THE CENTRE FOR internet & society

DESIGNಬೇಕು
ಡಿಸೈನ್BEKU

Workshop on Cyber Security Illustrations

Event Report

15th November, 2018 | Bangalore

By **Charana Reddy, Saumyaa Naidu**
Edited by **Pranav M Bidare, Arindrajit Basu, Karan Saini, Elonnai Hickok**

The Centre for Internet and Society, India
Design Beku

Introduction

Our artistic landscape in recent times has become increasingly defined by online visual narratives. Our perceptions are greatly altered by how ideas and concepts are illustrated. People tend to understand these concepts in a way which is limited to what the illustrations portray. In our image-saturated and image-driven culture, it is important not to misguide or be misguided.

Cyber security is one such concept which is mostly illustrated by stereotypical visual elements, such as a silhouette of a man, binary codes, locks, etc. People are primed to believe certain things due to the way they are shown or depicted. With an aim to break away from this clichéd imagery of cyber security, The Centre for Internet & Society conducted a workshop with Design Beku, a design collective based in Bangalore. The primary idea behind the workshop was to have a more nuanced take on cyber security, to engage in a discussion and brainstorming session with the members of the design community. The goal was to create visuals that depict the story and the history of the cyber security concepts at hand. These illustrations could replace the existing ones in newspaper editorials, or could be used along with written outputs that could get audiences to understand the concept in a more effective way.

The Workshop at a Glance

The day long workshop was organised on 15th of November in the CIS office in Bangalore. It was divided into two broad sessions. In the first session, the participants were briefed on the basic concepts of cyber security which the workshop would revolve around. Mainly, these involved: disinformation, surveillance in the name of security, cyber security community and government, companies like Facebook and Google becoming too big to be regulated, cross-Border data sharing, fintech security standards, implication of cybercrime on more vulnerable populations, economics of cyber security, International negotiations and norms formation and gender and cyber security. In the second session, the participants actively brainstormed different ways to visually narrate the concepts and problems which were discussed earlier in the day. This session consisted of exploring unconventional or non-stereotypical ways of graphically conceptualising the discussions.

Platforms and the Distortion of Truth

The discussion started by focussing on the distortion of the truth through platforms such as WhatsApp, Facebook, etc. Disinformation takes away the conversation from the real and important information as it is believed to be the absolute truth. Ideally, the message that was desired to be brought out was that information is to be verified before being shared with others. The discussion then shifted to the need for privacy and certain situations of unnecessary surveillance. Certain important questions related to the importance of privacy to different classes (and not just the upper middle class) were raised along with the thought of whether it was possible to convey the message--that everyone, regardless of class and community, is entitled to privacy--could be depicted through illustrations.

Security Researchers

The participants iterated that Security Researchers, or more commonly known as Ethical Hackers, are not given enough State recognition. Their services could be a priceless asset to improve the state of cyber security in the nation if utilised in the right way. A common goal was to change the conception of a hooded man (often white) sitting in front of a screen in a dark room as the only way to perceive hackers. Additionally, hacking was also desired to be depicted as an activity that is not necessarily malicious in nature, in the sense that it is useful and helpful in many cases. With respect to cross-border data sharing, the discussion involved the Cloud Act by the United States which was enacted in 2018. This act lays down certain requirements, fulfilment of which would qualify a foreign country to have access to content without undergoing a lengthy process. The need for regulation and security standards for the Fintech sector by the government was also briefly discussed.

Gender

Gender in cyber security was discussed in terms of how the discourse in going forward and that the representation and symbolism in security is presently largely male-based. The workshop also focused on the male-centric representation of ethical hackers and the lack of women involvement for various reasons. Key points arrived at during this part of the discussion included the perception of Cyber security as an inherently masculine line of employment with very little scope for participation of women, and the non-inclusion of the underrepresented in this sector. With respect to gender, another problem that was brought out was concerning safety applications. These apps give the impression that women need to be under constant watch or surveillance to feel/be safe. This was also a part of an initiative by the Internet Democracy Project which aims to fight gendered surveillance in India.[1]

Reclaiming Cybersecurity Imagery

Additionally, the first part of the workshop was also spent in exploring and mapping the existing imagery in cyber security. These include and are not limited to binary codes, lock and key, a circuit board, keyboards, an eye, anonymous masks, handcuffs, tunnels and cameras. Certain problems such as vulnerability of the system, lack of human elements, i.e., distancing the threat from the real impact, a trope of women coders, the details as to what is being secured and how, the identity of hackers, ecosystem of images were also identified.
In the second session, the workshop focused on *the how*: How the ideas, problems and lack of certain notions could be visually conceptualised. The aim was to reimagine the concepts and to come up with new ways to visually narrate them. This could be done by using metaphors of sound and speech, a digital shadow or animations. The demystification of cyber security as a concept is needed in images so that the impact and real concerns around it are better understood. Another key finding from this exercise was also the use of representative images for cyber security in media articles. Most visuals available on cyber security are stock images that have been created for generic use. The ecosystem in which these images exist also encourages visuals that can be used as clickbait. Hence, the need to bring about a larger change in creating these representative images was identified. In the context of ethical hackers, no one imagines them to be leading a normal life. The depiction of

[1] Denis Nolasco, (2018, March 28). Internet Democracy Project: Fighting Gendered Surveillance and access disparities in India, https://www.accessnow.org/internet-democracy-project/.

a day in the life of an Indian Hacker would allow people to understand the reality of the situation. However, normalcy is difficult to convey. Hence, the participants were of the view that illustrations should focus on enhancing the profiles of these hackers and promoting their importance.

Women's rights should be visualised in the context of holistic privacy (which includes gender and sexuality). Additionally, the group discussed that equality, pay gap, safety can also be taken as anchors for illustrating women’s rights. Fintech standards should be visualised in a way that shows the onus to be on the companies that come up with those standards. A phone could be used to illustrate cybercrime and surveillance together in the light of a precautionary tale. Furthermore, a phone can be used to create the visual narrative of being a central device to which cyber security concepts are connected. For instance, a phone can be used to depict various concepts such as privacy, tech created by women, cybercrime, surveillance, etc.

The ideation by all the participants led to inference that the visuals are to be created with the aim of behavioural changes such as vigilance, or awareness along with the aesthetics of the messaging that contextualise cyber security in India. All these concepts could be supported by the rule of law or any precedents as these concepts are not culturally Indian. Doing the same might have a larger persuasive value on the Indian audience. In order to contextualise this in India, aesthetic elements such as rangoli, mehendi and truck art can be used as a means of delivering the concepts more effectively. In conclusion, it was decided that the illustrations that are created out of this discussion could be used to serve as PSAs in non-digital spaces, could be used to explain about special issues to policymakers, could be used in collaboration with the International Centre for Journalists a larger outreach to the design community, illustrators at publications, and editors at media houses should be the step forward in order to bring about the desired change in the visual representation of cyber security.