Workshop on Cybersecurity Illustrations

15th November, 2018 | 10:00 am to 5:30 pm

The Centre for Internet and Society, Bangalore

CONCEPT NOTE

The notions around cybersecurity are deeply influenced by the visual associations available on it in the public sphere. The existing imagery on cybersecurity usually consists of stereotypical visual elements such as a silhouette of a man, binary codes, locks, etc. The dark colour palette in these visuals primarily comprising shades of blues and greens adds to the masculine imagery. The conception of the term is limited by these images. The Centre for Internet and Society hence, plans to engage with the design community in order to examine, explore, and expand this visual narrative of cybersecurity. CIS is organising a workshop on the 15th of November, in collaboration with a design collective in order to brainstorm ideas on creating illustrations for cybersecurity that shift the focus from coding to the human aspects.

Presently, the visuals suggest only data breaches when it comes to cybersecurity. Several nuanced concepts such as the implication on more vulnerable populations are not reflected in the images. The illustrations can also present the different stakeholders in the cybersecurity ecosystem. The workshop would be directed at generating more dialogues on cybersecurity through visuals.

Concepts for Illustrations

- Disinformation - fake news, election machine hacking
    - Disinformation commonly refers to the active spreading of false information to achieve specific objectives, often to weaken dependable sources of information, and distract public opinion (media and press). In the past, disinformation attacks have allegedly interfered with the outcome of elections.
- Surveillance in the name of security

    - Security and Privacy often emerge as tradeoffs for policy decisions. Often, regulation that is intended to provide security and oversight can be easily extended into acts of unauthorised and unnecessary surveillance.
- Cybersecurity community and government - relationship in India
    - The community of security researchers (ethical hackers) in India is an untapped resource that could greatly improve the state of domestic cybersecurity in India, if it is utilised by the government.
- Companies like Facebook and Google becoming too big to be regulated
    - Large data companies like Facebook and Google have amassed so many resources and acquisitions within them that it has become difficult and potentially impossible to sufficiently penalise them for violating laws, or their own terms of services.
- Cross border sharing - difficulty in procedure
    - An Indian citizen's data, when collected by a foreign company (like Facebook or Google) will be stored in a database in the foreign country. The process to obtain this data by Indian authorities is very tedious and cumbersome.
- Fintech security standards - easier transactions, but need for them to be secure
    - The Fintech industry in India is rapidly growing, and there is a need for a framework or a system of norms that must be followed by Fintech companies to protect their own systems and consumer's data. This is likely to be in the form of "standards" that are framed either by the government, or by the industry itself (self-regulation), or a combination of the two (co-regulation).
- Implication of cybercrime on more vulnerable populations
    - Among populations that are not conversant with specific technologies, or among illiterate populations, it is significantly easier to carry out cybercrimes. This situation only gets worse as technology becomes more advanced without an effective safeguard or policing mechanism against Cybercrime.
- Economics of cybersecurity - investment to prevent breaches
    - Due to the high-technological reliance of many cyber security tools and systems, private funding, often foreign is an attractive option for all sectors. However, this should be closely monitored and regulated to avoid lobbying efforts, or conflicts of interest.
- International negotiations and norms formation
    - Since the internet is a global good, any cyber security policy decision taken by India will have to be in the context of the international community. India's cyber-strategy will have to play off the strategies of other important countries to maximise security and development internally.
- Gender and cybersecurity-need for more female participation
    - Cyber security is an issue that is growing in importance. To ensure that all stakeholders handle cyber security matters in a reasonable way, it is important to ensure diverse representation within decision making bodies.

AGENDA

10:00 am to 11:00 am Introduction and Presentation of the Brief
11:30 am to 1:30 pm Brainstorming session (ideation and suggestions from participants for keywords)
1:30 pm to 2:30 pm Lunch
2:30 pm to 5:30 pm Breakaway session in groups (creation of draft illustrations)