Technology & Security Politics

The 2010 malware attack Stuxnet on the Iranian nuclear programme, deepfake videos of Kamala Harris circulating during the run-up to the US elections, and Ukrainian energy infrastructure being destroyed by Russian cyber-attacks. All these examples are situated within a newly evolving field of security politics: technology and digitalisation. There are two fundamental consequences of digitalisation for security politics: Firstly, security politics now also take place within the digital space and, secondly, new techniques and instruments are brought into conventional security politics, changing its means and forms.

Security politics that take place in the digital space, or cyberspace, deal with different phenomena: Cyberwar, cyber-terrorism, cyber-espionage, or cybercrime – and, accordingly, different actors ranging from the military to police forces are involved. Cyberspace is often referred to as the fifth domain of military activity, next to land, sea, air, and space. That means that war and conflict within cyberspace have different characteristics than in the other domains. For example, in cyberspace, soldiers no longer see each other face to face.

In addition to this, because of digitalisation, means of military activities and security politics have changed. Two central novel techniques are automation and artificial intelligence (AI). Due to automation techniques, weapons today have become more autonomous – including, e.g., drones. AI has become important in international security politics where it is included in security-related decision-making or in biometric identification or surveillance by police forces. Particularly generative AI is used by states and non-state actors for propaganda and the spreading of (mis-) information, also in the context of armed conflict.

This digitalisation of warfare and security politics adds ethical and practical questions that need to be addressed by security policy.

Firstly, both armed conflict taking place in cyberspace and new means of conflict blur the line between military and civilian spaces. Most cyberattacks do not attack military cyber infrastructure, but the general infrastructure of states, often critical infrastructure. Thus, it is likely that cyberattacks will impact civilians more than attacks in the other four domains of military activity – which requires, among others, new regulation and new forms of defence.

Secondly, digitalisation makes attribution of military acts more difficult. If a group attacks through cyberspace, it is more complicated to attribute this deed to the group than, e.g., if this groups attacks by airplane. Similarly, if AI supported autonomous weapon systems decide to shoot a soldier of another country, there is no rule in international law that decides whether this was an attack by the state or not. This then raises questions of responsibility and accountability.

Thirdly, ethical questions become important when using these new technologies. Should machines have the power to decide over life and death? Would their lack of empathy undermine the principle of human dignity? And do machines necessarily make better decisions, especially if they might act in a biased manner or hallucinate?

Future political action, be it at the EU, the UN, or the Munich Security Conference, will need to address questions such as:

- Is unlimited digitalisation within security politics desired? If not, how can it be limited?
- How do rules of conflict and defence capacities need to be adapted?

Important specialist terminology

Malware is a malicious software designed to cause harm or damage to a computer, sever, client, or computer network.

Autonomous weapons are any weapons that select and apply force to targets without human intervention or only little human oversight (ICRC).

Generative AI is a type of AI that can generate new content, here, e.g., videos or audios from training material.

Critical infrastructure encompasses physical and cyber systems vital to a nation, whose incapacity or destruction would severely impact physical and/or economic security, as well as safety (DIIS).

A civilian is a person who is neither member of state armed forces nor member of an organised armed group (ICRC).