The Universität der Bundeswehr München (Bundeswehr University Munich) is significantly expanding its Cyber Defence Research Center (CODE). CODE was established in 2013 with the objective to bring together experts from different faculties and scientific disciplines as well as expertise from industry and government agencies to conduct research in the cyber and information space. CODE pursues a comprehensive, integrated, and interdisciplinary approach to implement technical innovations and concepts for the protection of data, software, and ICT infrastructures in accordance with legal and commercial framework conditions. It has already established important strategic partnerships in this area. The objective of the expansion is to unite the research initiatives of the Bundeswehr and the Federal Government in the area of Cyber Defence and Smart Data and to establish the CODE Research Center as the primary point of contact in the cyber and information domain of the Bundeswehr and the Federal Government.

Research and teaching in the area of cyber security is already being carried out as part of the Bachelor's and Master's programs in the Computer Science Department. According to current planning, a new international Master's program in Cyber Security will be launched on January 1st, 2018.

The Universität der Bundeswehr München will therefore be appointing eleven Professors for its Computer Science Department on October 1st, 2017.

The Universität der Bundeswehr München is looking for personalities with outstanding scientific qualifications to fill these professorial positions, who will also contribute actively to the CODE research center. Besides excellent research work, the new professors are expected to develop demanding lectures, practicals, and seminars for the new Master's program in Cyber Security and to provide excellent teaching in their respective specialist area. Applicants are also expected to carry out teaching in the Bachelor's programs in Computer Science and Business Informatics, and to work closely with the other departments at the Universität der Bundeswehr München.

The Professorships will be provided with eight excellently equipped laboratories housed in a new building that is to be completed in the near future.

The candidates must have an excellent scientific track record, as demonstrated by a habilitation or equivalent scientific achievements, as well as significant excellent publications in academic journals. Proven teaching experience in their respective specialist area is highly desired. The new Professors should have an international perspective, e.g., based on participation in international research projects, and experience in acquiring third-party funding. The duties will also include active participation in the university's academic self-administration.

The Computer Science Department at the Universität der Bundeswehr München is seeking Professors for the following specialist areas of its Cyber Defence und Smart Data Research Center:

**University Professorship (W3) in Cryptography**

When it comes to transmitting, storing, and processing data, cryptographic methods are crucial to ensure that the data remains confidential, authenticated, and uncorrupted.

The remit of the Professorship includes encryption algorithms, random number generators and key management as well as their practical application within communication protocols – both from a provider's and an attacker's perspective.

**University Professorship (W3) in ICT Threat and Malware Analysis**

The complexity and heterogeneity of communication networks and ICT infrastructures requires a systematic assessment of potential attack vectors in order to derive priorities for protection mechanisms. Besides malware as a mass phenomenon in the form of viruses, Trojan horses and encryption-based ransomware, the Professorship also focuses on constructing sandbox analysis environments to identify malicious code in third-party software, such as smartphone apps and other software downloaded from the web.

**University Professorship (W3) in Business Intelligence Security**

Networked applications, IT services, and operating environments generate vast amounts of data that can be used for various purposes, including the detection of potential attacks, but the sheer amount of such data prevents any manual processing. The research tasks involved in the Professorship in Business Intelligence Security include big data and smart data algorithms for the aggregation, the correlation, and the analysis of large data amounts associated with security events for the purpose of providing specific support for decision processes concerning the prevention, the detection, and the response to attacks.

**University Professorship (W3) in Cyber Physical System Security**

The combination of networked applications with mechanical and electronic components, such as in industrial production facilities, assistance systems, and energy supply systems, has many advantages – but it also involves the risk that these cyber physical systems can be compromised or sabotaged through cyber attacks.

The Professorship focuses on the information security characteristics of cyber physical systems with their specific framework conditions, such as the constrained resources of embedded systems, real-time capabilities, and physical access by attackers.
University Professorship (W3) in Data Protection and Compliance

The development and procurement of complex software systems must comply with legal and sector-specific regulations, which must already be taken into account during the requirements analysis and planning stage. Ultimately, proof of compliance must also be demonstrated, e.g., by means of a certification.

The Professorship in Data Protection and Compliance focuses on the methods and tools needed for the technical implementation of requirements resulting from, for example, the European General Data Protection Regulation and the new German IT Security Act, and it will also develop IT concepts for the implementation of the privacy-by-design paradigm.

University Professorship (W3) in Forensic Methods and IT Security

In order to fully investigate and resolve security incidents, evidence must be gathered and analyzed while maintaining the integrity of the chain of custody. In order to deal with sophisticated attacks that are increasingly leaving fewer traces in compromised IT systems, the concealment of traces, the use of encryption and, for example, requirements regarding the automation and the scalability of digital forensics, the Professorship will research new approaches to analyzing the main and background memories of mobile and stationary systems as well as networked applications, among other topics.

University Professorship (W3) in Open Source Intelligence and Situation Assessment

The situation assessment and documentation in cyber space as a basis for planning and decision processes can no longer be completely achieved using dedicated sensors and traditional reporting channels. Instead, the analysis of public sources, such as social media and internet communities, has become crucial to ensure the timeliness and correct focus of situation reports.

The Professorship in Open Source Intelligence and Situation Assessment will develop methods for continuous information gathering in networked environments using experience and findings from previous operations, as well as methods to compile clear and concise situation reports.

University Professorship (W3) in Privacy Enhancing Technologies

As users often act carelessly with their personal data and internet providers frequently favor commercial interests over protective measures, it is becoming easier and less risky for organized crime to commit, among other things, identity theft.

The Professorship in Privacy Enhancing Technologies will research new approaches to eliminate or at least minimize the unnecessary or unwanted disclosure of information during the use of networked applications and to ensure that stored data is not analyzed and forwarded to third parties without user consent.

University Professorship (W3) in IT Vulnerability Management and Security Testing

Programming errors, insufficient adaptation to new operating environments, and negligent use of IT systems often lead to vulnerabilities that allow attackers to obtain unauthorized access to processed data or even take control of entire systems.

The Professorship in IT Vulnerability and Security Testing will deal with the systematic handling of such vulnerabilities in IT systems and testing methods for their identification and assessment, so that, for instance, penetration tests of networked applications can be employed to determine areas in which the security levels need to be improved.

University Professorship (W3) in Secure Software Development

The security of software crucially depends on the priority assigned to information security attributes during the requirements analysis, system design, and programming as well as the associated testing and approval procedures.

In the Professorship in Secure Software Development, the two disciplines of software engineering and security engineering overlap. It deals with methods, algorithms, and tools required for the implementation of software according to the secure-by-design, secure-by-default, and secure-in-deployment paradigms.

University Professorship (W3) in Usable Security and Privacy

Information security and data protection necessitate the implementation and use of technical mechanisms that are too complex to apply for many users. E-mail encryption procedures, for instance, have only been utilized by IT experts for decades because the time and effort necessary for their use is much too high compared to their subjective benefits.

The Professorship in Usable Security and Privacy will investigate user-friendly approaches to security and data protection procedures and to the implementation of graphical interfaces for human-computer interaction in order to enhance the usability and therefore ensure the extensive employment of important protective measures.

The Universität der Bundeswehr München offers academic programs directed primarily at Officer Candidates and Officers, who can obtain Bachelor’s and Master’s degrees within a trimester system. Depending on spare capacity, civilian students are allowed to enroll. The study course is complemented by interdisciplinary elements in an integrated program entitled „studium plus“.

Preconditions of employment and the legal duty positioning of Professors are based upon the “Bundesbeamtengesetz”. Employment as a “Beamtin/Beamter” requires that the candidate is not older than 50 at the date of appointment.

The University seeks to increase the number of female Professors and thus explicitly invites women to submit applications. Severely disabled candidates with equal qualifications will receive preferential consideration.

Please submit your application documents marked as Confidential Personnel Matter to the Department Head of the Computer Science Department at the Universität der Bundeswehr München, 85777 Neubiberg, by October 15th, 2016.