Hochschule Kempten
University of Applied Sciences

Planungsamt der Bundeswehr

Masterarbeit

„IT-Sicherheitsaudit kritischer Netzwerk-Infrastruktur bei Unternehmen und Behörden nach IT-Grundschutz des BSI, am Beispiel komplexer Netzwerkstrukturen in Netzen der Bundeswehr“

Prüfer: Herr Prof. Dr. Arnulf Deinzer (Hochschule Kempten)

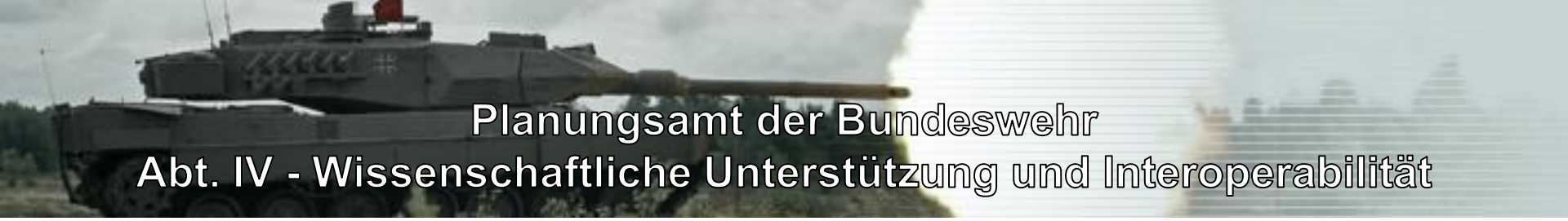
Verfasser: Florian Waibel

Kontakt: f.m.waibel@gmail.com

Betreuer: Hptm. Dirk Fickbohm
Hptm. Torsten Hedwig

Durchgeführt bei: Planungsamt der Bundeswehr

Kontakt Firma: Planungsamt der Bundeswehr
Abt. IV - Wissenschaftliche Unterstützung und Interoperabilität
Einsteinstraße 20
D – 82024 Taufkirchen
www.planungsamt.bundeswehr.de



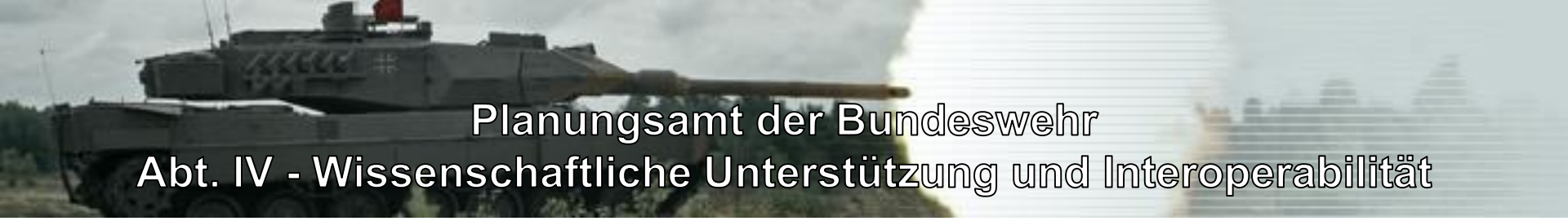
Planungsamt der Bundeswehr
Abt. IV - Wissenschaftliche Unterstützung und Interoperabilität

Übergeordnetes Ziel der Abteilung Wissenschaftliche Unterstützung und Interoperabilität ist es, **neue Entwicklungen** aus Wissenschaft und Technik sowie aus den Einsätzen frühzeitig zu **erkennen** und ihren **Nutzen** für die Bundeswehr zu **bewerten**.

Hierzu erfolgt die **IT-Unterstützung** (IT-U) für die Anwendung der Methoden **Concept, Development & Experimentation** (CD&E), **Operations Research** (OR), **Modelbildung & Simulation** (M&S) und **Architekturen** für das Planungsamt der Bundeswehr.

Hierzu wird der **Betrieb** der mobilen und stationären **IT- und Laborinfrastruktur** einschließlich der Anbindung der Simulations und Testumgebung der Bundeswehr (SuTBw) zur Unterstützung des Integrierten Planungs Prozesses (IPP) für **Einstufungen der Informationen bis Verschlußsache** (VS) GEHEIM/NATO SECRET/SECRET (Europa) EU **sichergestellt**.

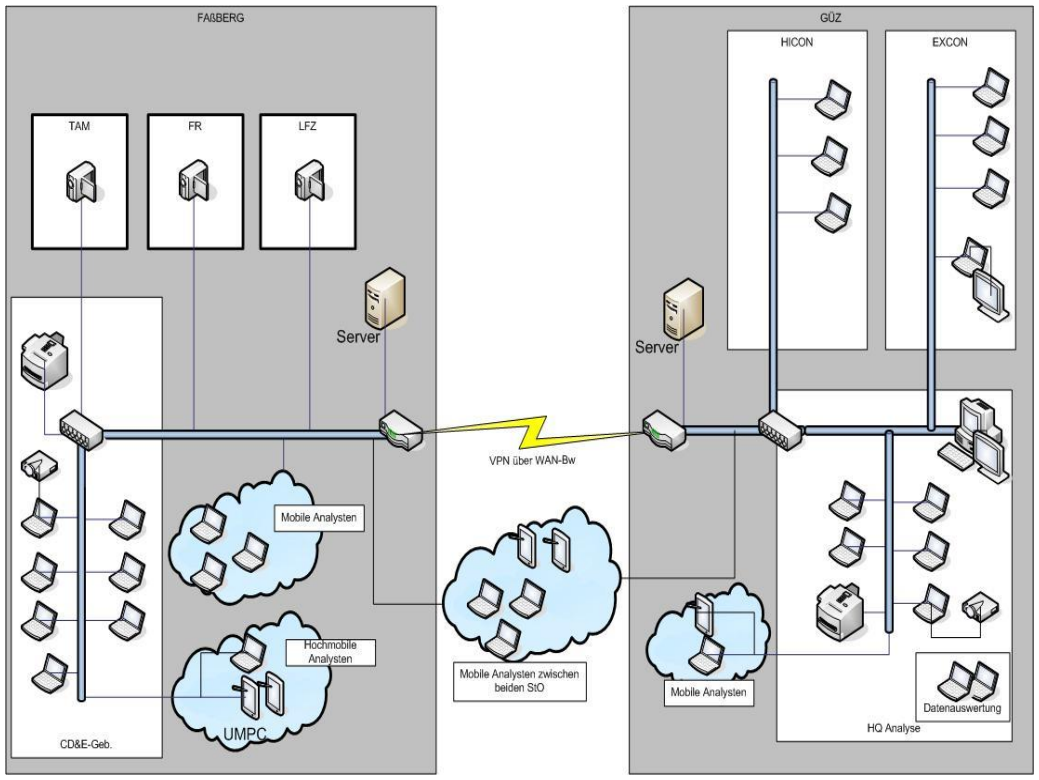
Ein **weiterer Auftrag** sind **Test und Evaluierung** (T&E) von **Software**, **Werkzeugen** und **Simulationen/Simulationssystemen**.



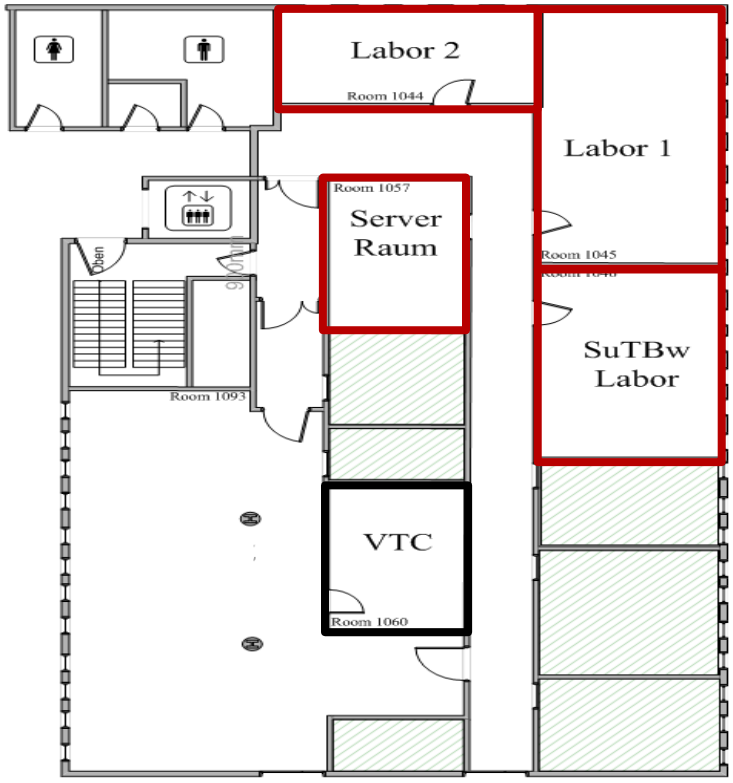
Planungsamt der Bundeswehr
Abt. IV - Wissenschaftliche Unterstützung und Interoperabilität

Die Unterstützung und Erprobung erfolgt sowohl bei der Truppe (auch über mehrere Standorte) als auch einer abgesicherten Laborumgebung. Hierzu sind **alle IT-Sicherheitsmaßnahmen der Bundeswehr** als auch des **BSI-Grundschutzes** zu berücksichtigen und ein **Auditing (gemäß ISO 27001)** der Netze (VS-Geheim bis Öffentlich) inklusive der Netzübergänge sicherzustellen.

Mobiler Aufbau eines Netzes



Stationärer Aufbau eines Netzes



Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheitsaudit nach IT-Grundschutz des BSI

Als **IT-Sicherheitsaudit** werden Maßnahmen zur Risiko- und Schwachstellenanalyse eines IT-Systems bezeichnet.

Ein **Audit** ist ein systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und deren objektiver Auswertung, zur Ermittlung inwieweit die Auditkriterien erfüllt sind.[1]

Es werden unter anderem Gewährleistung der **Vertraulichkeit**, **Integrität**, **Verfügbarkeit**, **Authentizität**, **Verantwortlichkeit**, **Verbindlichkeit** und **Verlässlichkeit von Daten** überprüft.

Die **IT-Grundschutz**-Vorgehensweise stellt zusammen mit den IT-Grundschutz-Katalogen des BSI und dessen Empfehlungen von Standard-Sicherheitsmaßnahmen inzwischen einen **De-Facto-Standard für IT-Sicherheit in Deutschland** dar.

[1] Begriffsbestimmung ISO 19011:2011-12 Ziffer 3.1

Aufgabenabgrenzung der Masterarbeit:

- **Beschreibung der Vorgehensweise zur Sicherstellung der IT-Sicherheit nach BSI Grundschutz**
- **Beschreibung der Planung und Durchführung eines IT-Sicherheitsaudits nach ISO Reihe 27000 und 19011**
- **Berücksichtigung besonderer Sicherheitsvorgaben bei hocheingestuften Informationen**
- **Audit an einem Netzwerk der Bundeswehr mit verschiedenen Subnetzen und einem Sicherheitsgefälle der eingestuften Informationen in einer abgesicherten Umgebung**
- **Ergebnissicherung und Standardisierung eines Auditkonzeptes**