# *At The* READY

## ADVANCING THE GERMAN CYBER RESERVE

*PER CONCORDIAM* ILLUSTRATION

By **Rupert Brandmeier**, **Jörn-Alexander Heye**, **Dr. Florian Rupp** and **Clemens Woywod**, military reserve officers, German Cyber and Information Domain Service

Tensions between the Western and Eastern political blocs decreased rapidly and substantially after the demise of the Soviet Union in 1991. Consequently, politicians in the reunified Germany increasingly questioned the rationale of compulsory military service until it was finally paused and quasi-disestablished in 2011. Thereafter, the Bundeswehr became an all-volunteer army, which has since been faced with the mounting challenge of finding sufficient numbers of appropriate recruits. Hence, the goals of increasing the importance of the reserve force and of shifting responsibilities from active service members to reservists have gained popularity in recent years. A primary building block of the pertinent master plan of the Ministry of Defense (MoD) is the deployment of an efficient cyber reserve.

The Military Information and Cyber Domain Service (MCS) is in charge of organizing all aspects of the cyber reserve. The MCS is the youngest branch of the military part of Germany's federal defense force, which also includes the Army, Navy, Air Force, Joint Support Service and Joint Medical Service. It is responsible for the cyber, information technology (IT), military intelligence, geoinformation and operative communications units. Unlike the traditional branches of the military, the MCS can act largely autonomously.

The MoD's 2016 "Report on Cyber and Information Domain" addresses the key pillars of the military cyber reserve by formulating three primary goals:

1. The creation of additional forces that can temporarily support the MCS in the case of large-scale cyber attacks.
2. The building up of strong cyber units consisting of IT experts through mutual exercises and grouping.
3. Increasing cooperation and dialogue between IT experts of the private, public and military sectors.

Then-German Defence Minister Ursula von der Leyen speaks at a ceremony in Bonn in 2017 to launch a new cyber defense unit dedicated to thwarting and responding to cyber attacks. THE ASSOCIATED PRESS

To strengthen the cyber defense, the MoD recognized the importance of qualified personnel. To attract qualified recruits to the active military and the reserve, the Bundeswehr builds on three components centered on education: a new cyber security program offered at the Bundeswehr University; separate recruitment track opportunities for computer specialists who are not following the traditional military career pattern; and an increased integration of reservists, IT experts in particular. The last two components represent a challenge because of the heterogeneous structure of the distribution of IT know-how, both in society and in the pool of reservists. Moreover, MCS cadre and experienced reservists can reach the public through talks, panel discussions and other events in order to spark interest in either active MCS careers or in joining the cyber reserve. Trial military exercises at MCS units can also be advertised.

## CYBER DEFENSE **STRUCTURE**

In an April 2020 study, the ETH Zürich's Center for Security Studies compared the cyber reserve forces of Estonia, Finland, France, Israel, Switzerland and the United States. The ETH study found that the organizational forms of cyber reserves vary significantly due to the different bureaucratic and military cultures. Although France, the U.S. and the Netherlands have voluntary armies (like Germany), the preconditions for establishing a cyber reserve are rather different due to peculiarities in the educational systems, military structures and labor market landscapes.

In Germany, the setup of a new cyber reserve is tied to the establishment of regional branches of the MCS. In addition to MCS' reserve headquarters, four regional reserve outlets distributed across Germany will be expected to improve connectivity to the local cyber reserve landscape. Located in areas populated by IT specialists, the outlets are to be staffed by experienced reservists serving in rotation. This concept provides regional and local cyber expertise that may otherwise not be at the disposal of the Armed Forces.

Then-German Interior Minister Thomas de Maiziere stands before a map in 2017 showing the number of cyber attacks over a 30-day span.
THE ASSOCIATED PRESS

Another benefit of decentralizing the MCS reserve is becoming evident during the present COVID-19 pandemic: the geostrategic factor. Regular and reserve units in certain regions may be unable to perform their tasks at the necessary level of effectiveness, while such shortfalls may not affect other parts of the country. Assignments can be transferred to an MCS outlet that is fully operational and can be staffed by additional reserve members to compensate for any inefficiencies.

Considering the MoD's primary goals, the tasks of an MCS reserve outlet start with the allocation of attractive training opportunities for reservists together with the preparation, realization and analysis of cyber exercises, both from a curricular (such as contents) and a logistical perspective. This includes the organization of on-site and online cyber security competitions to gain the attention of computer-oriented talents and to stimulate their interest in military careers. Specific hardware and software components (such as a cyber range) will be needed to support the courses and exercises. MCS initially proposes that each cyber reservist, based on their IT background, can qualify for one of five major fields:

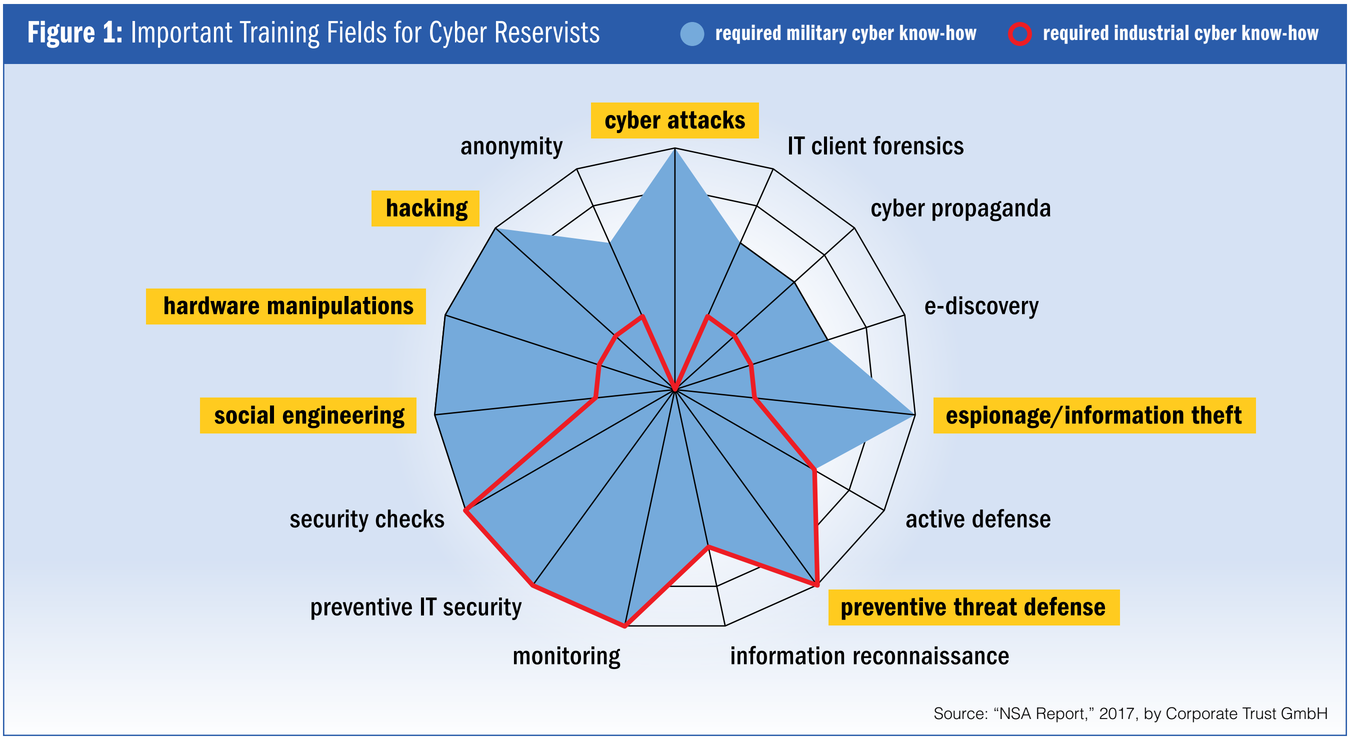
- **Red Team:** hacking simulations to test the resilience of computer infrastructure.
- **Cyber Intelligence:** gathering information about threats to reduce cyber risks.
- **Monitoring:** surveillance of networks, users and websites to identify failures and threats.
- **Open Source Intelligence (OSINT):** screening public internet sources for information.
- **Digital Forensics and Incident Response (DFIR):** examining digital components to identify illegal activity and implement a proper response in cases of proven cyber crime.

Other fields, such as those connected to the geoinformation tasks of MCS, may be identified in the future. Each outlet will identify the required skills potential reservists will need for a particular area of responsibility and will compile the qualifications of each reservist. Together with MCS headquarters, the outlets will develop general and individual qualifications for cyber reserve members. Once a reservist has been selected for one of the five fields, MCS will outline an individual training plan to develop the reservist into an expert.

When cyber incidents occur, the experts in each of the five fields should join their complementary expertise. Such a mitigation of cyber risks and the ability to cooperate can be tested in cyber security competitions. In addition, the cyber reserve should supply expertise in system administration, in the evaluation of the reliability and resilience of hardware and software products, in the installation of a secure network and in the protection of existing IT infrastructure. It should be familiar with organizational and communications aspects (public relations), be able to identify fake news, and be sensitized to issues of information security awareness. Finally, the reserve outlets cooperate with related organizations like the Bundeswehr Command and Staff College (Führungsakademie), Bundeswehr University, police academies and also with civilian institutions on all aspects of the cyber education of reservists. In particular, the outlets organize public events such as talks promoting the opportunities offered to prospective candidates by joining MCS or the cyber reserve.

The performance of the MCS reserve system can be challenged in national, international, or private-public-military cyber security competitions, which may feature capture the flag challenges, threat-hunting tasks, penetration-testing exercises and attack/defense simulations.

**Figure 1:** Important Training Fields for Cyber Reservists



Source: "NSA Report," 2017, by Corporate Trust GmbH

Cyber reservists will receive training in the areas of cyber attacks, espionage and information theft, preventive threat defense, social engineering, hardware manipulations and hacking.

While some problems constructed for competitions are designed to be solved by individuals, others are supposed to be tackled by teams composed of experts with specific abilities to distribute assignments.

## RESERVE TRAINING **CONCEPT**

The military cyber reserve's essential role is to provide units that can be activated rapidly to compensate for Bundeswehr personnel shortages during a military crisis (including cyber aggressions). One reason for the difficulty in recruiting sufficient active military cyber personnel is that about 30 other federal and state cyber authorities — such as the federal office for IT Security and the cyber security branches of state and federal criminal investigation offices — are relying on the same experts.

The private sector adds to the difficulties. Figure 1 compares key capabilities of cyber staff working on industrial and military cyber challenges. The 2017 publication, "NSA Report," from Corporate Trust, a German risk management company, has the detailed description of these capabilities. Monitoring, one of the major fields, is highly relevant to the industrial and military sectors. This means that MCS will try to motivate industry experts in this field to join the monitoring squad of the cyber reserve. A successful recruitment of monitoring experts will not need significant training because industry and military requirements in this field are similar.

Additionally, a big part of the "required military cyber know-how" cannot be recruited from the private sector because it simply is not available. For instance, it is difficult to find experts for the Red Team (or hacking squad) in industry. The need for proper continuous education and training of cyber reservists is obviously important. In particular, the education of Red Team members will represent a substantial challenge because hacking is neither a proper job description nor do any educational pathways yet exist.

Based on an analysis of desired capabilities and available resources, targeted courses can be developed and various deployment-oriented roles and ability profiles for the assembly of specialist teams can be defined. In the context of the five expert squads, from which the specialist teams will be formed, it should be pointed out that it is sufficient for members of a given squad to acquire purely theoretical knowledge in some of the 15 cyber areas defined in Figure 1, while acquiring practical computational experience, on top of a solid theoretical foundation, is essential in certain critical areas.

Table 1 provides for the five expert squads an exemplary assignment of theoretical and practical competences in six selected, representative cyber areas.

It is important that objective, verifiable criteria be used to assess available capacities. For this purpose, each cyber reservist will undergo a cyber fitness test before entering the training program. Analysis of the deviations between required and disposable qualifications allows for determining the number of participants, the curricula, location and timing of individual courses.

As already indicated, the training of Red Team members will be of particular relevance since it will be difficult for the cyber reserve to recruit candidates with expertise in offensive methods at a sufficiently high level.

Germany's government headquarters in Berlin were hacked by a Russian-backed group that infiltrated the secure computer networks in 2018.

THE ASSOCIATED PRESS

Figure 2 illustrates an example program based on which the MCS may configure a training schedule for a prospective Red Team member.

In this example, after completing the training program, the reservist should be an expert in three branches of "hacking science" of particular relevance: web exploitation, reverse engineering of software and binary exploitation. According to the example provided in Figure 2, this individual would require an upgrade in web exploitation and reverse engineering, while no immediate education in binary exploitation would be necessary.

Pathways are provided for the training of Red Team aspirants to become proficient in the three domains. In web exploitation, trainees need to reach expert level in penetration testing, i.e., in simulated cyber attacks to check for exploitable vulnerabilities of a computer system. In introductory theory courses, inexperienced attendees will be made familiar with KALI Linux and a selection of the more than 600 offensive tools offered by this platform. In the next step, apprentices will participate in tutorials demonstrating how KALI Linux tools can be applied to solve tasks supplied by the "Hack the box" server. To reach the next level, workshops, both featuring lectures and practical exercises, will address the solution of capture-the-flag challenges maintained by the security training tool Open Web Application Security Project Juice Shop.

Key for reverse engineering of software is the analysis of software to extract design and implementation information. To qualify for training in this field, a familiarity with Java and assembly is a precondition. In introductory courses, lectures on reversing and patching machine code and Java bytecode will be combined with tutorials. Follow-up workshops will demonstrate, both in theory and practice, how reverse engineering skills can be used to mitigate malware risks.

Finally, in binary exploitation, the subversion of binary code has the goal to access protected information. This is generally an advanced topic and an intermediate level in a programming language, like C, and assembly is mandatory to qualify for a preparation course. Here, lectures will first cover vulnerable

**Table 1**

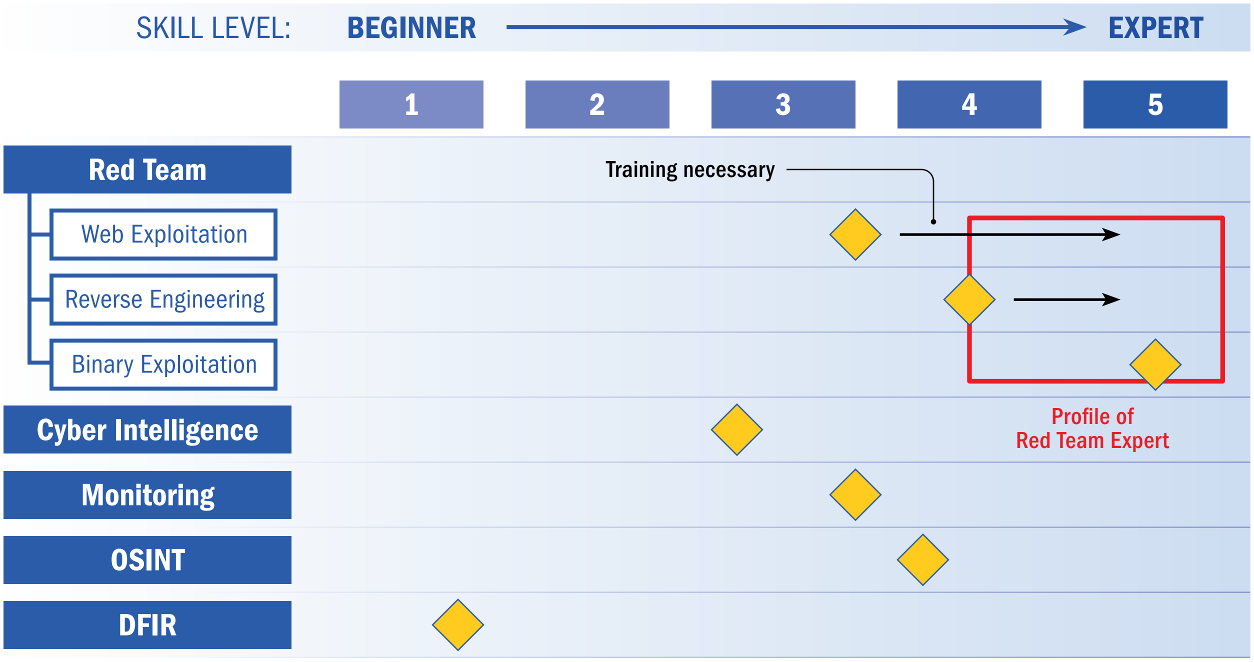
| | Hacking | Cyber Propaganda | Monitoring | Active Defense | Hardware Manipulation | Espionage / Information Theft |
|---|---|---|---|---|---|---|
| **Red Team** | P | T | T | T | T | T |
| **Cyber Intelligence** | T | P | T | T | T | P |
| **Monitoring** | T | T | P | T | T | T |
| **Open Source Intelligence** | T | P | T | T | T | T |
| **Digital Forensics Incident Response** | T | T | T | T | P | P |

**T** = theoretical competence **P** = practical competence

Source: Authors

This overview differentiates for members of the cyber reserve squads between practical (P) and theoretical (T) competences in six of the 15 cyber areas included in Figure 1. Theoretical competence in an area can be acquired by attending lectures covering subjects related to this area. Attaining practical competence in an area requires both theoretical background and actual computational experience.

**Figure 2:** Determining An Individual Training Schedule



Source: Authors

In this representation of a program for determining a training schedule, a reservist is trained to become a Red Team member, or hacking expert. Competence in hacking can be split into three subareas as shown. The initial skill levels of a reservist represented by the diamonds are determined by a cyber fitness test prior to the definition of the individual training program.

C functions, the use of simple exploits, the structure of the Global Offset Table, mitigations introduced in systems and essentials of Return Oriented Programming to avoid exploit mitigations. Next, trainees will have the opportunity to apply these techniques to binaries. Subsequently, workshops will focus on memory corruption, starting with instruction on how to exploit an overflow on Windows and proceeding to web browser exploitation. Teaching will be performed both in the form of lectures and tutorials.

## CONCLUSION

The German MoD recognized in 2016 that major cyber challenges for society and the Armed Forces can be addressed by a military cyber reserve. Moreover, cyber reservists are considered to be valuable multipliers of cyber awareness in society. The MoD acknowledged that reaching the goal of establishing a cyber reserve able to efficiently support MCS will require significant efforts to recruit sufficient numbers of qualified reservists and to ensure the education of members of the cyber reserve. In response to these demands, a new organizational structure of cyber defense is being developed for the purpose of integrating the cyber reserve with MCS. MCS reserve outlets will be distributed across the country to improve the recruitment of reservists and to secure the continuing education of members of the reserve force. In this article, we have outlined the plan to assemble a “model kit” of cyber experts with different specialization. MCS will tap this pool of cyber reservists to form teams able to cope with the requirements arising from supporting MCS in improving IT security and in countering various cyber threats. □

A worker in Efurt, Germany, transports a ballot box. Cyber attacks on critical infrastructure systems are a major concern of countries across the world.

THE ASSOCIATED PRESS