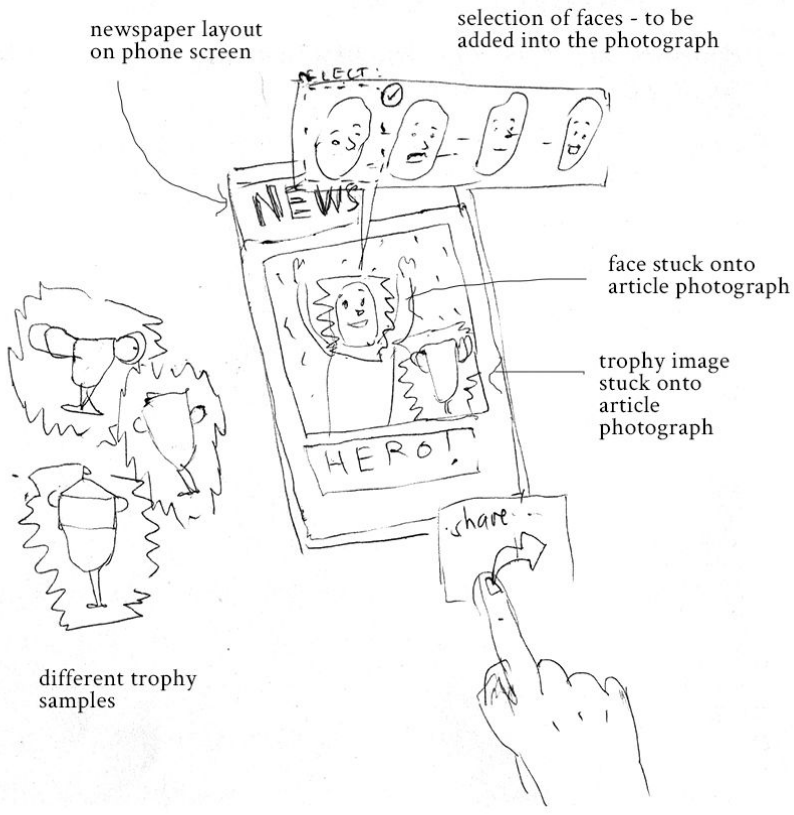


'Fake News Cascade' by Paul Anthony George

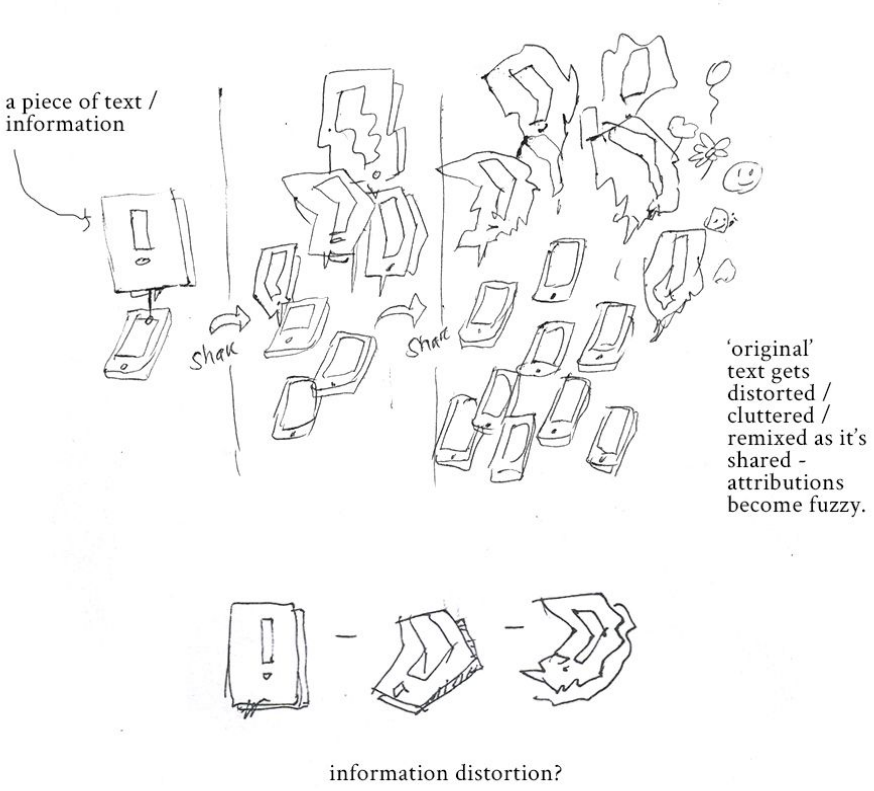


'Fake News' by Paul Anthony George



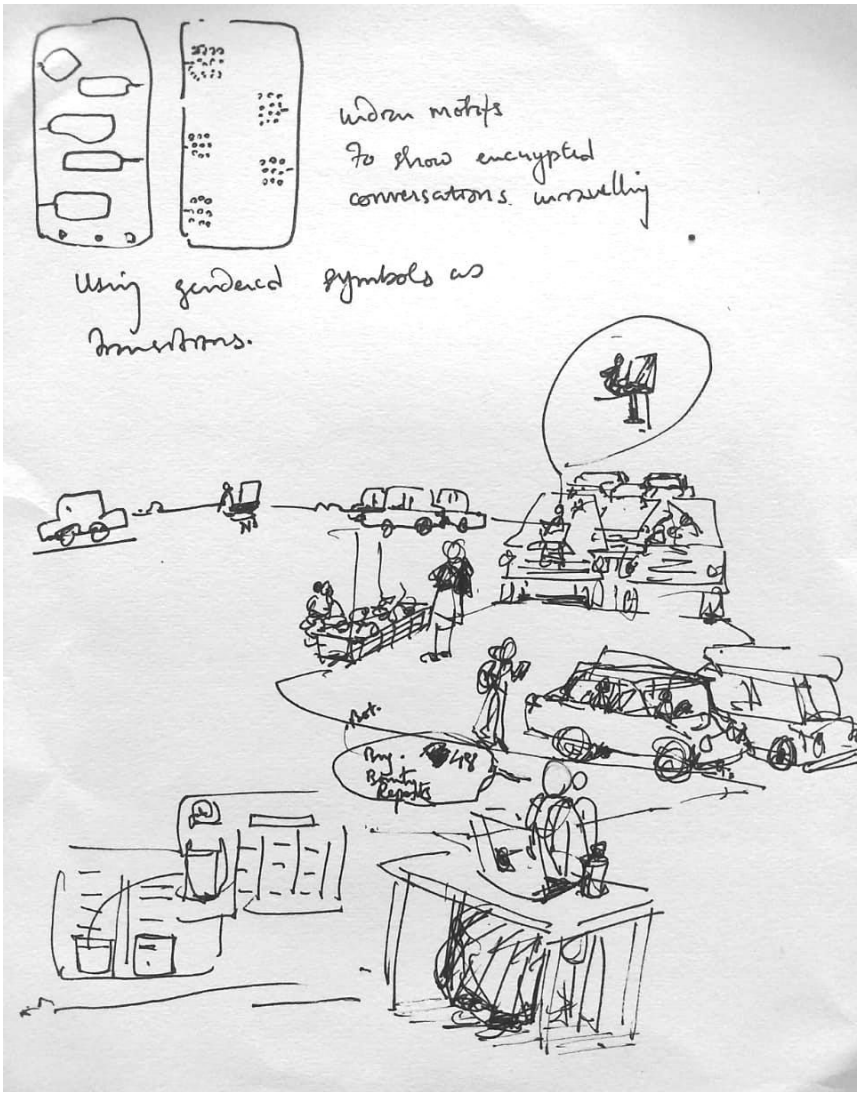


'Disinformation/ Fake News' by Roshan Shakeel; The sketch is about questioning the validity of what we see online, and that every message we see is constructed in some form or the other by someone else.

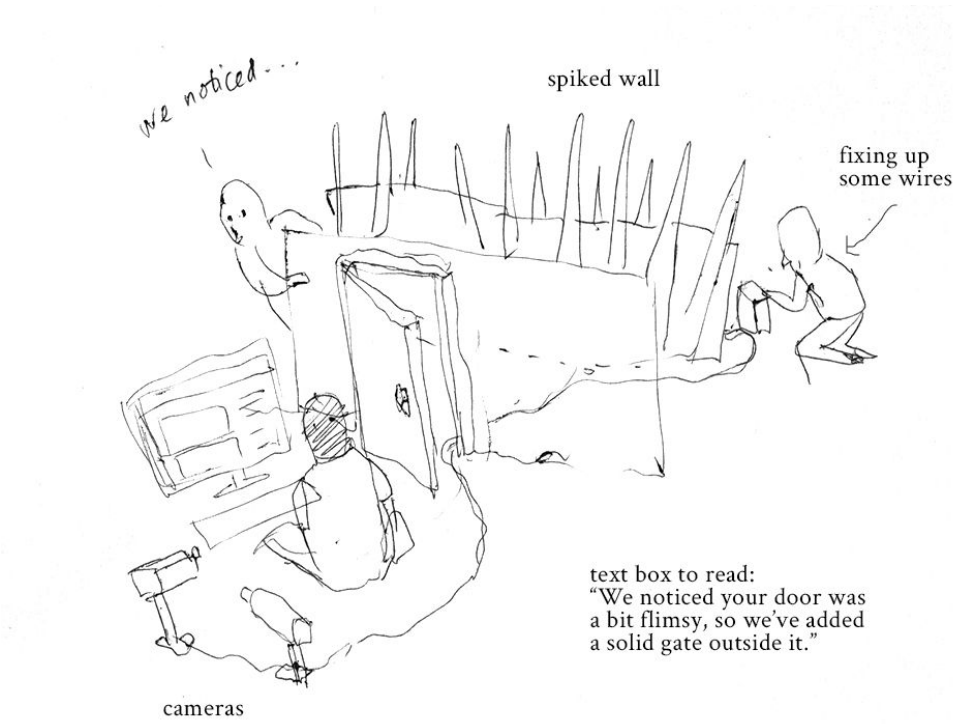


'Disinformation/ Fake News' by Roshan Shakeel; The sketch visualizes how the source of information ('the original') gets distorted after a certain point.

For ethical hacking, a visualisation depicting a day in the life of an ethical hacker was thought of to normalize hacking and to focus on their contribution in security research.



'A Day in the Life of an Indian Hacker' by Paul Anthony George



'Surveillance in the Name of Security' by Roshan Shakeel

Resources on ethical hacking (HackerOne)[2] and hacker culture (2600.com)[3] were also consulted as part of the exercise to gather references on the work done by hackers. This allowed a deeper understanding of how the hacker community depicts itself. Check Point Research[4] and Kerala Police Cyberdome[5] were also examined for further insight into cybersecurity. With regard to gender representation, sources that use visual techniques to communicate concerns and advocacy campaigns were also referred to. The Gendering Surveillance[6] initiative by the Internet Democracy project[7], which looks at how surveillance harms and restricts women, also offered insights on the use of illustrations supporting the case studies. Another reference was the "Visualising Women's Rights in the Arab World"[8] project by the Tactical Technology Collective[9]. The project aims to "strengthen the use of visual techniques by women's rights advocates in the Arab world, and to build a network of women with these skills".[10]

More visual explainers and animations[11] from the Tactical Technology Collective were noted for their broader engagement with digital security and privacy. A video by the Internet Democracy Project

[2] https://www.hackerone.com/
[3] https://2600.com/
[4] https://research.checkpoint.com/about-us/
[5] http://www.cyberdome.kerala.gov.in/
[6] https://genderingsurveillance.internetdemocracy.in/
[7] https://internetdemocracy.in/
[8] https://visualrights.tacticaltech.org/index.html
[9] https://tacticaltech.org/
[10] https://visualrights.tacticaltech.org/content/about-website.html
[11] https://tacticaltech.org/projects/survival-in-the-digital-age-ono-robot-2012/

that explains the Internet through *rangoli*[12], was observed specifically for setting the concept in Indian context through the use of aesthetics.

The workshop concluded with a discussion of potential visual iterations – imagery of cybersecurity that is not technology-oriented but focussed on the behavioural implications of access to such technology, illustrated public service announcements enhancing the profile of cybersecurity researchers or the everyday hacker. The impact of the discussion itself can indicate the relevance of such an effort. Artists and designers can be encouraged to create a body of imagery that shifts discourse and perception, to begin visualising for advocacy, demystify and stop the abstraction of cybercrime that can lead to a false sense of security, incorporate unique aspects of the debate within the Indian context, and generate new dialogue and understanding of cybersecurity. A potential step forward from this workshop would be to engage with the design community at large along with the domain experts to create more effective imagery for cybersecurity.

[12] https://internetdemocracy.in/2018/08/dots-and-connections/