03

ROLES AND RESPONSIBILITIES OF DIFFERENT ACTORS IN CYBERSECURITY

DR. MYRIAM DUNN CAVELTY, HEAD OF THE NEW RISK RESEARCH UNIT
AT THE CENTER FOR SECURITY STUDIES, ETH ZURICH

INTRODUCTION

To continue to respond to cyber threats and other challenges of the digital age, international cooperation is indispensable. GCCS2015 aims to strengthen and extend international security alliances by involving all relevant stakeholders, including private sector actors and civil society groups, in the search for lasting solutions to current and future cyber challenges.

Understanding different expectations and positions (in various geographical contexts) is important for fruitful multistakeholder interaction. However, when looking at the complex issue of cybersecurity and related topics, what type of actors have traditionally had what kind of roles and responsibilities? How have expectations about them changed over the years? And what would an optimal distribution of responsibilities look like from a civil society perspective? From many possible focal points, this webinar will pick the area of cybersecurity as its main case study. In the Q&A section, there will be time to discuss the particularities of other cyber issue areas if the participants wish to do so.

THE WHAT – WHAT IS THE TOPIC ABOUT?

Cyberspace is a domain decisively shaped by non-state (private) actors. This has important implications for cybersecurity: In contrast to many other security issues, private actors are not the ones that are pushing into traditional (state) security fields – it is the state that is currently trying to (re)establish its authority in a space cultivated by innovative practices of companies and consumers on the one hand and criminal actors on the other side. This is shaking up long-standing power relationships.

Expectations about the roles and responsibilities (self-assigned or with regard to other actors) are not always aligned with the expectations of others. Resulting socio-political conflicts are symptomatic for an issue that mobilises different stakeholders from different sectors with divergent interests and are an expression of the struggle over influence at the same time. Analysing the context of the different positions will help us understand both the history of cybersecurity but also what is needed for the future. Ultimately, only a careful mapping of expectations and interests will help us identify potential common ground.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

Cyberspace does not belong to only one type of actor. It is a space/place in which many different stakeholders do many different things at the same time. Very often, this is unproblematic. But there are certain issues that have led to considerable tensions between stakeholders. Especially in recent years, security has become a defining driver in reshuffling tacitly accepted power-relationships.

Security means different things for different people and in cyberspace as in the real world, questions over how much security should be produced for whom and at what price are endemic to this issue. If we look at how social entities with power (mainly states and big corporations) shape the cyberdomain, including the (physical) information environment by specific security-related practices, we see how the focus on the state and 'its' security crowds out consideration for the security of the individual citizen. In other words, the type of security that is currently produced is often not security relevant to the people. That way, a problem for human security is created.

THE WHO – WHO ARE THE MAIN PLAYERS?

We will focus on three main groups of actors (but will not treat them as monolithic blocks). Input from the participants will assure that different geographical contexts are given sufficient weight.

- We focus on (different types of) states. However, we will also break up this black box to look at how different bureaucratic units within the state have sometimes quite fundamentally different ideas about roles and responsibilities (law enforcement, regulators, military, and intelligence community), which considerable impact on cybersecurity issues.

- We focus on (different elements of) the private sector. Here, we will look at different types of companies and their role. For example, there are companies who are part of the cyber-infrastructure, often companies that substantially shape the way human beings interact online. Also, there are companies not directly connected to cyberspace, but implicated by cybersecurity because they are considered as owning or operating "critical infrastructures". Both types of private sector actors assume different roles and responsibilities.

- We focus on citizens and civil society groups. We will look at how recent cybersecurity developments are impacting on our lives and we will ask ourselves who is implicated in what way by the links that exist between the international security dimensions of ICTs on the one hand, and technical, human rights, development and governance issues on the other. The How – how is this topic being addressed?

To structure the session, we will first put the state at the centre and look at its past and current relationships to the other two actor groups: the relationship between the state and the private sector on the one hand and the relationship between the state and civil society/individuals on the other. After this, we will briefly look at the relationship between the private sector and civil society.

What the state expects from the private sector and what the private sector expects from the state will be the first area we look at. On the one hand, one

of the key challenges from the view of the state arises from the privatisation and deregulation of many parts of the public sector since the 1980s and the globalisation processes of the 1990s, which have put a large part of the critical (information) infrastructure in the hands of private enterprise. This creates a situation in which market forces alone are not sufficient to provide security in most of the critical 'sectors'. At the same time, the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is a flawed and undesirable option, because the same infrastructures that the state aims to protect due to national security considerations are also the foundation of the competitiveness and prosperity of a nation.

The second area we focus on is the relationship between the state and civil society. Very often, the focus on the state and 'its' security crowds out consideration for the security of the individual citizen, not least because more security often means less freedom/liberties. In other words, the type of security that is currently produced is often not security (directly) relevant to the people. That way, a problem for human security is created, which consists of both a sustained feeling of insecurity, insecurities in the form of (material) vulnerabilities in the infosphere, and exploitation of these insecurities by several political actors.

The third area is the interesting relationship between private companies and civil society, which is the least understood of the three blocks. For example, Big Data is considered the key IT trend of the future, and companies want to use the masses of data that we produce every day to tailor their marketing strategies through personalised advertising and prediction of future consumer behaviour. What are the security implications of that? What expectations do we have?

THE WHERE AND WHEN – WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Roles and responsibilities (both self-assigned and expected from others) are a cross-cutting issue in all cyber policy fields. Developing sensitivity to the different expectations and positions can help us understand policy processes. In addition, it will help us understand where civil society input might be warranted: Given the range of legitimacy and normative concerns as well as the technical issues involved in security matters, even deeper engagement of civil society than in other areas seems desirable.