INTERVIEW

"There is virtually no political or military conflict these days that doesn't also have a significant cyber component"

The Center for Security Studies (CSS) at ETH Zurich is a centre of competence for Swiss and international security policy. Prof. Dr. Andreas Wenger is Director of the CSS and provides comprehensive information on trends relating to digital transformation in the context of Information Security.

Digitisation is steadily forging ahead. Looking back, which developments were particularly important from a security policy perspective?
The commercialisation of the Internet in the 1990s led to a sudden expansion of cyberspace. This was accompanied by a similarly rapid increase in the social and economic importance of technologies that had actually been created for a different purpose. However, it soon became clear that cyberspace was fundamentally insecure and that the market did not ensure adequate security. As a result, governments increasingly began to grapple with cyber crime and cyber sabotage. Initially, governments focused their efforts on prosecuting cyber crime and protecting critical infrastructure, although this, in turn, could only be guaranteed by working hand in hand with the private sector.

What new threats have come to the fore in recent years from a security policy perspective?
In the last few years, cyber conflicts have taken on a strongly political and military aspect. Since STUXNET, i.e. the malware attacks on monitoring and control systems in the context of Iran's nuclear programme in 2010, the sabotage of critical infrastructure using cyberattacks is no longer a fictional scenario. The Arab Spring of the same year demonstrated that both public protest and state repression now increasingly take place over the Internet. The Snowden affair of 2013 underlined how widespread the practice of state espionage has become in cyberspace. The war in Ukraine in 2014 made it clear that cyberattacks are now an integral part of operations by armed forces and intelligence services. In parallel to this, the rise of Islamic State in Syria and Iraq in 2014 highlighted that non-state groups also make active use of cyberspace for recruitment, financing, communication and propaganda. In short, there is virtually no political or military conflict these days that doesn't also have a significant cyber component.

How is digitisation changing the power political map?
That probably won't be clear for a few years yet. What is clear, however, is that there has been a wholesale increase in the opportunities to exert power by manipulating information. This is partly because it is difficult, both in a technical sense and in terms of criminal law, to attribute attacks conclusively to specific sources. In the last few months, however, attempts by states to influence elections in Western countries have shown that the strategic effects of propaganda and counter-propaganda are hard to control. Although cyber technologies are cheap and can also be used by non-state actors to exert asymmetric influence, hacking has not undermined the traditional power structures as the great powers, in particular, are massively expanding their cyber capabilities. States that are significantly inferior to other states in terms of conventional power projection are increasingly relying on cyberattacks in order to gain information superiority, at least in localised conflicts.

How are governments adapting their security strategy to these changes?
The subject of cyber warfare has, without doubt, become a top priority for global security policy. Cyberspace is extensively integrated into the existing deterrent and defence systems. Among other things, this means that governments are establishing a legal framework for the offensive and defensive use of cyber capabilities, building up additional operational capabilities in both civilian and military applications, and creating new organisational structures and command centres. Although very little reliable data is available, it can be assumed that spending has risen sharply in these areas within both the secret services and the armed forces. Great efforts are also being made in the area of Information Security and in promoting digital literacy for all users.

What do these developments mean for multinational cooperation?
The fight against cyber crime calls for joint solutions as this is a global problem that affects everyone. Institutions such as the UN, Interpol or the Council of Europe are seeking to harmonise legislation in relation to prosecuting cyber crime. The area of cyber conflict has a more complicated starting position as states have very different interests from a power politics standpoint. The greatest progress has been made in discussions conducted within the NATO alliance aimed at applying the law of armed conflict with regard to cyber operations. However, it is often hard to define what should be considered a cyber weapon because the line between war and peace, internal and external security, political and criminal motives, and state and non-state actors becomes blurred in cyberspace.

Will we see a digital arms race in the years ahead?
If you believe all the rhetoric about building up cyber command centres, spending in this area is increasing everywhere you look. What we do know for sure is that modern armed forces see cyberspace as an operational dimension in its own right and are looking at structuring the tasks and processes in this area of operations. At the same time, the cyber dimension is closely linked to the dimensions of land, air, sea and space. Ultimately, that also means you have to assess the armament process from all angles. In the cyber sphere, there is particular uncertainty as to whether investment should be made primarily in offensive or defensive capabilities. Given the nature of the problem, this uncertainty is unlikely to be resolved any time

Prof. Dr. Andreas Wenger has been Professor of International and Swiss Security Policy at ETH Zurich since 2003. He is Director of the Center for Security Studies (CSS), which forms part of the Center for Comparative and International Studies (CIS) of ETH Zurich and the University of Zurich.

soon. It is linked to the question of whether expanding the cyber realm contributes, on the whole, to a destabilisation of strategic relations between states.

> Cyber risks are multidimensional – accordingly, it is difficult to formulate a shared Security Architecture for the state, the economy and society.

Has the digital world become less secure, per se, and what are the consequences of this?
That's another tricky question, partly because insecurity is a matter of opinion and partly because the starting position for the argument is unclear. Is the world less secure today than during the Cold War? One cannot simply look at new vulnerabilities in cyberspace and conclude that "we" have become less secure. So far, there have been very few fatalities as a result of the digital world. However, both the phenomena of violence and the solutions to it are evolving in the context of digital transformation, requiring state actors to adapt their security policy strategies on an ongoing basis. For example, criminality has changed and is increasingly focusing on cyberspace. The decline in "normal" burglaries may be related to this or to greater investments in security, which might in turn be a manifestation of widespread feelings of insecurity. It is therefore also important to gain a better understanding of these connections.

What new risks has digitisation created from the point of view of Information Security?
The socio-technical context is changing both quickly and on a lasting basis. The key elements of this are more-mobile networking, the automation of industrial production, the network-based control of systems and equipment, and the resulting exponential growth in volumes of data (big data, cloud computing). This is associated with new vulnerabilities and growing challenges in terms of securing the entire value chain, bringing particular importance to various so-called critical sectors such as health, energy, finance, transport, or indeed defence. This process of digital transformation will also be associated with new challenges for security policy.

How should states, armed forces and intelligence services respond to this development?
Cyber risks are multidimensional – accordingly, it is difficult to formulate a shared Security Architecture for the state, the economy and society. Cyber security and cyber defence can only be ensured holistically and at a nationwide level. They necessitate technical, organisational, social, political and legal countermeasures. A comprehensive cyber protection strategy includes efforts in the areas of early identification, resilience, criminal prosecution, defence and governance. Until a few years ago, efforts in many countries were focused on civilian approaches and decentralised measures. In the course of the politicisation and militarisation of cyberspace, as mentioned earlier, increasing attention is now being paid to military approaches and questions of operational priorities. The key issue, with respect to a state's ability to act in cyberspace, is coordination between civilian and military bodies. However, cyber security is not simply an issue to be tackled at the national level; it is also vital to incorporate business and science and to cooperate on the international stage with regard to multifaceted cyber standards.

The Center for Security Studies (CSS) is a centre of competence for Swiss and international security policy at ETH Zurich.

Risks in the digital workplace

Digitisation is having an enormous impact on the world of work. This also applies to highly sensitive areas such as state institutions and organisations. Although this makes the workplace more agile and efficient, it also potentially makes it increasingly easier to access secret information. However, there are ways to protect against cyberattacks.

Some talk of a revolution. What we can say for certain is that digitisation is changing the world of work. Information technology is pushing forward into more and more areas, and the world is becoming increasingly interconnected. Although this creates opportunities, there are also dangers lurking beneath the surface: greater functionality and networking are giving rise to new threat scenarios.

In Diplomacy, for example, this has been clear for a long time. Communication relationships have changed dramatically, especially with regard to the internal communication between foreign ministries and embassy staff around the world. Here, information is exchanged internationally over public networks that also transmit top-secret data.

Digital Diplomacy
Ambassadors regularly inform their home country of events in their host country – usually in the form of daily and weekly reports. This exchange takes place primarily using state-of-the-art communication technologies. Nowadays, corresponding technologies are available that allow even highly classified data to be sent from a single device. This information is then forwarded, partly in filtered form, to other offices and archived in the data centre. These investigations pertain not only to matters of security but also to the image of a state, which is diminished by the activities of non-state actors on a increasingly frequent basis.