Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Ludwig Leinhos, *Connections QJ* 19, no. 1 (2020): 9-19
https://doi.org/10.11610/Connections.19.1.02

Policy Article

Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr

Lieutenant General Ludwig Leinhos

Cyber and Information Domain Service, Bundeswehr, Germany

Abstract: Current conflicts are increasingly carried out in hybrid forms, including attacks on technical networks and campaigns aimed at influencing public opinion. The Bundeswehr has responded to this development by pooling its capabilities in this field and combining them in the new Cyber and Information Domain Service. On par with the classic service branches—Army, Air Force, and Navy—this service, with its approximately 14,500 members, makes an important contribution to the whole-of-government security provision.

Keywords: cyber domain, cyber operations, critical infrastructure, hybrid threat, joint fusion centre.

Policy Highlights

In Germany, the provision of cybersecurity—i.e. a condition where risks from cyberspace have been reduced to an acceptable minimum—is a whole-of-government task. This is laid down in the 2016 White Paper,[1] the current basic document on German security policy. There are few areas where internal and external security are as closely intertwined as they are in cyberspace. This includes the joint protection of critical infrastructure.

Nevertheless, even within a whole-of-government approach, there exist areas of responsibility. The Federal Ministry of the Interior, for instance, is responsible for cybersecurity and the protection of civilian infrastructure. It also has the lead responsibility for Germany's cybersecurity strategy. The Federal Foreign Of-

[1] "White Paper on German Security and the Bundeswehr," 2016, https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf.

fice shapes international cybersecurity policy, while the Federal Ministry of Defence is responsible for cyber defence.

In order to conduct its operations, the Bundeswehr, as a military organization, particularly depends on the availability, confidentiality, and integrity of data, IT-based services, and network-enabled infrastructure. For this reason, Bundeswehr cyber defence places particular emphasis on the protection of friendly systems. An essential instrument to ensure this is a comprehensive, digitally generated, situation picture that also includes information space and is made available to other government agencies as part of a network-enabled approach. In information space, people perceive, interpret, and spread information beyond the technical sphere. What is known as "published opinion" is an essential aspect of our considerations.

Apart from preventive measures, reactive and active measures (cyber and information domain operations) may also become necessary when it comes to ensuring the protection of friendly systems. Cyber and information domain operations can take the form of independent as well as supporting operations. In a conflict, they present a conceivable option for initial operations, which can, if necessary, even be conducted at a time when conventional forces have not yet been alerted. Cyber and information domain operations are subject to the same legal constraints as those of other Bundeswehr forces.

In addition to the whole-of-government approach, multinationality is another basic principle of German cyber defence – as well as German security policy in general. Here, we aim at working together with EU and NATO partners as well as in a bilateral, multilateral, and UN framework to ensure cybersecurity and establish the accompanying legal framework.

Policy Challenges

The German Federal Government regards threats from cyber and information space as one of the key challenges facing German security policy. Digitalization has penetrated all areas of life and together with the increasing interconnectedness of individuals, organizations, and states, this offers unique opportunities. At the same time, however, it leaves governments, societies, and economies particularly vulnerable.

Since its 2016 Warsaw Summit,[2] NATO has viewed cyberspace as an independent domain of operations – similar to the land, air, sea, and space domains. In cyberspace, armed forces can use suitable software to reconnoitre and subsequently engage enemy systems, amongst other things. In practical terms, this could entail, for example, the interruption of logistic chains, the corruption of data crucial to operations, or the restriction of the availability of key enemy C2 and information systems.

[2] "NATO Warsaw Summit Communique," July 2016, paras 70-71, www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber.

By including not only the electromagnetic spectrum but also and especially information space, the Bundeswehr has deliberately defined this new military domain in a more comprehensive way than NATO does. Activities in the information environment, such as fake-news campaigns, continue to increase, making it possible to deliberately stir up unrest. International and national conflicts are more and more influenced by propaganda and disinformation. Consequently, information is becoming one of the core resources of the future.

The cyber and information domain distinguishes itself from the classic domains of operations by several unique features. It is characterized by a high degree of complexity. Territoriality is complemented by virtual reality. The cyber and information domain cannot be divided into combat sectors with clear spatial boundaries. The same holds true for the manoeuvring of troops. Nevertheless, physical effects can be achieved in the cyber and information domain, too. The place where cyber and information domain operations create an effect, however, can be tens of thousands of kilometres away from where the action was initiated. Time, too, plays a different role, considering that effects in cyberspace can be achieved over any distance without delay. Given sufficient preparation, effects are produced in near real-time.

The attribution of attacks poses a problem. Thanks to the available technical possibilities, actions can be concealed extremely well. In addition, there are a large number of possible perpetrator groups and motives. By now, the possibilities of digitalization have made it possible for non-state actors to achieve effects by way of cyberattacks which previously could only be achieved by state actors.

To sum up, today's conflicts are essentially characterized by their hybrid nature. Attacks in cyberspace and disinformation campaigns that remain below the threshold of armed attacks need to be taken into consideration just as much as the massive use of cyber operations as part of a national and collective defence scenario. A clear analysis leading to an informative situation picture is, therefore, of essential importance.

As Chief of the Cyber and Information Domain Service, I see it as my responsibility not to confine myself to minimizing the risks described above. For the Bundeswehr, digitalization also offers enormous opportunities, which will be discussed below.

Policy Implementing Structures and Whole-of-Nation Context

Possible threats to governments, economies and societies are multi-faceted and include data theft, espionage, damage of critical infrastructure, disruption of government communications and are as diverse as the agencies that deal with them. Often hybrid strategies are used to exploit the interfaces between responsibilities, for instance, between internal and external security.

Therefore, the closing of ranks and a system of exchange at national level are an absolute necessity. At the strategic level of the state's cybersecurity architecture, the responsibility for coordinating the cooperation within the Federal Government as well as between the government and the business sector rests with

the National Cyber Security Council. At the operational level, the National Cyber Response Centre, a forum to promote the cooperation of government agencies in the cyber and information domain, was established as early as 2011 under the auspices of the Federal Office for Information Security, which is subordinate to the Federal Ministry of the Interior. In cooperation with all key actors, the National Cyber Response Centre is currently undergoing further adaptation towards an interagency operational-level institution. This is an essential step towards establishing even more efficient structures for ensuring Germany's future ability to act in this field. Here, the involvement of national Internet service providers, too, is indispensable. As a representative of the Bundeswehr, the Cyber and Information Domain Service actively contributes to this process. Once the further adaptation of the National Cyber Response Centre has been completed, it could be used to disseminate information provided by the new Joint Cyber and Information Domain Fusion Centre.

In order to make a vital contribution to cybersecurity in Germany as early as during the development stage of key technologies, the Federal Ministry of Defence and the Federal Ministry of the Interior have been working together to build up the Agency for Innovation in Cyber Security since late 2018. This agency will award targeted contracts for ambitious research projects with high innovation potential. In this way, it will be able to tread new paths in order to maintain Germany's prominent role in technological innovation.

With the Cyber Innovation Hub, the Federal Ministry of Defence has its own interface between the start-up scene and the Bundeswehr.

The Federal Office for Information Security provides support to government institutions, such as the German Bundestag, on issues of information security. If required, it dispatches computer emergency response teams to re-establish information security as quickly as possible. For the Bundeswehr, this task is performed by the Cyber and Information Domain Service.

The attribution—i.e. the identification of the perpetrators—of a cyber-attack primarily falls within the responsibility of law enforcement agencies in cooperation with the intelligence services.

As long as the Bundeswehr is not itself affected by a cyberattack, the German Basic Law limits its role to the provision of administrative assistance and support in the event of particularly grave accidents. This does not mean, however, that a serious attack on critical infrastructure cannot result in a military response in the context of national and collective defence.

Policy Implementation

Protection & Operations, Reconnaissance & Effects, Geospatial Information

The Bundeswehr has been closely concerned with the issue of information security since the 1990s. For more than 20 years, it has run its own IT security organization, which it is currently developing into a comprehensive information secu-

rity organization, placing a particular emphasis on raising awareness about the utilization of IT equipment among Bundeswehr members. In response to the effects of increasing digitalization, the new German Cyber and Information Domain Service was inaugurated in April 2017. This major organizational element currently comprises approximately 14,500 military and civilian personnel. It has pooled established units with relevant expertise and expanded existing know-how.

The task spectrum of this major organizational element is very diverse. One focus of its activities is the protection and operation of the Bundeswehr IT system both at home and in theatre. Its capabilities are not limited to establishing the required connections; it also has situation centres that monitor the IT system around the clock. This is where attacks are detected and, if necessary, contained. In addition, before IT systems and systems with IT components can be employed in the Bundeswehr, they are tested and accredited by a central agency with regard to information security.

The overall responsibility for information security in the Bundeswehr rests with the Bundeswehr Chief Information Security Officer (CISOBw) who also acts as my deputy in the position of Vice Chief of the Cyber and Information Domain Service.

Capabilities for reconnaissance and effects in cyber and information space are also being strengthened and further developed. This includes cyber operations, such as the infiltration of enemy IT networks and the detection of vulnerabilities in friendly systems. Military intelligence provides evaluated reconnaissance results, for instance, radar imagery tailored to specific requirements or high-resolution images for the protection of own and allied forces. Electronic warfare and operational communications are also included in the capabilities of the Cyber and Information Domain Service. Operational communication looks at the factors of information and perception, such as: What do people in theatre say about military operations? Is false information circulating about the Bundeswehr? Once these questions are answered, countermeasures can be taken, if necessary.

The members of the Geoinformation Service assist all areas of the Bundeswehr in achieving their mission by providing high-resolution, quality-assured, digital and analogue geospatial information of all kinds.

Joint Cyber and Information Domain Fusion Centre

The complexity of cyber and information space makes sound analysis indispensable. For this reason, the Cyber and Information Domain Service has established its own situation centre for the cyber and information domain. Through the fusion of existing (partial) situation pictures from all functional areas relevant to the cyber and information domain, the Joint Cyber and Information Domain Fusion Centre generates a valid situation picture that forms the basis for determining possible courses of action and exploiting synergy effects. Analysts process various types of data—both structured and unstructured—from different sources; in future, they will also make use of artificial intelligence and big data

methods. For instance, by correlating data from the Bundeswehr IT system with other military intelligence information as well as open-source information gathered from social networks, conclusions can be drawn that can indicate a growing hybrid threat or a coordinated cyber-attack. The analyses thus obtained can then be made available to users in the Bundeswehr and also to other government agencies.

Software Expertise in the Bundeswehr

The Bundeswehr Cyber and Information Domain Service is capable of developing its own software as well as adapting commercially available software products to Bundeswehr or NATO requirements. Since 1 April 2019, the Bundeswehr Centre for Software Expertise has pooled these capabilities and continues to develop them. The inherent possibilities can hardly be overestimated. This allows us to make a decisive contribution to digitalization in the Bundeswehr – from the equipment of commando forces and combat posts to Bundeswehr data centres. One outstanding example—just one of many—is the harmonization of C2 information systems. The Bundeswehr has harmonized the existing C2 information systems of the armed forces, adapting them for service orientation. This project, as well as the succeeding projects that build on it, such as the German Mission Network, will enable the Bundeswehr to provide the majority of its mission-oriented IT from data centres through a "Bundeswehr private cloud" and, for mission-related tasks and exercises, a "mission cloud." The Bundeswehr Centre for Software Expertise makes a crucial contribution in this field.

Harnessing Artificial Intelligence

The work of the Bundeswehr Centre for Software Expertise has already made it clear that the Cyber and Information Domain Service also places great value on exploiting the opportunities offered by digitalization. This also applies to the use of artificial intelligence (AI). For digitalization, AI presents a quantum leap – just as the assembly line did for industrialization. Weak AI—which, in contrast to strong AI, is limited to solving specific user problems—will become an integral part of our everyday lives, a tool that will assist us around the clock. This technology has enormous potential, particularly when it comes to structuring large amounts of data because, like a kind of metal detector, AI tools can find the proverbial needle in the haystack of big data.

A possible military application can be found, for instance, in early crisis detection. For this purpose, the Federal Ministry of Defence has been developing, in cooperation with industry, an IT support project for early crisis detection since 2017. Participants in the project include the Bundeswehr University in Munich. The above-mentioned Joint Cyber and Information Domain Fusion Centre of the Cyber and Information Domain Service will also employ AI tools in future in order to speed up decision-making and put it on a sounder basis. Here the immense advantage of AI becomes apparent. It relieves the analysts so that they can concentrate on what machines cannot do, i.e. drawing conclusions and deriving and assessing options for action. Here we touch on an issue that I regard as extremely

important: The decision about what to do with the information must and will always be made by human beings.

In the areas of Bundeswehr training, materiel maintenance, and logistics too, AI will certainly bring improvements in the future. The Army, for instance, is currently identifying possible uses of AI and machine learning techniques and implementing them as part of prototype projects. The Air Force is investigating the potential of employing AI in the Air Command and Control (AirC2) planning process and the use of AI in mission planning. In the medical field, imaging analysis is already being used in diagnostics.

It is, however, not only the Bundeswehr that has realized the military potential of AI; other nations are also stepping up research. Thus, the use of AI for military purposes is a topic of strategic importance.

Digital Networking on the Battlefield

My organizational element is responsible for the operation, use, protection, and further development of the Bundeswehr IT system. This ranges from office communication equipment, the provision of which is in the hands of the federally owned BWI company, to Bundeswehr weapon systems interfaces – from the Eurofighter system support equipment to the Navy's seaborne operations centre and the tablet computer of the infantry soldier on the battlefield. My objective is to provide the armed forces with the required IT services in an efficient and secure way. Here, particular attention is paid to the design of the overall system in order to ensure seamless transitions and interoperability, both internally and with external partners such as allied armed forces or other government agencies.

The Cyber and Information Domain Service plays a key role in the digitalization of the armed forces. It acts as the central armed forces requesting authority for IT projects. The Digitalization of Land-Based Operations (D-LBO) programme is a prominent example. This project is not only aimed at replacing the old SEM and TETRAPOL radio sets with IP-based services, but at the digital interconnection of all soldiers and vehicles on the battlefield as part of a mobile and seamless, nationally and multinationally interoperable network. It is intended that this will be guaranteed even in national and collective defence operations, which are characterized by frequent command post relocations and mobile conduct of operations. Modernizing the IT equipment of tens of thousands of vehicles and personnel is a mammoth project that will take several years to complete. The D-LBO programme is the key to the modernization of mobile information supply during operations.

Multinational and Whole-of-Government Approach

Multinationality has already been mentioned as an important guiding principle. It applies to the networking of systems and actors of different levels of command on the battlefield just as much as, in a very practical form, to the numerous NATO, EU, and binational exercises. In 2019, the Cyber and Information Domain Service again took part in the world's largest international live-fire cyber defence exercise, the NATO exercise *Locked Shields*. The Bundeswehr computer forensics

experts were chosen as the best team in their category for the fourth time in a row.

At the military-strategic level, too, we maintain close contact with our partners. Thus, while only in the second year of our existence, we were given the chairmanship of the Cyber Commanders Forum for one year. This body regularly brings together the cyber commanders of several NATO and non-NATO nations in order to strengthen multinational cooperation.

Furthermore, thanks to our cooperation with other national institutions, the Cyber and Information Domain Service also contributes to national security and strengthens Germany's cybersecurity architecture. For instance, close cooperation has developed with other security agencies, such as the Federal Office for Information Security. In our eyes, the development of the National Cyber Response Centre, which is subordinate to the Federal Office for Information Security, into an inter-ministerial and operational-level institution is essential for Germany's future capacity to act. With our expertise, we contribute to this process and address the issues, wherever possible, maintaining close contact with all parties involved.

In addition, we have agreed on first cooperation projects with the business and science sector, for instance with the German Telekom company, with the Fraunhofer Institute for Communication, Information Processing, and Ergonomics (FKIE), and—our most recent cooperation since May 2019—with Bitkom, Germany's leading association for information technology, telecommunications, and new media. At the regional level, the Cyber and Information Domain Service is part of the Cyber Security Cluster Bonn, maintaining connections with business companies, educational institutions, and government agencies in order to share information and best practices. This is achieved, for instance, through mutual job shadowing or the opening and support of training measures.

Personnel and Materiel

Suitably qualified and motivated personnel is increasingly becoming a strategic resource. Like many organizations and companies, the Bundeswehr faces the challenge of recruiting young talents in the field of cyber and information technology. From conversations with potential employees, we have learned that the Bundeswehr, with its specific task portfolio, is definitely an attractive employer for this target group. We use this as an advantage and offer incentives, for instance, by promoting education and training measures for our members. In January 2018, an international Master's degree programme in cybersecurity was launched at the Bundeswehr University in Munich. There, we are also creating a research centre for computer science and cybersecurity, which is unique in Germany.

As Chief of the Cyber and Information Domain Service, I fulfil the same role as the chiefs of staff of the other services when it comes to developing personnel requirements for the career paths that fall into my responsibility, i.e. cyber and information technology, military intelligence, operational communication, and geoinformation. This means that I have the lead responsibility for the design of

these predominantly technical career paths. For these careers, we will establish a holistic view on personnel issues across all major organizational areas and thus improve the existing range of individual professional perspectives.

Currently, we are also developing possibilities to take informal cyber and IT expertise of potential employees into stronger consideration, which will allow us to make attractive offers to these applicants, too. In addition, we have made significant progress when it comes to personnel augmentation by reservists and lateral entry employees. With more than 800 individuals interested in working for the cyber reserve and over 1400 users of the cyber community platform, a Bundeswehr virtual forum, the Cyber and Information Domain Service also benefits from external expertise. Furthermore, we are creating various flexible working opportunities and attempting to provide financial incentives, for instance, in the form of bonus payments for urgently needed IT specialists.

Regarding the issue of materiel, it is my wish to further streamline procurement and maintenance processes. Given the rapid development cycles in the cyber and IT sector, this is the only way we can ensure adequate equipment and maintenance. Numerous defence projects already exist that contribute to the modernization of C2 capability in the Bundeswehr. Above, I have described in detail how the Cyber and Information Domain Service contributes to this through the digitalization of land-based systems.

International Law

In general, the use of military cyber capabilities is subject to the same constraints under international and constitutional law that apply to any other operation of the German armed forces. At the international level, there also exists a definitive but non-binding regulation on how to apply existing international law to cyber operations, the Tallinn Manual 2.0.[3] These legal and ethical foundations are to be taken into account for all measures in cyber and information space. So, although the foundations of legal security have been laid down, there is still much to be done in this area. Indeed, it is indisputable—and has by now become consensus—that the binding international rules that govern armed conflict between states must also be applied to the cyber and information domain. Therefore, in order to allow a quick response to attacks if necessary, the issue of how these rules are to be applied to this new domain must be considered in detail.

The Way Forward

The challenges in the cyber and information domain, which have been described above, will increase further, both in quality and in quantity. Therefore, adequate protection is vital for the state, the economy, and society. In Germany, this is regarded as a national task, which is to be approached together with international partners.

[3] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

This is also how the most recent major organizational element of the Bundeswehr sees itself. The Cyber and Information Domain Service is responsible for the Bundeswehr IT system as well as for reconnaissance, effects, and geoinformation. During routine duty, operations, and exercises, it closely cooperates with other parts of the Bundeswehr as well as with friendly armed forces and other national authorities.

With respect to digitalization in the Bundeswehr, it is important not only to counter the risks but also, and especially, to exploit the inherent opportunities. This largely applies to technical aspects. At the same time, however, a new way of thinking is required when it comes to operations in cyber and information space. Cyber and information domain operations constitute an independent field of operations and provide support to land, air, and maritime missions as part of conventional military operations. Therefore, in order to provide politicians with non-kinetic options, these capabilities must be developed across the entire spectrum of cyber and information domain operations.

The government must maintain its capability to act and to ensure the protection of the people and the provision of basic services. Here, the capabilities of the Bundeswehr in the cyber and information domain can make a vital contribution.

Disclaimer

Acknowledgement

Journal *Connections: The Quarterly Journal*, Vol. 19, 2020 is supported by the United States government.

About the Author

Lieutenant General **Ludwig Leinhos** joined the Bundeswehr as Air Force officer candidate in 1975. His studies of electrical engineering and graduation as Diplom-Ingenieur at the Bundeswehr University Munich were followed by training and assignments in the field of electronic warfare. From 1988 until 1990 he attended the General Staff Officer Course at the Bundeswehr Command and Staff College in Hamburg.

His subsequent military career was characterized by various ministerial staff and leadership assignments in Germany and abroad in the fields of command and control systems, signals intelligence, as well as IT planning and application. As General Manager at NAPMA, he was responsible for the program management organization of NATO's AWACS fleet. From 2013 until 2016, he was in charge of cyber defence and numerous IT standardization issues, among others, as Director, NATO Headquarters C3 Staff at NATO Headquarters in Brussels.

From 2016 onwards, Lieutenant General Leinhos as Director, Activation Staff of the German Cyber and Information Domain Service has set the course for the new Service of the Bundeswehr, and on 1 April 2017 became the first Chief of the German Cyber and Information Domain Service.