Session A4

Dual-use in a digital world

Chair: Jurriën Hamer (Rathenau Institute)

A ´technological race´ is developing between several global players around strategic key technologies such as automation, artificial intelligence and robotics. This is not purely a civil research agenda, as technological supremacy is considered a strategic goal for both economic and military power. As a result, military and security interests are increasingly shaping the relationship between science, technology and society. They deserve a wide public and political debate in order to arrive at a though-out and democratic decision making about science and technology in society.

The aim of this session is to identify the breadth and depth of this emerging agenda. This session therefore invites a wide variety of contributions including ***among others*** the following topics:

- Digitalisation raises new questions about dual-use technologies, i.e. products and technologies normally used for civilian purposes but which may have military applications. Current dual-use procedures and protocols are mainly designed around concerns for biological, chemical and nuclear science and technology. How do these apply to the digital technologies such as robotics and AI?
- Digitalisation has led to the emergence to cyberspace as a new domain for conflict and potentially even cyberwarfare. Given the emergence of offensive cyber technologies and the threat of escalation, how can governments contribute to sustainable cyber-peace?
- Digitalisation is increasingly blurring boundaries between military and civil R&D. This means that universities and public research institutes are, intended or unintended, involved in military-relevant R&D. Are there potential dangers of militarisation of universities and public research institutes? How can these concerns be addressed?
- The current race for technological supremacy in strategic fields such as AI is leading to geopolitical tensions in science and technology. This might put pressure on the ideal of a global and open academic community. How can the ideals of openness and internationalisation be sustained in light of rising geopolitical tensions?

The dual-use dimension of digital technologies is a relevant but often ignored topic by TA institutions and universities. The goal of this session is to facilitate an open discussion that can help to shape our thinking and understanding of the challenges at hand. The format of this session will be a short presentation by each contributor. All presenters will be asked to prepare a few statements in advance. After all presentations, the presenters will be asked to take part in a panel-discussion, where the prepared statements will be discussed in a plenary setting with the audience.

Towards a cyberspace without conflict

Author: Jurriën Hamer (Rathenau Institute)

A growing number of countries are capable of carrying out cyber-attacks that cause enormous damage to businesses, individuals and government institutions. Almost every country also uses cyber weapons. They spy on one another and try to infiltrate each other's digital systems; some states even engage in cyber sabotage or spread disinformation. A new type of conflict is being fought with information technology, which I refer to in this paper as an 'information conflict'.

This paper will explore the concept of an information conflict, and offer suggestions on tackling and de-escalating them. Concretely, this paper suggests five possible solutions:

1. Continue cooperating to increase international cyber security. Important international initiatives have been taken to improve the security of cyberspace, such as the IMPACT coalition, the European network of Cyber Emergency Incident Response Teams and the NATO cyber exercises. These collaborative efforts are and will remain very important.
2. Conclude clear international agreements on de-escalation in relation to cyber sabotage, disinformation and cyber espionage. Although the Netherlands and other countries have taken important steps to formulate international rules governing cyber-attacks, such as the Tallinn Manual and the Paris Call for Trust and Security in Cyberspace, there are very few binding rules that relate specifically to the information conflict. One option might be a cyber convention.
3. Ensure that the cyber arsenal is responsibly managed. It is important to prevent further proliferation of cyber weapons. That calls for international coordination of the build-up of cyber weapons and for effective collaboration with technology companies in removing vulnerabilities in their products. This collaboration also calls for as much transparency as possible, especially among allies.
4. Protect the independence of technology companies. Technology companies perform a crucial role in creating a secure digital environment. They close the holes in their software and can bring robust digital applications onto the market. It is important to help companies to make their operations as secure as possible. Governments are taking a risk if they insist that companies secretly weaken the security of their products. Governments must therefore regulate both the technology and technology companies in a sensible manner.
5. Invest in a debate on international cyber security. The information conflict must be subjected to a democratic debate: it is citizens who are particularly affected by cyber-attacks. Citizens thus must be resilient. It is also up to citizens to give direction to the digital future. De-escalation of the information conflict therefore calls for a public and political debate.

Dual-use by design? How ungoverned digital identification practices affect individual agency

Author: Stefan Strauß (Institute of Technology Assessment)

The development and use of digital technologies is driven by an increasingly indistinct mix of economic and security purposes. This can already be observed with the emergence of their core technology, i.e., the Internet: together with the MIT, the US Ministry of Defense played a leading role in the creation of its predecessor the ARPANET serving mainly military purposes. The Internet evidently became a global sociotechnical metasystem fostering freedom of information and democracy in many respects. However, at the same time accompanied by certain ambivalences regarding transparency and control over information processes with enormous impact on human rights and particularly privacy. This contribution ties in here and sheds light on a controversial key practice in a digitally networked society: the gathering and processing of information affecting individual identity. As will be shown, identification practices are closely linked to a complex and blurry conglomerate of political and economic interests in the realm of security. Actors involved can be described as a "surveillant assemblage" (Haggerty/Ericsson 2000) building a functional entity to use digital technology as political and economic instruments of control. This is discernable in a number of interrelated sociotechnical phenomena, particularly in the overlaps between big data, securitization and surveillance (Lyon 2014; Strauß 2018), as highlighted in social media platforms as well as in the emergence of digital identity

management systems. Several big data brokers have strategic partnerships with intelligence agencies; e.g., Palantir Technologies contributed to develop the NSA's surveillance tool "XKeyscore", inter alia categorizing users of privacy tools as "extremists" (Greenwald 2014; Doctrow 2014; Biddle 2017); database providers like Oracle and other firms with relations to the global intelligence community exploit consumer data to create identity graphs "including what people say, what they do and what they buy" (Oracle 2015); recent data scandals around Facebook/Cambridge Analytica highlight how privacy-intrusive exploitation of social media jeopardizes the legitimacy of democratic processes (Lewis/Hilder 2018) and automated scoring systems such as in China's so-called "social credit system" (Botsman 2017; Rollet 2018) alarmingly highlight how digital technology can be misused to establish panoptic, totalitarian power. Ultimately, all these practices involve identification mechanisms which are key in every digital technology. I thus argue that there is an increasing economization and securitization of digital identification entailing a privatization of privacy which together reinforce asymmetric power distributions and undermine individual agency (Strauß 2019). Consequently, increasing sociotechnical identifiablity is the ultimate core risk of privacy protection in the digital age. This contribution elaborates how and why this is the case and discusses potential approaches to improve privacy impact assessment with better standards for digital technology to tackle this and related ethical risks.

Dual-use of 5G technology

Authors: Urszula Soler (The John Paull II Catholic University of Lublin), Mariusz Busiło (The Polish Chamber of Information Technology and Telecommunications)

5G technology has in the recent years been put in the spotlight for both civil and military use, creating large expectations of society and technology advancements (smart cities, Internet of Things, autonomous transportation, distance medical treatment etc.), as well as being the tool for raising fears and fueling political and economic conflicts all over the globe. If not being overhyped the 5G technology promises so many revolutionary use cases that is automatically creates conflicts and a kind of tech-race in which the winner will develop and implement and control the technology underlying future services as well as the military battlefield. It is currently being named 'the new cold war on tech', which is currently fought between USA and China, where countries in Europe are being even called the 'collateral damage'. The war on tech is not a typical military conflict, but a conflict in which opponents try to outrun the other with development speed, advancement and coverage, as well as control of their technology, including the data it will generate. The current choices of the technology vendor will impact the future military alliances due to compatibility and trust issues.

In the presentation the authors describe basic use cases of the 5G technology and its impact on civil services as well as internal security and military systems. The analysis will cover sample benefits of the 5G technology, as well as the selected risks it causes. The authors will try to address selected areas of potential risks with necessary the self-regulatory and regulatory (forced) measures aimed to manage and limit the risks.