THE CENTRE FOR internet & society

Roundtable: Cyber-security & Private Sector

Concept Note

October 17, 2018

Omidyar Network Office,
Bangalore

BACKGROUND

An increased proliferation of cyber attacks from multiple vectors and a variety of actors has necessitated a multi-stakeholder response to cybersecurity that requires private sector involvement-both at the policy and technical fields.. This contribution has come in the recent past not only through active involvement at the domestic levels but also through norm-setting in the international arena. This symposium seeks to discuss the various cyber-security concerns in the Indian private sector and maps initiatives being undertaken by various actors towards furthering cyber-security in an attempt to identify challenges,points of tension, brainstorm solutions-thereby mapping the way forward through engagement not only with private sector actors but also in dialogue with civil society and policy-makers. CIS has undertaken some preliminary research in this area to further discussion in this area and serve as a forum for sharing perspectives for various stakeholders.

The symposium will be divided into three sessions,broadly in the form of a round-table with different modus operandi in each session.

SESSION 1

Scoping: Offensive and Defensive Capabilities in Cyberspace

This session will map various defensive and offensive measures undertaken by private sector actors, The format of the session will be in a round-table format where the discussants will share insight from their organisations' experience with cybersecurity measures.

CIS's research suggests that all cyber operations undertaken by the private sector cannot be painted with one brush and need to be graded on a spectrum that would clearly demarcate actions that fit within a common understanding of what constitutes ACD. In order to arrive at the spectrum of active cyber defense, we must first define its perimeters and establish a dividing line between measures that fall within the binary categories of 'active' and 'passive cyber defense.' Activities that produce effects only within the defendant's network may be termed 'passive cyber defense.' To qualify within the spectrum of active cyber defense, the operation must, at least partially infiltrate external networks - belonging either to adversaries or proxy networks being utilised by adversaries. Paul Rosenzweig has drafted a comprehensive typology of ACD measures based on the nature of effects the measures could have on information infrastructure—including observation, access, disruption, and destruction. The Centre for Homeland Security at George Washington University (CHSGWU) has based its spectrum of cyber defense tactics based on the intent of the actor implementing them. For example, the use of tarpits, sandboxes and honeypots which are technical tools that prevent the hacker from entering a network's perimeter are on the defensive end of the spectrum. On the other hand, among others, the use of hacking tools to infiltrate the adversary's networks and recover stolen information would fall within the offensive end of the ACD spectrum."

This session will be conducted in two halves separated by a coffee break.

SESSION 2

Conceptions of cyber-security

Economic approaches: Are there financial best practices and measures that the financial sector can incorporate into their strategy in order to improve or mitigate damage caused by cyber-security? Topics of focus include: (1) Scoping existing literature and measures on the economics of cyber-security, (2) Cyber-security insurance in India (3) High-level regulatory options in this space.

Rights-based approaches: Cybersecurity should be an all-encompassing project that involves not only top-down approaches that safeguard against attack vectors but also the creation of an atmosphere of trust and feeling of being secure when operating in cyberspace. A rights-based approach to cyber-security would examine the practices being implemented by both the private sector and government entities in fostering this atmosphere of trust-by safeguarding privacy, freedom of expression and other human rights in this sphere.

SESSION 3

Private Sector Perspectives on Data Localisation

Since a range of proposed policies and statutes have proposed data localisation as a means of safeguarding access to data and cementing the rule of law in cyberspace, public debate has raged on the efficacy of this measure. The purpose of this session would be to gather private sector perspectives on this issue and debate whether we have adequate capacity-legal and technological to usher in this new regime.

SESSION 4

Emerging Technologies and their Use in Devising Cyber-Security Practices

There are various technical vectors that can improve cybersecurity across organisations. This session will focus on the role of blockchain and Artificial Intelligence (AI) in improving cybersecurity standards. Discussion would focus both on the technical and legal/policy ecosystem. The format of this session would be different from the first session, in the sense that it would be lead by two presentations that are then commented on by discussants at the round-table.
