Program

The structure of the workshop will be fully participatory for each session. We will ask several participants to take the lead in some panels, and to present the main challenges or comment on certain background materials.

The panels will focus on the following themes:

1. Should there be limits on use of Active Cyber Defense measures used by the private sector?
2. Cyber protection of individuals and small businesses
3. Protecting against attacks on the political system
4. Cybersecurity and Surveillance: the public/private interface
5. Encryption policy and legitimate hacking

1. THE USE OF CYBER ACTIVE DEFENSE BY THE PRIVATE SECTOR

Should there be any ethical/regulatory limits on the use of cyber security measures by the private sector?

Cyber-security measures used by the private sector can be responsive (ex-post) or defensive (ex-ante). Still, some measures might also be proactive. Increasingly, companies are taking a proactive (or preventive) approach, seeking to reduce cyber threats to begin with. This approach may not only cause damage to the attacker but also involve collateral risks to third parties, such as intrusion of privacy and damage to data and systems. Recently Microsoft President Brad Smith called for a new Digital Geneva Convention. This convention, he argues, should be led by IT companies, which would undertake to restrain the use of cyber technology and pressure governments to implement norms that would protect civilians.

- What liabilities might be involved in developing and using active cyber defense? Should companies be free to develop and use such measures?
- What are the roles and responsibilities of the cyber industry in setting limits on the use of cyber-security measures?
- Should IT companies self-restrain the use of cyber technology? Is self-regulation sufficient? Should regulation make room for ethical restriction imposed by industry?
- Can we envision a cyber-equivalent of Green Technology (e.g., Green Cyber Technology?)

- What alternative institutions, processes, frameworks can offer better oversight, accountability, liability, and remedy of cyber defense practices?

2. CYBER PROTECTION OF INDIVIDUALS ANS SMALL BUSINESS

How to protect civilians against cyber attacks?

In many countries governmental cyber-security policy involves securing both the governmental system and critical infrastructure, but the role and responsibility of governments in the protection of individual civilians is yet to be developed. There is little discussion on the protection of individual users, microbusiness and civil society organizations. Cyber-security issues pertaining to civilians raise a whole new set of challenges: inadequate protection for civilians (and by civilians) using a variety of home and small-business applications, devices, platforms and social networks may create critical vulnerability—which is widespread and more difficult to address. Individuals may often lack the resources and expertise necessary to minimize risk and address attacks as they occur. Some solutions (e.g., a security shield offered by the state) may lack sufficient safeguards to privacy, and may carry potentially harmful economic ramifications (e.g., cost, innovation, competition).

- What should be the role and responsibility of the different stakeholders: government, industry and civil society, in protecting civilians?
- Can markets take care of it? What forms of market failures might unfold? Should governments intervene? And if so, how?
- What regulatory schemes, policy measures, or technological solutions might be available in this context?
- How may we ensure that efforts will respect human rights and the rule of law?
- How may civilians' literacy and resilience to cyberattack be enhanced, and risks to civil liberties and cyber markets be minimized?
- Should there be an equivalent 911 for cyber security emergencies? Or an "iron shield" designed to protect civilians and small businesses?

3. CYBER ATTACKS ON THE POLITICAL SYSTEM

There are growing cyber security concerns involving potential hacking of the political system by state actors. Cyber attacks on campaigns, political parties and elections are threatening the stability of democracies worldwide. Taking action against these types of measures may involve unprecedented challenges for freedom of speech and commercial practices.

- How should countries protect themselves against these types of attacks?
- Is there a way to distinguish legitimate commercial speech (e.g. advertising) and political campaigns from illegitimate hacking of public discourse?
- What are the boundaries of legitimate attempts to influence public opinion and illegitimate hacking of the political process?
- What might be the role of the IT sector (e.g., social media) in monitoring and addressing such attempts?

4. CYBER SECURITY ANS SURVEILLANCE: THE PUBLIC/PRIVATE INTERFACE

How to reconcile surveillance and cybersecurity needs and improve the public/private interface?

Cybersecurity and surveillance are apparently pulling in contradictory directions. On the one hand companies and governments seek strong measures to protect the IT infrastructure, their proprietary data, and the personal data of their employees or customers. On the other hand governments and companies often require surveillance and data analytics to ensure cyber security and national security, as well as to lay bare fraud and crime. Strong cybersecurity measures may compromise surveillance by state agencies and create impediments.

IT companies are well placed to enable surveillance and access to data, of their systems and products. Yet, in the post-Snowden era, which undermined public trust in private/public collaboration, some leading companies now seek to retain consumers' trust by taking a strong stance against governmental surveillance. Microsoft's position disputing the authority of the US law enforcement agencies to access data stored outside the US is but one illustration. At the same time, IT companies may depend on collaboration with the government in identifying

vulnerabilities and addressing cyber risks. The recent WannaCrypt attack, which has targeted a vulnerability in Windows and was allegedly stolen from the NSA, demonstrates the contradictory interests in this ecosystem.

The private sector is situated in the midst of this conflict. Companies are unsure as to their best response: cooperate with the government or push back and strive to carve out their own responses. Governments are reluctant to report vulnerabilities to vendors, and contemplate various regulatory responses. Is there another way to address these challenges?

- Which models of cyber collaboration best serve industry and national security?
- What existing principles and instruments should govern corporate responsibility in the context of cyber security and human rights?
- What alternative institutions and processes can offer better coordination and oversight?
- Can we envision new forms of interventions, to ensure the rule of law without compromising the effectiveness of cyber-security measures?
- In this environment of public/private collaboration, how to safeguard civil liberties?

5. ENCRYPTION POLICY AND LEGITIMATE HACKING

Is it time to reconsider regulation of encryption?

Strong encryption is vital for safeguarding essential economic interests, protecting national security and ensuring human rights and civil liberties. Yet encryption may also be used for hostile and criminal activities. Strong encryption may create barriers to law enforcement and national security agencies in their effort to monitor illegal activities to protect security and safety.

Governments are tackling this challenge with a variety of legal and technological strategies, using different techniques (e.g., back doors and key escrow, or promoting weaker standards in standard-setting bodies). In tandem, the industry is struggling to develop its own set of responses to decryption by competitors and state agencies.

The debates on the optimal tradeoff in crypto policy are now resurfacing, as regulators around the world call on companies to avoid cryptography that cannot be

decrypted for law enforcement purposes. There are several regulatory initiatives to mandate exceptional access mechanisms.

A related issue is the attempt to control export of cyber-security technologies for national security purposes. The Wassenaar Arrangement seeks to set some limits on the export and dissemination of dual-use technologies. What new challenges are introduced by the newly emerging crypto debate?

- The crypto wars have been fought in the past. What is new about this round?
- What are the benefits and detriments of strong encryption on civil rights (privacy, free expression) economic interests, and national security?
- Should encryption be regulated? Are there alternatives beyond regulation?
- What governmental strategies are legitimate and useful?
- What is the role of industry in setting encryption standards? Should industry be held accountable for using weak encryption standards?
- What are the technical implications of some of the policy proposals? How are they likely to shape the encryption design?
- How can cryptography researchers contribute to addressing these tradeoffs in a different way?
- Is the Wassenaar Arrangement adequate? What are other tools or forms of intervention that can reconcile national security, foreign relations and innovation in cyber?