Analyses OSW

CENTRE FOR EASTERN STUDIES 12.04.2017 www.osw.waw.pl

The Cyber and Information Space: a new formation in the Bundeswehr

Justyna Gotkowska

On 5 April a new organisational structure was formed as part of the Bundeswehr: the Cyber and Information Space (*Cyber-und Informationsraum*, CIR). It holds the same rank as the Joint Support Service and the Joint Medical Service, which function in parallel with the three branches of the armed forces (the Army, the Air Force and the Navy). The CIR will group together all the Bundeswehr structures dealing with IT, cyber-security, military reconnaissance and geo-information, as well as with psychological warfare. The CIR is designed to strengthen the protection of the Bundeswehr's computer networks and weapon systems, but also to develop capabilities for offensive actions in cyberspace.

The newly-created CIR Command will supervise the Strategic Reconnaissance Command, the IT Command and the Geoinformation Centre, as well as their subordinated units, which had all previously been part of the Joint Support Service. After the integration of all the above-mentioned units this year, the CIR should include around 14,000 civilian and military staff; there are plans for further expansion. The CIR's Inspector is Gen. Ludwig Leinhos, who from 2013 to 2016 was Director of the NHQC3S (NATO Headquarters Consultation, Command and Control Staff) at NATO Headquarters in Brussels.

The German Ministry of Defence also underwent a transformation related to the new emphasis on the areas of cybersecurity and IT. Since October 2016 the structures of the ministry have included a CIT (Cyber/IT) Department, which deals with the planning and implementation of the national cyber-security strategy in the defence sector, and is responsible for the cyber-security of the Bundeswehr's computer systems.

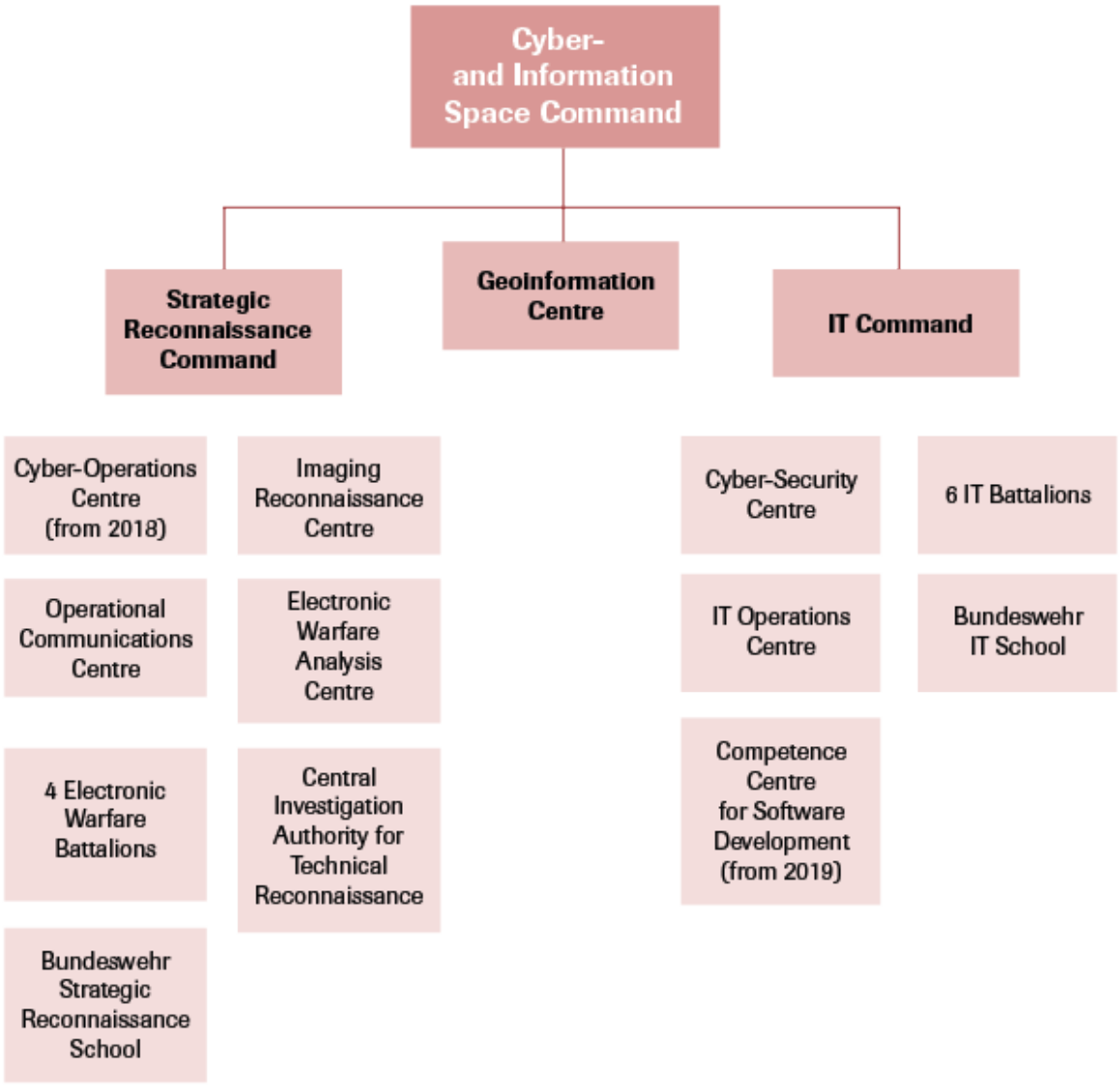
Commentary

- The creation of this new formation in the Bundeswehr shows that Germany is treating cyber- and IT issues as matters of increasing importance for the functioning of the Bundeswehr, national security and the future of warfare. This is also demonstrated by the White Paper on German Security Policy and the Future of the Bundeswehr from July 2016. Challenges from the cyber and information domain came second on the list of challenges for German security policy (after transnational terrorism). According to the defence minister's statements, in January/February this year alone the Bundeswehr was the target of more than 280,000 cyber-attacks. The creation of the CIR within the Bundeswehr also reflects trends within NATO; cyberspace was recognised as a part of

collective defence and the domain of operations at the Warsaw summit in July 2016.

- The creation of the CIR Command must also be seen as one of the projects which aim to improve the image of Ursula von der Leyen as an effective and modern defence minister. So far von der Leyen has focused on introducing new, more transparent and efficient procedures in the procurement of arms and military equipment for the armed forces, and on increasing the attractiveness of service in the Bundeswehr (by offering better opportunities to combine family life and work, etc.).
- Despite the media hype around the creation of the CIR, the new formation is mainly based on subordinating commands and units which already operated within the structures of the Bundeswehr (which in total number almost 14,000) to the new CIR Command. Until recently, the defensive and offensive cyber-capabilities were developed mainly by two units totalling each up to 60 people: the CERTBw (*Computer Emergency Response Team of the Bundeswehr*), which was created in 2002 and has handled computer security incidents; and the CNO (*Computer-Netzwerk-Operationen*) unit, subject to the Strategic Reconnaissance Command, which has carried out electronic warfare tasks. In the future, both units are to be expanded and transformed respectively into a Cyber-Security Centre and a Cyber-Operations Centre. According to media reports, the CNO first carried out a cyber-attack in 2015 (on the Afghan mobile network) as part of German efforts to release a German citizen who had been kidnapped in Afghanistan.
- The Bundeswehr has, and will continue to have, problems with expanding its defensive and offensive cyber-capabilities. The reason for this mainly lies in difficulties with employing IT professionals, connected with the competitive German market in this area and the general unpopularity of service in the military. The German Ministry of Defence is thus planning to open a new course in Cyber-Studies at the Bundeswehr University in Munich in 2018 in order to recruit new staff. In addition, in March this year the Inspector-General of the Bundeswehr published a concept for supporting a cyber-community in the military by encouraging cooperation with reservists and professionals hitherto unconnected with the armed forces.
- The creation of the CIR has galvanized discussion in Germany on whether parliamentary approval would be needed for the Bundeswehr to conduct cyber-attacks (the Bundestag needs to approve foreign deployments of the Bundeswehr). On the one hand, the possibility to use offensive cyber-capabilities will probably be included in the mandates for future foreign operations (e.g. in Africa or the Middle East) which the government will submit to the Bundestag. On the other hand, according to Ursula von der Leyen, the Bundeswehr should also be able to carry out 'offensive defence', that is, to conduct cyber-attacks countering aggressive cyber activities by third countries during peace-time if they undermine the Bundeswehr's combat readiness and ability to fulfil its tasks.

Annex: The structure of the Cyber and Information Space (*Cyber-und Informationsraum*, CIR) of the Bundeswehr


Cyber- and Information Space Command
Strategic Reconnaissance Command
GeoInformation Centre
IT Command
Cyber-Operations Centre (from 2018)
Operational Communications Centre
4 Electronic Warfare Battalions
Bundeswehr Strategic Reconnaissance School
Imaging Reconnaissance Centre
Electronic Warfare Analysis Centre
Central Investigation Authority for Technical Reconnaissance
Cyber-Security Centre
IT Operations Centre
Competence Centre for Software Development (from 2019)
6 IT Battalions
Bundeswehr IT School