German army prepares for cyberwar

Johannes Stern
2 May 2016

Germany's Bundeswehr (Armed Forces) are massively stepping up their capability in the field of electronic warfare. Last Tuesday, Defence Minister Ursula von der Leyen (CDU, Christian Democratic Union) issued a "general order" that provides for the establishment of a new and separate department in the defence ministry and the establishment of a military organization for cyberwar.

With an Inspector General at its head, the new unit will have the de facto status of a new service within the Bundeswehr. It will be led from a Cyber and Information Command (KdoCIR) in Bonn, with around 13,500 staff (unofficial figures already speak of up to 20,000 cyber warriors).

Its establishment will be carried out in two stages. According to the order of the day, "a new department Cyber/IT (CIT) will be established by the fourth quarter of 2016 with bases in Bonn and Berlin," and then "by the second quarter 2017, a new and sixth military unit for Cyber and Information Resources (CIR)."

According to the official defence ministry website, the aim is "to gather together the tasks of cyber, IT, military intelligence, geo-information and operative communications." The plans go back "to the work of an establishment team, which the minister had ordered last year to make the Bundeswehr future-proof in cyberspace." The team was led by Deputy Inspector General of the Bundeswehr, Lieutenant General Markus Kneip, and the Commissioner for Strategic Defence Control, Gundbert Scherf.

While von der Leyen is seeking to justify the establishment of the new cyber department by citing "the protection of Germany and its citizens," the official "final report on the Cyber and Information Resource" by Kneip and Scherf makes clear what is really at stake: the formation of a powerful department to conduct offensive cyberwarfare.

The report makes clear that the Foreign Ministry, the Interior Ministry and the Defence Ministry have agreed to "the common cyber security architecture ... in the context of the White Paper." The 2016 White Paper elaborates the ministry of defence's new doctrine for the Bundeswehr and provides, among other things, for the deployment of the Bundeswehr at home and an expansion of operations abroad, independently of Germany's post-war allies.

It is exactly these objectives that are being followed by the creation of a new branch of the armed force for cyber defence. It means in practice shelving the prohibition of Bundeswehr missions at home, as well as the separation of the police and army that were anchored in the constitution following the experiences of the Kaiser's Empire, the Weimar Republic and the Nazi dictatorship. "In no other field of activity are internal and external security so intertwined and therefore can only be guaranteed holistically and by the whole state," the final report says.

"With regard to the issue of cooperation in cyber security and defence, the fluid boundaries between domestic and foreign, the BMI [Federal Interior Ministry] and BMVg [Ministry of Defence] have therefore developed a common understanding of the complementary and closely interlinked arrangements." These include the "joint protection of critical infrastructure." The Bundeswehr must therefore "make an increasingly important contribution to general government preventive security."

Contrary to the official propaganda that the new department would only serve for the "defence" against cyber-attacks, the final report makes clear that the Bundeswehr is prepared to enter into its own offensive cyberwarfare.

There was a broad understanding that "defensive and offensive skills are always needed to conduct effective cyber action," the report says. Other countries also keep "the option open of using the full range of military

assets against cyber-attacks in the context of deterrence." The "military relevance of the CIR as a dimension of its own in addition to land, air, sea and space" should therefore be "taken fully into account."

In fact, the cyber warfare measures named in the defence ministry report, such as "espionage, information manipulation, possible cyber terrorism, including up to large-scale sabotage attacks against critical infrastructure," have been an integral component of the imperialist wars of aggression in which the Bundeswehr has played an increasingly prominent role.

The Kosovo war (1998-1999), the first international combat mission by German soldiers since Hitler's defeat in the Second World War, is generally regarded as the first actual cyber war. During their bombing operations, NATO disrupted Serbian air defences, including the use of high-frequency microwave radiation, crippled the Yugoslav telephone network and hacked into Russian, Greek and Cypriot banks to access the accounts of Serbian President Slobodan Milosevic. On the other side, Serbian units disrupted NATO computer servers and listened in to unprotected NATO communications.

Since then, NATO, and especially the United States, have greatly expanded their capabilities for cyberwarfare. At the NATO summit in Bucharest in April 2008, the military alliance formulated its aspiration to "offer assistance to alliance members on demand in defending against a cyberattack." Shortly afterwards, NATO established the Cooperative Cyber Defence Centre of Excellence in Tallinn in Estonia to "defend the information sphere."

Officially, the massive stepping up of NATO's cyber capabilities, and now also Germany's, is being justified by pointing to the "hybrid warfare" conducted by Russia and the danger of international terrorism. In reality, it has long been planned and is considered necessary by all the imperialist powers to defend their economic and geo-strategic interests in the 21st century.

In a lecture to the German Atlantic Association, former Inspector General of the Bundeswehr and chairman of the NATO Military Committee, Klaus Naumann, already stated in 2008: "All in all, the 21st century promises to be a rather turbulent century in which there will be some conflicts, and next to the familiar war between states there will also be new forms of armed conflict such as cyberwarfare and the struggle by transnational forces against states. It will in the beginning, and probably for the foreseeable future, be a world without world order, not least because the Pax Americana has lost its significance in Europe, no longer really applies in the Middle East, but is irreplaceable and only remains a stability factor par excellence in the Pacific."