Germany activates new cyber warfare unit

Johannes Stern
8 April 2017

On Wednesday, German Defence Minister Ursula von der Leyen officially commissioned the country's Cyber and Information Space Unit (KdoCIR). The new military command will form a separate part of the Bundeswehr (armed forces), along with the army, navy and air force. The unit is to be set up in two stages: its personnel currently totals 260, but is due to expand to 13,500 soldiers by July 1.

In future, the tasks of cyber warfare, information technology, strategic reconnaissance and geo-information systems of the Bundeswehr and operational communication will be placed under the central control of the KdoCIR.

The KdoCIR's first head of staff is Lieutenant General Ludwig Leinhos, a commander with a reputation as a "cyber warrior." Before being appointed head of Cyber and Information Space, he was responsible for cyber defence at NATO Headquarters in Brussels.

According to the *Süddeutsche Zeitung*, Germany is seeking to take the lead internationally in the field of cyber warfare and thereby position itself "for the warfare of the future."

Von der Leyen boasted at the launch of the unit: "Today's initiation of the cyber and information space command is more than a milestone for the Bundeswehr. This puts us in the top league internationally."

The last edition of the military newspaper *Bundeswehr* writes jubilantly in its editorial: "Within NATO, it [the Bundeswehr] is playing a pioneer role: even though allies like the United States have long recognized the military importance of digital space—they have not so far carried out the step of unifying all agencies under one roof."

Contrary to official propaganda, which declares that the new department is mainly responsible for "defence" against cyber-attacks—according to von der Leyen the computers of the Bundeswehr were already attacked more than 280,000 times this year—there can be no doubt that the Bundeswehr is gearing up for offensive cyber warfare.

Von der Leyen stated: "And to clarify one thing: If the networks of the Bundeswehr are attacked, then we can defend ourselves. As soon as an attack threatens the functioning and operational capacity of the armed forces, we can also defend ourselves offensively."

In the Bundeswehr's concluding report on cyber and information space states that "defensive and offensive abilities are always required to carry out effective cyber measures." Other states had also opted "to use the full range of military means against cyber-attacks in the context of deterrence." The "military relevance of the [cyber and information space] as its own dimension alongside land, air, sea and space" should therefore be "comprehensively taken into account."

The cyber war measures mentioned in the report, such as "espionage, information manipulation, possible cyber terrorist acts, and even large-scale sabotage attacks, for example in critical infrastructure," are new forms of devastating military warfare and the Bundeswehr is determined to play a leading role.

In her speech von der Leyen pointed out that the word "cyber" appeared "72 times" in the new Bundeswehr white paper, "purely numerically on every second page." This shows "graphically" how the topic of cyber and digitization will dominate the next decade," she said. There is "hardly any area in the Bundeswehr not affected by it. Whether in the sphere of logistics, mobility or communication in Germany, as in the application of almost all our weapon systems."

Von der Leyen instructed the troops assembled in Bonn on their global tasks: "Only as a team can you meet the challenges. And we can see that from now on you are a team because you all wear the same dark blue beret, with your own badge. The small globe in the badge stands for global intelligence gathering and

networking.”

In order to recruit, educate and send the necessary “cyber-soldiers” into battle, an international master’s program for CyberSafety has been established at the Bundeswehr University in Munich and a so-called “CyberInnovation Hub”—an “interface of research, science, economy and industry” is to be set up.

The costs reach into the billions. All in all, the current budget includes around €1.6 billion for all IT-related expenses. “For 2018, we are planning another significant increase. Additional personnel costs of just under one billion euros each year,” von der Leyen reported.

Officially, the massive expansion of cyber warfare capabilities by the Bundeswehr is justified by the “hybrid warfare” alleged to be carried out by Russia. In reality, it has been planned long in advance and is considered necessary by the ruling class to assert its economic and geostrategic interests in the 21st century using the most modern and aggressive military means.

In a lecture for the German Atlantic Society, the former general inspector of the army and chairman of the NATO Military Committee, Klaus Naumann, declared as early as 2008: “All in all, the 21st century promises to be a restless century in which along with conflicts and well-known forms of war between states, new forms of armed conflict such as cyber war and the struggle of transnational forces against states will take place.”

Since the official announcement of the return of German militarism at the Munich Security Conference in 2014, the German Defence Ministry has worked feverishly to set up its cyber command.

The build-up is supported by all of the parties represented in the German parliament. Hanspeter Bartels (Social Democratic Party, SPD), the German army representative in the Bundestag, said the new cyber unit was urgently needed. The unit makes clear that the German army “is not interested in half measures.” However, he continued, “the personnel demands of the new cyber command ... should not cannibalise the rest of the Bundeswehr. ... All its other forces also need IT specialists or telecommunication experts, as they used to be called.”

The Green Party had already supported the first cyber war operations by the army in the post-war history of Germany, as part of the Red-Green federal government led by Gerhard Schröder (SPD).

In the Kosovo War (1998-1999), NATO troops interfered with Serbian air defence using high-frequency microwave radiation, paralysed the Yugoslav telephone network and hacked into Russian, Greek and Cypriot banks to access the accounts of Serbian President Slobodan Milosevic.

With the German ruling class preparing for a new war offensive, the Left Party has also lined up behind the Bundeswehr’s cyber-offensive. In a comment in the *Tagesschau* on Wednesday, party chairman Dietmar Bartsch meekly asked “the federal government to present a concept aimed at respecting parliamentary participation rights.” After all, “the Bundeswehr is a parliamentary army and not the army of the federal government”.