The Challenge of Digitalisation – the Bundeswehr Cyber and Information Domain Service

By Jürgen Setzer

GenMaj Jürgen Setzer, Vice Chief of the Cyber- and Information Domain Service and Chief Information Security Officer of the Bundeswehr

Digitalisation offers tremendous opportunities for science, economy, government and civil society and thus for each and every one of us living in democratic and liberal societies.

At the same time, however, it also provides enormous opportunities for potential enemies – be they criminals, terrorists or state actors – and thus involves considerable dangers to our society. The possibilities of digitalisation have given rise to a new form of conflict, for which we need to prepare. Cyber attacks on states and their critical infrastructure as well as business enterprises and private households have already become reality. From a technical point of view, future conflict scenarios will be characterised by digitalisation, artificial intelligence and automation.

Besides attacks from cyberspace, activities intended to manipulate or influence opinion, such as fake news campaigns and disinformation, have become all too common. Therefore, the inclusion of the information domain is of particular importance. Consequently, both cyber and information space are of vital importance when it comes to national security and thus the military.

As early as 2016, at the summit in Warsaw, NATO recognised cyberspace as a military domain in its own right – much like the domains of land, air, sea and space. Armed forces can both reconnoitre and engage enemy systems in cyberspace. In practical terms, this could involve, for example, the interruption of logistic chains or the modification of data crucial to enemy operations. Paralysing C2 and information systems would also be an option.

In the Bundeswehr, we have deliberately chosen a broader definition of this new military dimension – one that includes the above-mentioned information domain as well as its central aspect: information. Information is perceived, interpreted and disseminated by human beings. Hence, what is called “published opinion” constitutes an essential part of the information domain.

The new cyber and information domain is characterised by a high level of complexity. Territoriality is complemented by virtual reality. Cyber and information space cannot be divided into traditional combat sectors with clear spatial boundaries.

Contrary to classic kinetic operations, cyber operations can also achieve the desired effects by non-lethal means or for a limited period of time. Nevertheless, physical effects can be achieved in cyberspace, too. Moreover, the place where cyber operations create an effect can theoretically be tens of thousands of kilometres away from where the action was initiated. Time, too, plays a different role in cyber and information space. An effect can be achieved over any distance almost without delay. Hence, effects are achieved in real time.

Against this backdrop, the Bundeswehr established its new Cyber and Information Domain Service on 1 April 2017. Thus, the importance of this new domain is now reflected in our organisational structure.

As the Cyber and Information Domain Service was established, its main tasks were defined. These tasks are considerably more comprehensive than the commonly used shorthand description “cyber” may suggest. The Cyber and Information Domain Service is in charge of protecting and operating the Bundeswehr IT system in Germany and on operations abroad. In addition, the Cyber and Information Domain Service is also responsible for military intelligence and provides situation information in the form of thoroughly evaluated reconnaissance results. We can access enemy IT networks to gather or manipulate information and employ electronic warfare capabilities to ensure the safety of own and friendly units on missions abroad. The Bundeswehr Geoinformation Centre provides each user with individual geo-referenced information – from weather forecasts and soil conditions to digital 3D terrain models.

The Cyber and Information Domain Service has pooled the existing expertise in the Bundeswehr, established and developed additional capabilities and strengthened those areas that will be of particular importance in the future. At the command level, our Joint Cyber and Information Domain Situation Centre provides the Bundeswehr as well as other ministries with a fused situation picture of cyber and information space. As the responsibilities of the Cyber and Information Domain Service increased more and more, the Cyber Operations Centre was established in spring 2018. This agency pools the specific capabilities that are required in today’s world to prepare and conduct military cyber operations for the purpose of reconnaissance and effects. As a result, the Bundeswehr possesses an effective institution whose activities, taken also in cooperation with other actors, will significantly enhance Bundeswehr mission accomplishment in the age of digitalisation and hybrid warfare. This opens additional, non-kinetic courses of action for the military and political leadership and expands the range of suitable responses in crisis situations. The Bundeswehr Cyber Security Centre pools the cyber defence capabilities of the Bundeswehr. It is here that the Bundeswehr computer networks at home and abroad as well as in theatre are monitored 24/7. If cyber attacks are detected or critical IT security incidents occur, Bundeswehr computer emergency response teams restore IT security around the globe.

Cyberspace knows no borders. Hybrid strategies exploit interfaces between responsibilities, for instance internal and external security. Therefore, it is indispensable that we close ranks and share knowledge both at the national level – as part of an interagency approach in cooperation with enterprises, science and society – and at the international level.

Cooperation projects aimed at the mutual exchange of information, knowledge and personnel as well as the mutual opening of basic and advanced training programmes are essential when it comes to strengthening national resilience. In addition, an active exchange at the international level is vital. Attacks from cyberspace as well as campaigns on social media and messenger services do not stop at national borders. Their effects can be felt at the transnational level. International cooperation across national boundaries is absolutely imperative if we are to master these challenges successfully. In the military sector, close bilateral cooperation is already taking place at the EU and NATO level. Here, too, an effective contribution to national security must always be one of our goals.