CyFy 2017 Draft Panels

1. Cyber Security Incident Reporting

Debilitating cyber-attacks against the private sector have led to increased demands for reporting cyber incidents and disclosing data to national CERTs, understandably in particular for companies active in the critical infrastructure space. This has complicated efforts to protect the privacy and raised concerns that governments may leverage knowledge gained from incident reporting to further their strategic interests. The question that then arises is whether incident reporting mitigates cyber risks or leaves systems more vulnerable. This panel will discuss how the public-private cooperation on information sharing must reflect the multiplicity of actors, interests and capabilities in cyberspace.

2. Digital Geneva Convention

Earlier this year Microsoft proposed a Digital Geneva Convention (DGC) to ensure that states and the private sector commit to protecting users from nation-state attacks during times of peace. The DGC sought a commitment from the private sector to support online defence, an establishment of an independent attribution organization to investigate significant cyberattacks, as well as a call for governments to come together to preserve the stability of cyberspace. This panel will discuss what such a regime would look like, the path towards it and in particular, what role and responsibilities emerging nations could play.

3. Cyber Security of Payments Systems and Gateways

Consumers using digital payment methods face risks pertaining to data security and privacy at multiple stages of the transaction. The cyber insecurity combined with the proliferation of cheap smartphones in the market and the availability of a universal ID in India (Aadhaar) represents an additional point of vulnerability in the user. This panel will ideate solutions for how 'single points of failure' within different payment networks can be identified and ring-fenced. It will also discuss steps that can be taken to harmonise regulatory systems in place to protect the digital payments ecosystem.

4. Cloud Computing

Cloud computing has become so core to modern economy that companies that do not rely on it for its cost benefits, big data insights and innovation, risk being left behind. Its increasing ubiquity is forcing regulators worldwide into a rethink of rules relating to data, whether they relate to privacy, confidentiality, security or sovereignty. It also throws up complex questions around the ownership of data and accessing it for law enforcement investigations. This panel will look at how governments in emerging economies can use their powers to encourage secure cloud adoption, either by adopting cloud first policies or/and adopting modern data classification frameworks, thus giving their local economies much needed additional impetus for growth.

5. Encryption

The economic argument for encryption is powerful yet understated. It is a crucial technology for preserving the integrity of communications, protecting user privacy and also the commercial veins of the digital ecosystem. Many cloud service providers and device manufacturers are enabling the encryption of user data to protect themselves and their users. This development raises significant concerns among law enforcement and intelligence officials that the spread of strong encryption will reduce their ability to anticipate, prevent or investigate serious crimes, terrorist activities and military threats. The panel will examine the trade-offs between information security and legitimate government access.

6. Digital Westphalia

The Westphalian system has struggled with the reality that most online interactions involve multiple jurisdictions, based upon the physical locations of users, servers, Internet platforms and TLD operators. It is perhaps time to conceive a new Digital Westphalia where non-state entities are assigned roles and responsibilities of these actors are clearly defined to reflect their current avatar as primary suppliers of the digital infrastructure upon which cyberspace is founded.

7. Gender in Tech

Technology promises to unshackle identities and communities that have traditionally been marginalised. But how have sites that incubate technology responded to the real and pressing problem of gender inequality? This panel will assess if technology giants and startups, themselves evangelists for a better world, have promoted the same ethos and sensitivity that their technologies promise. Technologies aimed at tackling gender-based violence have often led to the creation of a parallel internet for women, affecting their accessibility and engagement online. Panellists will examine whether these technologies have been successful or have ended up deepening pre-existing inequities.

8. Future of Work

With its non-physical nature of workplaces, cyberspace offers individuals from diverse backgrounds an opportunity to collaborate and innovate. In an increasingly globalized world, it is no longer enough to imagine discrete hubs where these innovations arise. States will need to adopt regulations for relaxing borders so that data can flow and innovation can truly flourish. And yet, these regulations must be imagined in a manner that does not allow for the dilution of the economic potential of cyberspace.

9. Countering Violent Extremism in South Asia

In the midst of a global war on terror, the effectiveness of conventional 'use of force' approaches have often been called into question. Cyberspace is the primary theatre of the war for hearts and minds which is a critical element of this conflict. South Asia is centrally implicated in this conversation on radicalization, given the hotbed of radicalization in its immediate neighbourhood. If violent extremism is to be systemically eliminated, then the means through which radicalization occurs must be addressed. Can online radicalization be neutralised by scripting narratives that combat divisiveness and violence?

10. Capacity Building for Tackling Cyber Crime

A deficiency in evidence-based cyber security research and capacity building has made emerging nations an attractive destination for cyber criminals. The panel will identify specific challenges that cyberspace poses in maintenance of law and order and suggest methods to leverage existing cyber security capabilities to meet these challenges. It will identify international best practices and examine the need for a new framework that will serve as a blueprint for policymaking in the area.

11. Fourth Industrial Revolution

The world as we know it is transforming, fuelled in a large part by technology and advancements in science. From biotechnology in Asia to AI in Silicon Valley, technologies are creating ripple effects that impact societies and their institutions in addition to their economies. How will these technologies transform the ways in which we live, work and interact with one another?

12. Militarisation of Cyberspace

With more countries absorbing and integrating “cyber” capabilities into their instruments of warfare, cyber deterrence is slated to become a central pillar of military planning. This panel will take stock of watershed military events and cyber-attacks in recent years, whether their frequency has contributed to an “arms race” and what new national security doctrines mean for regional and global stability. It will also examine the impacts of these developments not only in the stability of cyberspace but trust in the online environment and globalisation of technologies.

13. Emerging Regime on Lethal Autonomous Weapons Systems

In 2016, the High Contracting Parties to the Convention on Certain Conventional Weapons set up a Group of Governmental Experts (GGE) to study the international policy and military consequences of the use of Lethal Autonomous Weapons Systems. This panel, featuring GGE representatives, will assess the emerging regime for LAWs, their linkages to existing non-proliferation or export control architectures and finally, the consequences for widespread adoption of "autonomous" technologies in warfare for Asia.

14. The Future is shared

Digital transformation is dramatically changing the way we live and work. As industries transform through innovation, new business models are emerging, disrupting the established status quo. Examples are countless, from Ola, Uber (in transportation), Oyo, Air BNB (in housing), sharing of spectrum and infra in telecom, sharing of data centres in IT. These changes can be positive, as they improve the management of increasingly scarce resources; however are also introducing new labour models and putting a strain on governments trying to deal with a looming unemployment crisis, resulting from ever increasing automation. In an age where assets are no longer owned but shared, what regulatory challenges are likely to emerge?

15. Security: Anonymity v. Identity

As countries digitise their economies, as well as develop new, internet-based economic activities, they increasingly rely on technology for value and wealth creation. As a result, securing the digital ecosystem and enhancing user confidence become critical goals. While emerging markets have moved towards greater regulatory protection for their ICT networks, "digital identity" programmes for efficient targeting and disbursement of services also lure them. Using India's Unique Identity (UID) initiative as a case study, this panel will weigh the twin objectives of security and identity-based e-governance, and their recurrent clash that makes policymaking difficult for the digital economy.

16. Development Partnerships for Cyber Capacity

Capacity building initiatives in cyberspace are reliant on ever-changing dynamics of foreign policy postures and priorities of resource allocation. This panel will explore if existing development partnerships can be adapted for cyber capacity building in the emerging world. Traditionally, cyber capacity building has been restricted to public sector efforts due to the sensitive nature of the medium. How can both public enterprises as well as private technology companies share expertise and best practices on cyber capacity building?