Germany's Cyber Strategy—Government and Military Preparations for Facing Cyber Threats

Omree Wechsler

Germany is a leading member of the European Union and one of the world's strongest economies. Consequently, it is a central target for cyberattacks from states, terror organizations, and criminal groups. Dealing with the threat to German democracy posed by campaigns to disseminate false information—plus the cyber threat posed by Russia—has led to changes in the German security concept, causing the German government to seek to increase its cyber independence and to establish offensive capabilities in this space. Understanding how Germany copes with cyber threats and its future plans on this issue is vital for learning and comparing, while it also provides new insights about this problem, particularly for other democratic countries.

The first part of this article describes the German government's preparations in the field of cyber security, cooperation between German authorities, and preparations relating to personnel and reinforcements for the relevant institutions. The second part describes preparations at the security-military level and how Germany is adapting to the new challenges. The last part of the article examines the situation from an international angle and looks at how Germany sees its role as an international leader in the cyber field.

Keywords: Cybersecurity, Germany, strategy, government preparations, military preparations

Omree Wechsler is a researcher at the Yuval Ne'eman Workshop of Science, Technology, and Security and at the Blavatnik Interdisciplinary Center for Cyber Research, Tel Aviv University.

Cyber, Intelligence, and Security | Volume 2 | No. 1 | May 2018

Introduction

On February 23, 2011 Germany published its comprehensive cyber strategy. The document defines its perception of the cyber threat, determines guidelines for a cyber security strategy, and defines the goals and steps to implement them. The steps taken by Germany since the publication of this strategy in 2011 have focused on protecting critical infrastructures, increasing public awareness, making manufacturers responsible for supplying secured products, reinforcing IT security among government agencies, setting up the National Center for Cyber Defense (Cyber Abwehrzentrum – Cyber A-Z), establishing the National Council for Cyber Security, improving the efficiency of fighting crime in cyberspace, and positioning Germany as key actor in the efforts to provide cybersecurity in Europe and around the world.

In November 2016, the German cabinet approved a new strategy document on the subject of cybersecurity, which was published by the Ministry of the Interior. The new strategy is broader than its 2011 predecessor, with details about four main areas in which Germany must take action: safe and independent use of the digital environment; cooperation between the German state and the economic sector in the cyber field; building an effective cybersecurity architecture in the public sector; making Germany a central actor in the European and global cyber policies.

Perceiving the Threat

While the German strategic document of 2011 presented the cyber threat in fairly general terms and described the complexity of cyberattacks, in contrast, the 2016 document indicates the growing importance of Germany in the cyber field vis-à-vis the rise in the number of cyberattacks and their complexity. The 2016 strategic document deals, inter alia, with the social, economic, political, and personal damage caused by cyberattacks and describes them as a threat to stability, public order, and democracy. It also defines targets where the results of an attack would be particularly damaging, both publicly and privately. They include attacks on critical infrastructures, especially the energy sector and the power grid; attacks on banking infrastructures and financial institutions, and manipulations of the stock exchange; manipulation of autonomous systems, and of data traffic used by IT systems, such as in the field of health; and dissemination of false information, misleading reports, and fake news to manipulate public opinion and thus threaten free society and democracy.

The German Ministry of Interior, which as mentioned was responsible for drawing up the strategy, identified various types of cyberattacks and their motives: The motive for committing cyberattacks is broad and could be ideological or criminal. Attackers may be terror organizations, organized criminal gangs, military units, or intelligence services of other nation states. The varied background of the attackers and their level of professionalism render it very difficult to detect, monitor, and analyze attacks. The authors of the document warn against political or military conflicts that could be accompanied by hostilities in cyberspace. Such conflicts could escalate into a full-fledged cyber war, or even into cyberattacks just below the level of an armed conflict.

The overall picture suggests that an array of threats is composed of many players with different capabilities and motives. Therefore, the document's authors conclude that the classic means of protection for existing IT systems are not enough. They assume that the number of cyberattacks will increase, their complexity will grow, and the main targets of cyberattacks will be German society, economy, and industry, as well as German democracy.

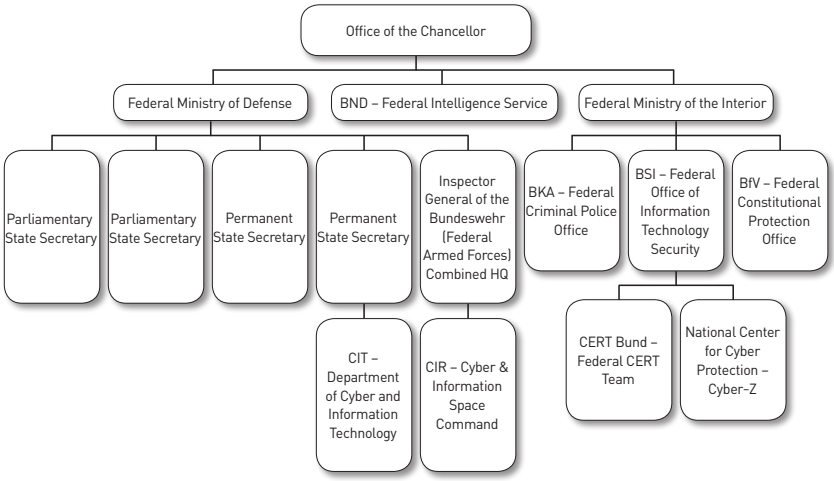

Diagram 1: Security and Cyber Entities in Germany

Government Preparations

Government entities responsible for the field of cyber in Germany are the Federal Office of Information Technology Security (BSI); the Federal Office for Protection of the Constitution, which acts as the internal security agency

(BfV); the Federal Intelligence Service (BND); the Federal Criminal Police Office (BKA); the Ministry of Defense (BMVg); the Ministry of the Interior (BMI); and the Federal Office of Civil Protection and Disaster Assistance (BBK), which corresponds to the Home Front Command in Israel.

The Office of Information Technology Security

The Office of Information Technology Security or the BSI (Bundesamt für Sicherheit in der Informationstechnik) is a federal office under the authority of the Ministry of the Interior, which also functions as a national cyber security authority. The BSI was set up in 1991, with the aim of providing IT services to government entities, IT system manufacturers and suppliers, and users. Today the BSI is responsible for protecting Germany's information technology and for implementing its national IT security policy. It is also responsible for a range of activities, such as early warning, prevention and incident response, issuing warnings on malware and vulnerabilities in products, establishing training channels, and raising awareness among government entities and the public. The office is also responsible for the information exchange between government ministries, institutions, and organizations in the private sector; formulating security standards for operators of critical infrastructures and products; and qualification and training processes for organizations and products.[1]

The BSI is responsible for other entities engaged in handling cyber threats, such as the National Center for Cyber Defense (Cyber A-Z), the Federal CERT Team (CERT-Bund), and the Civilian CERT (Bürger-CERT). The latter is responsible for increasing awareness of cyber threats among the public and small businesses.[2]

Strengthening the National Center for Cyber Defense

The National Center for Cyber Defense or the Cyber A-Z (Cyber Abwehrzentrum) is a federal institution designed to protect against electronic attacks on Germany's IT infrastructures and its economic sector. The center

1 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, "Germany: Cyber Readiness at a Glance," *Potomac Institute for Policy Studies* (October 2016), pp. 5–7; http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf; "Cyber-Sicherheitsstrategie für Deutschland 2016," Bundesministerium des Innern, 2016, p. 17.

2 Hathaway et al., "Germany: Cyber Readiness at a Glance," pp. 5–7.

was set up following a cabinet resolution in February 2011 and began operating in Bonn in June that year, under the BSI.[3] The main tasks of the Cyber A-Z are to prevent cyberattacks and provide information and early warning of such attacks. The center shares information about profiles and identities of the people behind cyberattacks, and about the weaknesses of IT products.

The Cyber A-Z is not an independent entity but rather is the outcome of a number of cooperation agreements between German authorities engaged in cyber protection. Therefore, the separation between the jurisdiction and responsibility of the various authorities, particularly between the police and the intelligence services, is maintained while cooperating in the center's framework.

The 2016 strategy document recommends that Cyber A-Z should be further developed as a coordination center, and in the future be given the independent ability to analyze and prepare updates that will accurately describe real-time situations. It also recommends that the National Center for Cyber Defense should function as a center for shared training and exercises for how to cope with cyberattacks.[4]

Strengthening the analysis and response capabilities of government ministries

Germany is investing in the establishment of Mobile Incident Response Teams (MIRT), which are subordinate to the BSI. The purpose of these teams is to analyze the situation during an attack and help local teams to handle the incident and its consequences. The mobile teams provide assistance, by request, to constitutional bodies, federal authorities, and operators of critical infrastructures and important installations. The purpose of the assistance is mainly to mitigate incidents and threats, enable recovery, and to return to normal activity.[5] The MIRTs are supposed to receive assistance from special units of the Federal Criminal Police Office (BKA) and the Federal Office for Protection of the Constitution.

Other teams are supposed to be set up under the BKA. These teams, called Quick Reaction Forces, will form a legal unit whose role will be to

3 The authorities that play a central role in operating the Cyber A-Z: the BfV, the BSI, and the BBK. Other authorities that cooperate and are involved with the center's activity are the BKA, the BND, the federal police, and the army (the Bundeswehr).

4 "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 28

5 Ibid, p. 29.

provide a fast response to cyberattacks through close coordination with the various state prosecutors in Germany or with the Federal Attorney's Office. The teams should accelerate processes of enforcement and arraignment, working with the German enforcement authorities.

The BfV has also set up Mobile Cyber Teams, consisting of IT experts and intelligence experts with experience of analyzing cyberattacks. These teams include people who are fluent in foreign languages and who deal with cyberattacks by foreign intelligence services and terror organizations.[6]

Strengthening existing CERT teams and setting up additional emergency response teams

As stated, the Federal CERT Team is a branch of the BSI with the responsibility of assisting the authorities, operators of critical infrastructures, businesses, organizations in the private sector, local authorities, and research institutions. In addition, the Federal CERT is responsible for maintaining contact and coordinating with foreign and international CERT teams.[7] The German government intends to invest additional resources to enlarge the Federal CERT Team and broaden the knowledge and expertise of its members, as well as setting up new CERT teams.

Strengthening the early warning capabilities of the German Federal Intelligence Service

The Federal Intelligence Service (BND) is responsible, inter alia, for monitoring and recording attempts by external elements—states, terror or criminal organizations—to carry out cyberattacks on Germany's infrastructures, as well as on its economic and civilian sectors. Monitoring and documenting attempted attacks should enable the BND to construct a model of how the attackers behave and thus provide early warning whenever suspicious activity on their part is detected.

The BND works with IT experts and analysts in order to build an early warning system for cyberattacks. The system is intended to identify potential attacks, analyze them, and build a map of threats. Early detection efforts are based on SIGINT, intelligence that is gathered by means of initiated internet scans as part of a policy dubbed "Signals Intelligence Support to Cyber

6 Ibid.

7 Ibid, p. 34.

Defense."[8] Development of the early detection system began in 2014, and by 2020 about 300 million euros will have been invested in this project. It is being executed in collaboration with the intelligence agencies of Germany's allies and is expected to provide a response to attempts at network espionage.[9]

The BND uses sensors installed on optical fibers all over the world. They give the German intelligence service the ability to track data traffic in other countries and to monitor cyberattacks in advance. This method also enables the German intelligence service to gather information about malware and to maintain a database of attack tools.[10]

Strengthening legal and constitutional frameworks in cyberspace

The German government is working to strengthen enforcement and judicial authorities in order to fight cybercrime. First, the government will be responsible for allocating resources to the relevant authorities and for the additional skilled manpower required in the fields of detection, criminology in cyberspace, and criminal identification in digital space. Secondly, the government will assist the security and enforcement authorities to develop and build analysis and assessment systems. Thirdly, special emphasis will be placed on matching the technology with the powers and means available by law to enforcement and juridical entities. The development of both aspects side by side is intended to avoid gaps between the law and the technology. Fourthly, the government will stress cooperation between German authorities and other countries, emphasizing exchange of information, professional knowledge, and experience between the German authorities and their counterparts in other countries and between those at federal and local level within Germany.[11] An example of the type of cooperation that Germany wishes to reinforce is the existing cooperation with the European Union in

8 Ibid, p. 32.

9 "300 Millionen für Frühwarnsystem gegen Cyberattacken," *Spiegel Online*, May 16, 2014, http://www.spiegel.de/netzwelt/netzpolitik/bnd-arbeitet-an-fruehwarnsystem-gegen-cyberattacken-a-969899.html.

10 Frederik Obenmaier and John Goetz, "Geheimdienst verstärkt Kampf gegen Cyber-Angriffe," *Süddeutsche Zeitung*, May 9, 2014, http://www.sueddeutsche.de/politik/abwehr-von-schadsoftware-geheimdienst-plant-fruehwarnsystem-fuer-cyber-angriffe-1.1956067#redirectedFromLandingpage.

11 "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 30.

general and with specific EU entities, such as the EU Agency for Network and Information Security (ENISA) and the Europol Center for Cyber Crime.

Strengthening the powers of German entities that deal with cyber threats finds expression, inter alia, in enhancing the powers of the Federal Criminal Police Office and the Federal Police in the fields of cybercrime, cyber espionage, and so on. In addition, the German government has undertaken to reinforce and extend the Center for Cyber Crime operating within the framework of the Federal Criminal Police Office. The aim is to strengthen the center's abilities to investigate and assess situations and also to update the criminal law with more severe penalties for cybercrimes.

In order to deal with spying in cyberspace, the authority of the Federal Office for Protection of the Constitution will be enhanced, including improving its abilities to maintain more effective tracking and analysis of changing patterns of behavior shown by terrorists and extremist elements on the internet.[12]

Military Preparation

Two important organizational steps have been taken in the field of military security in order to improve Germany's preparations for dealing with the cyber threat: the establishment of the Cyber and Information Technology Department (CIT) of the Ministry of Defense and the establishment of an independent Cyber and Information Space Inspectorate (CIR), alongside branches of the military. These steps are intended to provide protection for military IT systems and to formulate military strategies that will render the security forces relevant in the digital age, by providing defensive and offensive cyber capabilities.

Cyber and IT Department

In September 2016, the Minister of Defense Ursula von der Leyen announced the establishment of a new department, Cyber und Informationstechnik (CIT). Klaus Hardy Muehleck was appointed head of the new department, with a staff of about 130.[13] The CIT will build a military cyber security layout

12 "Digitale-Agenda: Mehr Sicherheit im Cyberraum," *Bundesregierung*, 2014, https://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/6_Sicherheit/6-5_Cyberraum/cyberraum_node.html.

13 Before his current appointment, Muehleck was chief information officer at Thyssenkrupp, chief information officer at Volkswagen (2004–2011) and responsible for information technologies at Audi (2001–2004).

based on the national cyber security strategy. It will also lead processes of professionalizing the German army in the field of data security and will be responsible for cyber and IT in the military field.

The CIT Department has two sub-departments: one in Berlin, which will handle cyber and IT governance, planning, and strategy in the field of information technology. Its tasks will include digital policy and managing IT initiatives. This department will also be responsible for building the IT system of the Ministry of Defense and the German army. The second sub-department will be set up in Bonn, and its purpose is to provide IT services and handle the implementation and routine operation of military IT systems. Other areas of responsibility will include protection of IT systems, passive cyber protection, and encryption security.[14]

Cyber and Information Space Command (CIR)

The Cyber and Information Space Command (Cyber und Informationsraum) was set up as part of the German army in November 2015. Its task was to examine organizational aspects, areas of responsibility, and tasks facing the German army (the Bundeswehr) in the fields of cyber and information. In October 2016, General Maier Ludwig Leinhos, a three-star general, was appointed to head the new command, and in April 2017, the CIR began to function as a military command headquarters in every way. It is expected to become fully operational by the start of 2021. The CIR began its activity with an initial staff of about 260 people, which by July 2017 had grown to about 13,500 people. This is expected to increase to about 14,500 in 2021. 1,500 of the posts are reserved for civilians.[15]

The tasks of the CIR are defined as passive and active defense in cyber and information space. The German army is a sensitive target for hundreds of daily cyberattacks, first and foremost aimed at stealing information and data and to interfere with IT-supported weapons systems. The Bundeswehr's central importance to the NATO alliance also makes it a target for hackers. Because of this sensitivity, the primary aim of the CIR is to protect the Bundeswehr's networks and IT systems. Passive defense involves monitoring,

14 "Verteidigungsministerin stellt neue Cyber-Abteilung auf," *Bundesministerium der Verteidigung,* October 5, 2016.

15 "German Military to Unveil New Cyber Command as Threats Grow," *Reuters*, March 30, 2017, http://www.reuters.com/article/us-germany-military-cyber/german-military-to-unveil-new-cyber-command-as-threats-grow-idUSKBN1712MW.

early detection, analysis, and assessment of damage, plus the ability to neutralize the threat and assist in the return to normal function. The CIR's other tasks are to protect government institutions, public entities, and critical infrastructures against cyberattacks from foreign elements, such as nation states and terror organizations, as well as the struggle against propaganda, disinformation, and fake news.

In addition to passive defense, the Bundeswehr is developing offensive capabilities that it defines as "active defense." These are expressed in the ability to collect intelligence about foreign networks and systems and to interfere with their operation. These offensive capabilities are still being developed and are under the responsibility of the CNO (Computer Network Operations) team, composed of about eighty experts, graduates of the computer science departments in the Munich Military Academy, who specialize in hacking into networks and servers, carrying out manipulations and causing damage.[16] Although the CNO team has existed since 2009, under the Cyber and Information Space Command, it has been extended and transferred from the Operations Department of the Bundeswehr Strategic Command to a new cyber operations center and its capabilities in the field of scanning networks, collecting intelligence, and enemy simulation are expected to grow.

These capabilities of the German army have aroused a lively debate among legislators in Germany and drawn criticism from the public, which is mostly against the use of force and fearful of entering a "cyber war" or cyber arms race and is therefore suspicious of the idea of providing additional powers and capabilities to the security forces. Indeed, the offensive capabilities represent a fundamental change in the German security concept, making it more pro-active than previously.[17]

Recruitment system for the Cyber and Information Space Command

The Bundeswehr works with the Ministry of Welfare and Development in the field of recruiting new personnel for the CIR. The intention is to create a mechanism for recruitment and employment that will include career development tracks for the recruits and operate with the dynamism and

16 Christian Kahl, "Vom Kampf in der fünften Dimension," *Bundeswehr Journal*, May 3, 2013, http://www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension.

17 Isabel Skierka, "Bundeswehr: Cyber Security, the German Way," *Digital Frontiers* (blog), *Observer Research Foundation*, October 20, 2016, http://www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/.

flexibility that characterize the IT market. The aim is to achieve the target number of recruits and train personnel who can use their initiative and think flexibly. The idea of addressing target groups that until recently were not candidates for recruitment—including people who were found unsuitable for a military framework, people from immigrant families, holders of dual citizenship, dropouts from formal education, and candidates in other professional fields—is also being considered. Recruitment devices to find suitable candidates include competitions and tournaments to discover IT talents, start-up competitions, recruitment of candidates from the field of gaming, and the provision of scholarships for relevant studies.[18] The Bundeswehr has also set up a research department, the Cyber Cluster, at the Munich Military Academy, and launched a program of studies for a degree in cyber security, which is expected to produce about seventy graduates each year.[19]

The International Arena

Germany sees the international arena not only as an opportunity to strengthen its cyber security through partnerships and joint initiatives but also as a platform for strengthening its economy and industry, which is largely based on exports. Germany's positioning at the center of the international arena in the field of cyber and IT reinforces its reputation and political status all over the world. In the strategy document of 2016, the German government seeks to position itself at the forefront of the regional-European and international efforts to build resilience, handle cyber threats, and define standards for cyber security.

There are four main areas in which Germany intends to promote its cyber security policy: Europe and the European Union; NATO; the international arena; and bilateral co-operations.

Europe: The security of the European market and the regular continuity of trade on the continent are the greatest interests of the German government. With the growth of digital trade, the question of cyber security for the European single market is also gaining importance. An overlap exists between the German interest in securing the online economy, the networks and information systems that are being used, and the interest of the European

18 "Abschlussbericht Aufbaustab Cyber- und Informationsraum," *Bundesministerium der Verteidigung*, April 2016, pp. 31–33.

19 Ibid., pp. 35–36.

Commission, whose purpose is to create trust and security in the projects of the European Union, including the digital single market.

Another of Germany's interests is to preserve human rights and privacy when using the internet. Against this background, the German government announced its support for European Commission regulations to regulate the transfer of data and information within Europe and to protect privacy and commerce.[20]

The government is also working to strengthen Germany's status in the framework of European cyber policy, through its growing involvement in the EU foreign and defense policy. The German government supports the promotion of research by German academics in the field of IT security and works to connect them with their counterparts all over Europe, as well as promoting the local IT industry. A large part of promoting the German industry and increasing Germany's involvement in shaping the EU cyber security policy finds expression in support of EU projects dealing with legal and technical issues relating to cyberspace, such as the use of electronic identification and signatures by businesses and authorities. This makes it possible to identify users and provides full cooperation with the European Union Agency for Network and Information Security (ENISA).[21]

NATO: Germany's foreign and defense policy considers NATO as the backbone upon which the Euro-Atlantic alliance rests. Germany's membership ensures both its security and that of Europe. According to the German strategy, the collective security concept of NATO also applies in cyberspace, and therefore NATO must also become capable in cyberspace, alongside the spheres of sea, air, and land. Germany is a leading partner in the processes of building NATO's cyber security formation and of an effective deterrence policy in cyberspace in the face of threats of "hybrid" warfare; that is, the combination of kinetic and cyber warfare.[22]

The international arena: Germany has positioned itself as a leader of discussions in international organizations, headed by the Organization of Security and Cooperation in Europe (OSCE) and the United Nations (UN) on matters affecting compliance with international law in cyberspace; closing cyber loopholes in international law; developing norms, regulations, and

20 "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 40

21 Ibid.

22 Ibid.

principles concerning responsible conduct by states in this field; and also reinforcing the capabilities and authority of the UN in cyberspace.

Other areas where Germany plays a part is in raising awareness of the risks in cyberspace; expanding frameworks for sharing information on cyberattacks and incidents; reinforcing the international response; increasing the severity of penalties for economic espionage and cyberattacks; and actively supporting stronger supervision of the export of technologies that can be exploited for offensive behavior in cyberspace.[23]

Bilateral contacts: Germany works to support its partners and help them to build capabilities for detecting, preventing, and responding to cyber incidents, and strengthen their digital infrastructures. As part of Germany's efforts to be perceived as a reliable player in the international arena, it encourages other players to introduce legislative reforms on cyber matters, sign treaties and take confidence building measures to strengthen cyber security.[24]

The Challenges and Potential Consequences of Germany's Preparations

Notwithstanding the various preparations, the increased manpower and the widening of powers for various authorities and other entities, the German government still faces a number of challenges in cyberspace. Some of these are legal constraints affecting the use of offensive cyber capabilities and cooperation between the army and intelligence and espionage units, while others are the gaps in the realm of employing a professional workforce. Germany's preparations in cyberspace also have several potential consequences for its ambitious foreign and defense policy in the international arena.

Constitutional gaps regarding the use of force

As part of the military restraint that has characterized Germany since the end of World War II, the German constitution states that any use of military force for purposes that are not purely defensive requires a parliamentary mandate. A report from the German Ministry of Defense states that the need for the parliamentary mandate is also valid for operations in cyberspace.[25] Due to the complexity of this space, where it is not always possible to distinguish

23 Ibid, p. 41.

24 Ibid, p. 42.

25 "Abschlussbericht Aufbaustab Cyber- und Informationsraum," p. 5.

between defensive and offensive moves, questions arise as to how and in which cases the army must turn to parliament for its approval. It appears that the section in the constitution requiring parliamentary approval for active defense operations or a preemptive strike could pose a challenge to cyber operations, particularly in the case where rapid, covert responses are needed. A means of bridging these gaps has not yet been found.

Cyberattacks require accurate intelligence about target networks and systems and about weaknesses that can be exploited. Such intelligence as well as spying and other actions required to prepare for a cyberattack is the province of the intelligence services. Therefore, the German army will have to cooperate and share information with the German espionage and intelligence services. In the United States, such cooperation is seen as obvious, particularly since the US Cyber Command shares the same leadership with the National Security Agency (NSA) and uses its assets and the intelligence it provides; such cooperation in Germany, however, faces severe constitutional constraints. Although the legal dimension of cooperation between intelligence units and the army and enforcement agencies in Germany is beyond the framework of this paper, it should be noted that there is a legal debate over the types of information that espionage entities, particularly the BND, are permitted to share with other German authorities.[26] Moreover, the BND is subordinate to the Office of the Chancellor, while the army is subordinate to the Ministry of Defense, and the Federal Office for Protection of the Constitution is subordinate to the Ministry of the Interior. Therefore, it is not clear how they will be able to maintain cooperation. Furthermore, there is still no definition of the division of powers between these three entities regarding the collection of data relating to cyber operations.

Challenges of recruiting skilled personnel

Another problem that is not unique to Germany is recruiting and training personnel to fill the new jobs in the CERT teams, and particularly in the Cyber and Information Space Command of the Bundeswehr. In spite of the announcement by the German army that the Cyber Command has already been staffed by soldiers selected from other branches of the military, the

26 Kai Biermann, "BND-Überwachung: Warum schickt der BND der Bundeswehr abgehörte Daten?" *Zeit Online,* March 18, 2015, http://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung/komplettansicht.

Bundeswehr still faces the challenge of setting up a reserve pool for the new command. In a letter from the federal office responsible for military armaments and equipment to reserve soldiers in the field of IT, they were asked to give names of civilian colleagues in the field.[27] The letter also stated that the army needed hackers, IT developers, IT security experts, penetration testers, and more.[28]

Apart from the difficulty of recruiting talented and experienced IT people, the Bundeswehr suffers from low recruitment rates and has an image of being an unattractive employer. There has also been criticism of the army's ambitious plans, with claims that it is insufficiently flexible and that its pace of training, procurement, and equipping itself does not match the pace of initiative and innovation in hardware and software markets, nor the rapid pace of change in cyberspace.[29]

The academic curriculum launched by the Bundeswehr to train IT people is a positive step in the right direction, but given the expectation of about seventy graduates from the program each year, it appears that it will take a long time before the army's needs are met. In this situation, there is a fear that the Bundeswehr will have to turn to private contractors to perform some of the jobs. This option raises worries about maintaining national security, given the many examples of leaks and national security breaches through contracted staff working for the NSA in the United States.

Opportunities in the international arena

Germany's ambitions and its wish to leverage its international status as well as its economy and industry are not new. In recent years, Germany has actively and consistently participated in international forums dealing with cyber security, information and communications technologies, such as the UN, the European Union, NATO, the G7 summit, the European Organization

27 The Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support.

28 Matthias Monroy, "Herausforderungen im Cyber- und Informationsraum: Bundeswehr sucht Tips für Aufbau einer Cyber-Reserve," *Netzpolitik,* April 26, 2016, https://netzpolitik.org/2016/herausforderungen-im-cyber-und-informationsraum-bundeswehr-sucht-tips-fuer-aufbau-einer-cyber-reserve/.

29 Nina Werkhäuser, "German Army Launches New Cyber Command," *Deutsche Welle*, April 1, 2016, http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517.

for Security and Cooperation, and others. Germany has also taken part in dialogues concerning the development of cyber capabilities and has actively participated in the discussions of the UN Group of Governmental Experts (GGE) to define norms of conduct in cyberspace.

Germany's bilateral activity has been and is still characterized by providing aid on cyber matters to developing countries and by cooperating on these matters with developed countries.[30] Examples can be found in the talks held in Berlin with delegations from India;[31] in the signing of a cooperation agreement with the Estonian Defense Industry Association;[32] and in the cooperation agreement with Singapore on cybersecurity.[33]

In addition to these trends, which are expected to continue, Germany has found new opportunities in the international arena: President Trump's "America First" policy and the ongoing lack of clarity regarding the United States and its relative distance from the European Union and NATO, at least in comparison to the Obama administration, could give Germany the opportunity to play a more central role in the leadership of the western countries. Specifically, the closure of the Office of the Cyber Security Coordinator in the US State Department in 2017, which could be seen as damaging the diplomatic capabilities of the United States in the field of cybersecurity, could be an opportunity for Germany's ambitious foreign policy.[34]

The possible exit of Britain from the European Union will apparently lead to gaps in the EU security and intelligence gathering. This is also true for cybersecurity. The vacuum left by the departure of Britain—considered

30 Hathaway et al., "Germany: Cyber Readiness at a Glance," p. 13.

31 "Indo-German Intergovernmental Consultations in Berlin—Strengthening Cyber Cooperation," *German Missions in India*, May 31, 2017, http://www.india.diplo.de/Vertretung/indien/en/__pr/Politics__News/Merkel__Modi__2017__update2.html.

32 "Cyber-Security Council Germany and Estonian Defence Industry Association sign cooperation agreement, agreeing upon fostering transnational cooperation in the area of cyber security together," *Cyber-Security Council Germany*, September 14, 2017, http://www.cybersicherheitsrat.de/data/PRESS-RELEASE-Cyber-Security-Council-Germany-and-Estonian-Defence-Industry-Association-sign-cooperation-agreement.pdf.

33 Prashanth Parameswaran, "What's in the New Singapore-Germany Cyber Pact?" *The Diplomat*, July 11, 2017, https://thediplomat.com/2017/07/whats-in-the-new-singapore-germany-cyber-pact/.

34 Morgan Chalfant, "Tillerson Moves to Close State Cyber Office," *The Hill*, August 29, 2017, http://thehill.com/policy/cybersecurity/348438-tillerson-moves-to-close-state-cyber-office.

a central player in this field—could encourage Germany to step in with its capabilities. The British exit could harm not only cybersecurity but also the whole range of information sharing between EU countries, including Germany.

Conclusion

Germany sees the cyber threat as paramount and is therefore preparing to protect its economy, industry, security forces, and critical infrastructures. It is doing so through a range of actions on various fronts: legal, constitutional, military, federal, and local. Germany's comprehensive strategy published in 2016 specifies the main steps intended to provide a response to the cyber threats it faces. This strategy supports strengthening and expanding entities and units for cyber protection and renewed military preparation, including setting up specialist entities for cyber defense.

In the area of government preparations, Germany emphasizes expanding existing bodies and reinforcing their capabilities. A striking example is the expansion of the National Center for Cyber Defense (Cyber A-Z), which acts as the link between government ministries that are legally responsible for cyber activity, and also the granting of independent capabilities to this unit for the purpose of analyzing, assessing, and defining the situation as well as adding a platform for practicing and simulating emergencies. Other examples include the reinforcement of local response capabilities by means of federal aid.

In the military arena, Germany set up the Cyber and Information Technologies Department that operates under the Ministry of Defense. The department is responsible for strategic military cyber planning and for building the Bundeswehr cyber security layout. It also set up the Cyber and Information Space Command, which is responsible for protecting the army's networks and IT systems and is intended to be equipped with both defensive and offensive capabilities. Its potential offensive capabilities represent a significant change in German policy, which until now had avoided using force and building offensive capabilities as it could arouse public criticism.

In the international arena, Germany apparently sees international and bilateral cooperation not only as a strategic move to strengthen national cyber security but also as an opportunity to leverage and reinforce its economic and political status in Europe with its bilateral partners and international organizations by playing a major role in the joint effort to handle cyber

challenges. Positioning itself as a cyber power is Germany's attempt to strengthen its international, political, and diplomatic standing, as well as its industry and technology and export-based economy.

Germany joins a long line of European countries, including Britain and France, that are worried about espionage, data theft, instability, external influences on public opinions, and foreign intervention in their democratic processes and therefore are choosing to invest efforts and resources to mitigate these threats. However, there are constitutional challenges to Germany's strengthening in the field of military cyber, and particularly the use of offensive cyber weapons and the principles of active defense, which is part of the role of the new CIR. Other challenges in the areas of equipment and personnel are evident, but they are not unique to Germany. The partial measures taken to deal with these challenges are a step in the right direction but are not expected to provide a complete solution to the problem.

Germany is undergoing an interesting process, mainly due to its power and centrality to European and international politics and economy. It is possible that events with international influence, such as the Trump Administration's "America First" policy, will force Germany to increase its security expenditure, which includes cyber defense and cyber warfare. Other events, such as the British exit from the European Union, are expected to affect Germany's security in general and its cyber security in particular, since it is linked to the security of the entire European Union.

Another interesting process is the deep change in Germany's security concept, which in spite of constitutional challenges, is increasingly based on active defensive and offensive means. This is a tremendous change for a country that has avoided the use of force for the last seventy years. This change, however, is expected to encounter many opponents, both within the German public and legislature, making it harder to implement.