BUMBLEBEE

cyBersecUrity prograMm für cyBer Kräfte mit einer miLitärischEn cyBEr rangE

Programm / Ausschreibung	FORTE, FORTE, F&E-Dienstleistungen (FED_2022)	**Status**	laufend
Projektstart	01.10.2023	**Projektende**	31.03.2026
Zeitraum	2023 - 2026	**Projektlaufzeit**	30 Monate
Keywords	Cyber Sicherheit, Cyber Range, Curriculum, Schulungen, Konzept Trainingsplattform		

Projektbeschreibung

BUMBLEBEE ist ein Projekt, das dem Bundesministerium für Landesverteidigung (BLMV) ermöglichen soll, zukünftige Cyber-Kräfte eigenständig, durch ein auf die Bedürfnisse und Anforderungen abgestimmtes Curriculum für Cyber-Security, auszubilden. Aufgrund der Digitalisierung und Vernetzung der staatlichen Infrastruktur ist es wichtig, dass Soldaten auch im Bereich der Cyber Abwehr geschult und eingesetzt werden können. Diese Ausbildung für Cyber-Kräfte soll über herkömmliche Ausbildungen an Hochschulen hinausgehen. Infolgedessen, wird durch BUMBLEBEE eine Trainingsplattform konzipiert, welche eine flexible Gestaltungsmöglichkeit von Infrastrukturen ermöglichen soll, unterschiedliche Bedrohungsszenarien beinhalten kann und unterschiedliche Operatoren involviert, militärische und zivile Domänen integriert, so wie nationale und internationale Zusammenarbeit bei der Bewältigung der Aufgaben fördert.
Des Weiteren zielt das Projekt BUMBLEBEE darauf ab ein Konzept zur Qualifizierung der Cyber Trainer für die Aus- und Weiterbildung von Cyber Kräften und Soldaten zu entwickeln. Daher wird zusätzlich ein Ausbildungslehrgang für die Cyber Trainer entwickelt, um die Trainer mit den notwendigen Fähigkeiten, Kompetenzen und Fertigkeiten im Bereich Szenario Entwicklung sowie IT, OT und militärische technische Komponenten design und Implementierung auszustatten. Dadurch sollen die Cyber Trainer befähigt werden selbstständig Szenarien zu entwerfen und technische Komponenten in der Cyber Range zu implementieren und dem BLMV wird es ermöglicht somit ihre eigenen Cyber-Kräfte und Cyber-Trainer auszubilden, ohne auf externe Unternehmen oder Organisationen angewiesen zu sein.

Abstract

The project BUMBLEBEE focuses on enabling the Federal Ministry of Defence (BLMV) to independently provide training in cyber security to future cyber forces through a tailored curriculum. With the digitalisation and networking of the state infrastructure, it is important that armed forces can also be prepared and deployed to deal with cyber defence. Such training for cyber forces is intended to go beyond conventional university programmes. Consequently, BUMBLEBEE will design a training platform which will allow flexible configuration of infrastructures, include different threat scenarios and engage different operators, integrate military and civilian domains, as well as promote national and international cooperation to accomplish the missions.
Furthermore, the BUMBLEBEE project focuses on developing a qualification concept for cyber instructors for the initial and further training of cyber forces and soldiers. Thus, an additional education and training programme for the cyber trainers is

developed in order to equip the instructors with the necessary skills, competences and abilities in the area of scenario development as well as IT, OT and military technical component system design and implementation. This will allow the cyber instructors to independently design and implement scenarios and technical components in the cyber range and enable the BLMV to train its own cyber forces and cyber instructors without relying on external entities or organisations.

Endberichtkurzfassung

Das Projekt Bumblebee hat eine wissenschaftlich fundierte und zugleich praxisorientierte Grundlage für die Aus- und Fortbildung militärischen Personals im Cyber- und Informationsraum geschaffen. Im Mittelpunkt stand die Frage, wie Personal in SOC- und NOC-nahen Funktionen so qualifiziert werden kann, dass sicherheitsrelevante Ereignisse frühzeitig erkannt, richtig eingeordnet, strukturiert dokumentiert und entlang definierter Prozesse weiterverarbeitet werden können. Der Projekt zeigt, dass hierfür nicht nur technisches Wissen erforderlich ist, sondern ein integrierter Ansatz, der fachliche, organisatorische, prozessuale und didaktische Anforderungen miteinander verbindet. Ein zentrales Ergebnis des Projekts ist die systematische Bedarfsanalyse für militärische Cyberausbildung. Diese hat gezeigt, dass der Qualifizierungsbedarf nicht primär in der Ausbildung hochspezialisierter Expertinnen und Experten liegt, sondern vor allem in der Befähigung von Personal für operative Erstreaktions-, Überwachungs- und Unterstützungsaufgaben. Besonders relevant sind dabei Kompetenzen in der Früherkennung sicherheitsrelevanter Ereignisse, der strukturierten Lagebeurteilung, der regelgeleiteten Eskalation sowie der nachvollziehbaren Dokumentation und Kommunikation. Die Analysen und Workshops machten außerdem deutlich, dass ein tragfähiges Ausbildungsprogramm heterogene Eingangsvoraussetzungen berücksichtigen, praxisnah gestaltet und eng an realistischen Einsatz- und Bedrohungsszenarien ausgerichtet sein muss. Darauf aufbauend wurde im Projekt ein technisches Zielbild für eine integrierte Trainingsumgebung entwickelt. Dieses Zielbild geht über klassische Lernplattformen oder isolierte Einzelübungen hinaus. Konzipiert wurde eine Trainingsumgebung, die Hands-on-Labs, Cyber-Range-Szenarien, föderierte Übungen und bei Bedarf auch Hardware-in-the-Loop-Elemente auf einer gemeinsamen, reproduzierbaren und sicher betreibbaren Grundlage zusammenführt. Besonders wichtig ist dabei die Ausrichtung auf einen hochsicheren, möglichst vom Internet entkoppelten Betrieb. Mit der Entwicklung zweier Referenzarchitekturen – einer VM-zentrierten und einer cloud-nativen Variante – wurden nicht nur technische Lösungsoptionen beschrieben, sondern auch ein belastbarer Entscheidungsrahmen geschaffen, der Sicherheitsanforderungen, Skalierbarkeit, Betriebsaufwand, Integrationsfähigkeit und Governance systematisch berücksichtigt. Damit liegt ein tragfähiger Referenzrahmen für den Aufbau einer militärisch anschlussfähigen Trainingsplattform vor. Ein weiteres Kernergebnis ist die Entwicklung eines strukturierten Curriculums für das zukünftige militärische SOC- und NOC-Personal. Das Curriculum wurde als kompetenzorientiertes, praxisnahes und spiralförmig aufgebautes Ausbildungsmodell konzipiert. Es verbindet Basisausbildung, gemeinsame operationelle Wissensgebiete, rollenbezogene Spezialisierungen sowie integrative Abschlussübungen zu einer kohärenten Ausbildungsarchitektur. Von besonderer Bedeutung ist dabei, dass ein gemeinsames begriffliches und prozessuales Fundament mit differenzierten Vertiefungen für SOC- und NOC-Rollen kombiniert wird. Dadurch wird nicht nur die individuelle Qualifizierung gestärkt, sondern auch die Zusammenarbeit zwischen Rollen, Teams und Organisationsbereichen verbessert. Das Curriculum übersetzt die Ergebnisse der Bedarfsanalyse und die Möglichkeiten der Trainingsumgebung in konkrete Lernziele, Module und didaktische Formate und leistet damit einen wesentlichen Beitrag zur Sicherstellung der Führungs- und Einsatzfähigkeit der Streitkräfte im Cyber- und Informationsraum. Hervorzuheben ist die didaktische Weiterentwicklung des Ausbildungsansatzes im Projektverlauf. Die Evaluierungen der Übungen zeigten deutlich, dass reine Kombinationen aus Theorieblöcken und nachgelagerten Übungen nicht ausreichen, um die angestrebte Handlungskompetenz wirksam aufzubauen. Aus den Rückmeldungen wurde deshalb ein grundlegender didaktischer Wandel abgeleitet: weg von einer

lehrveranstaltungsähnlichen Struktur, hin zu stärker szenario- und praxisbasierten, zusammenhängenden Lernformaten. Diese Neuausrichtung erwies sich als richtig. Vor allem Cyber-Range-Szenarien, eingebettete praktische Aufgaben und eine schrittweise Vorbereitung auf Werkzeuge und Infrastruktur wurden von der Zielgruppe als besonders lernwirksam wahrgenommen.

Ein Erfolgsfaktor des Projekts war die empirische Validierung durch vier (Cyber-) Übungen . Diese Übungen dienten nicht nur der Demonstration, sondern auch der iterativen Überprüfung und Weiterentwicklung des Curriculums, der Trainingsunterlagen und der technischen Umgebung. Die dritte Übung bestätigte bereits die Überlegenheit eines stärker szenariobasierten und praxisorientierten Zugangs. Die abschließende vierte Übung im März 2026 zeigte schließlich, dass das überarbeitete Curriculum mit seinem mehrtägigen, aufeinander aufbauenden Trainingsdesign unter realitätsnahen Bedingungen tragfähig ist. Besonders die Cyber-Range-Übung erwies sich erneut als das didaktisch wirksamste Element des Gesamtformats. Ebenso wurde bestätigt, dass die gezielte Vorbereitung auf Analysewerkzeuge und die Trainingsinfrastruktur Einstiegshürden reduziert und den Kompetenzaufbau deutlich unterstützt. Insgesamt konnten Curriculum und Trainingsunterlagen damit erfolgreich unter realitätsnahen Bedingungen erprobt und als relevanter, belastbarer Rahmen für zukünftige Ausbildungsformate validiert werden. Über die einzelnen Arbeitsergebnisse hinaus liegt ein weiterer wichtiger Projekterfolg in der konzeptionellen Geschlossenheit des Gesamtansatzes. Bumblebee hat nicht nur einzelne Materialien, Module oder technische Konzepte hervorgebracht, sondern einen konsistenten Referenzrahmen entwickelt, in dem Bedarfsanalyse, Trainingsumgebung, Curriculum und Evaluierung ineinandergreifen. Damit wurde keine isolierte Schulungsmaßnahme geschaffen, sondern eine belastbare Grundlage für die schrittweise Institutionalisierung militärischer Cyber-Ausbildungsfähigkeit. Zugleich wurde deutlich, dass die langfristige Wirksamkeit eines solchen Programms von kontinuierlicher Qualitätssicherung, Lessons Learned und einer systematischen Weiterentwicklung abhängt. Auch dafür liefert das Projekt wesentliche Grundlagen. In der Gesamtschau leistet das Projekt Bumblebee damit einen substanziellen Beitrag zur Stärkung militärischer Handlungsfähigkeit, organisationaler Resilienz und professioneller Reaktionsfähigkeit im Cyber- und Informationsraum. Die Ergebnisse zeigen, dass wirksame militärische Cyberausbildung dann besonders erfolgreich ist, wenn sie technische Inhalte mit organisationalen Prozessen, realitätsnahen Trainingsumgebungen und evidenzbasiert weiterentwickelten didaktischen Formaten verbindet. Mit Bumblebee liegt hierfür nun eine tragfähige, wissenschaftlich fundierte und praktisch erprobte Grundlage vor.

The Bumblebee project has established a science-based and practical foundation for the training and professional development of military personnel in the cyber and information domain. The focus was on how personnel in roles related to SOCs and NOCs can be trained to ensure that security-related incidents are detected at an early stage, correctly classified, documented in a structured manner, and processed in accordance with defined procedures. The project demonstrates that this requires not only technical knowledge, but an integrated approach that combines technical, organisational, procedural and didactic requirements. A key outcome of the project is the systematic needs analysis for military cyber training. This has shown that the training requirement lies not primarily in the training of highly specialised experts, but above all in equipping personnel for operational first-response, monitoring and support tasks. Particularly relevant here are competencies in the early detection of security-relevant events, structured situation assessment, rule-based escalation, and traceable documentation and communication. The analyses and workshops also made it clear that a viable training programme must take into account heterogeneous entry requirements, be designed to be practical, and be closely aligned with realistic

operational and threat scenarios. Building on this, the project developed a technical target vision for an integrated training environment . This target vision goes beyond traditional learning platforms or isolated individual exercises. A training environment was designed that brings together hands-on labs, cyber range scenarios, federated exercises and, where required, hardware-in-the-loop elements on a common, reproducible and securely operable basis. Of particular importance here is the focus on highly secure operation that is decoupled from the internet as far as possible. The development of two reference architectures – a VM-centred and a cloud-native variant – not only described technical solution options but also created a robust decision-making framework that systematically takes into account security requirements, scalability, operational overhead, integrability and governance. This provides a viable reference framework for the development of a training platform compatible with military requirements. A further key outcome is the development of a structured curriculum for future military SOC and NOC personnel. The curriculum was designed as a competence-oriented, practical and spiral-structured training model. It combines basic training, shared operational knowledge areas, role-specific specialisations and integrative final exercises into a coherent training architecture. Of particular importance here is the combination of a common conceptual and procedural foundation with differentiated specialisations for SOC and NOC roles. This not only strengthens individual qualifications but also improves collaboration between roles, teams and organisational units. The curriculum translates the results of the needs analysis and the capabilities of the training environment into concrete learning objectives, modules and didactic formats, thereby making a significant contribution to ensuring the command and operational capability of the armed forces in the cyber and information domain. Of particular note is the didactic refinement of the training approach over the course of the project. The evaluations of the exercises clearly showed that mere combinations of theory blocks and subsequent exercises are insufficient to effectively build the desired operational competence. A fundamental didactic shift was therefore derived from the feedback: away from a lecture-style structure, towards more scenario- and practice-based, coherent learning formats. This reorientation proved to be the right approach. In particular, cyber range scenarios, embedded practical tasks and a step-by-step introduction to tools and infrastructure were perceived by the target group as particularly effective for learning.

A key factor in the project’s success was the empirical validation through four (cyber) exercises . These exercises served not only as demonstrations but also for the iterative review and further development of the curriculum, training materials and technical environment. The third exercise already confirmed the superiority of a more scenario-based and practice-oriented approach. The final fourth exercise in March 2026 ultimately demonstrated that the revised curriculum, with its multi-day, progressive training design, is viable under realistic conditions. The cyber range exercise in particular once again proved to be the most effective didactic element of the overall format. It was also confirmed that targeted preparation for analytical tools and the training infrastructure reduces entry barriers and significantly supports the development of competencies. Overall, the curriculum and training materials were thus successfully tested under realistic conditions and validated as a relevant, robust framework for future training formats. Beyond the individual deliverables, a further key project success lies in the conceptual coherence of the overall approach. Bumblebee has not merely produced individual materials, modules or technical concepts, but has developed a consistent reference framework in which needs analysis, the training environment, the curriculum and evaluation are interlinked. This has not created an isolated training measure, but a robust foundation for the gradual institutionalisation of military cyber training capability. At the same time, it became clear that the long-term effectiveness of such a programme depends on continuous quality assurance, lessons learnt and systematic further development. The project also provides essential foundations for this. Taken as a whole, the Bumblebee project thus makes a substantial contribution to strengthening military operational capability, organisational resilience and professional responsiveness in the cyber and information domain. The results show that effective military cyber training is particularly

successful when it combines technical content with organisational processes, realistic training environments and evidence-based, further-developed didactic formats. With Bumblebee, a viable, scientifically sound and practically proven foundation for this is now in place.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Landesverteidigung