



Sicherheit



YNSIDE

ynside.extranet-bw.de

INFOS AUS DER BUNDESWEHR AUCH UNTERWEGS



BUNDESWEHR

INTRO



Im Informationskrieg

In einer zunehmend digitalisierten Welt wird Datensicherheit immer wichtiger. Für die Bundeswehr gehört der Schutz der eigenen Informationen ebenso zu einem durchdachten Sicherheitskonzept wie der Schutz der eigenen Liegenschaften, des Personals und Materials. Gefahren drohen nicht nur durch direkte Angriffe, sondern auch durch gezielte Desinformationskampagnen und Propaganda. Dem wirkt die Bundeswehr mit transparenter Informationsarbeit und Aufklärung entgegen. Das Thema Sicherheit betrifft also in vielerlei Hinsicht nicht nur die digitale Welt, sondern ist auch ein Kampf um Informationen.

Titel: Y/C3 Visual Lab, Kollage
S. 3: Shutterstock/Avocado_studio

Zum Schutz der Truppe

Damit die Bundeswehr ihren Auftrag erfüllen kann, muss sie sich selbst schützen.

Keine leichte Aufgabe für eine Organisation mit über 260.000 Angehörigen und rund 1.500 Liegenschaften im In- und Ausland – aber unverzichtbar.

TEXT Florian Stöhr

Gefahren erkennen

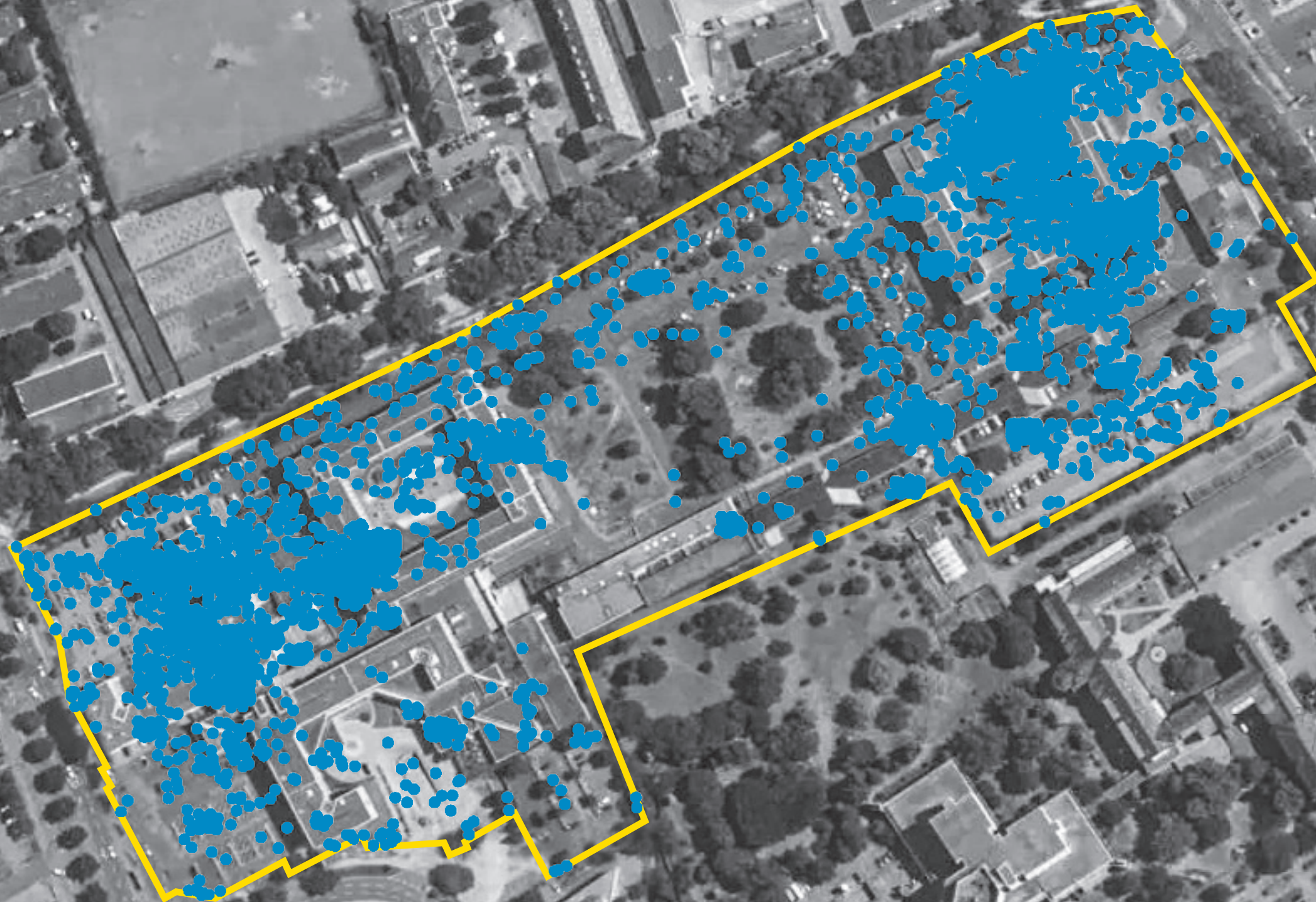
Sie war ursprünglich für Mali gedacht, jetzt ist sie in Deutschland im Einsatz. Die Bundeswehr hat 2024 drei Exemplare der schnell verlegbaren Fahrzeugdurchleuchtungsanlage erhalten. Das Röntgensystem besteht aus einem spezialisierten Lkw, dem Eagle M60, und einer Kontrolleinheit, die in mehreren Hundert Metern Entfernung stehen kann. Die Bildauswerter können so aus sicherer Distanz ein Fahrzeug inspizieren, das in eine Dienststelle fahren will. Ihnen bleibt dabei nichts verborgen – weder unbedenkliche Ladung noch versteckte Waffen. Denn selbst dicke Stahlwände sind kein Hindernis für das System. Zwölf Fahrzeuge können pro Stunde untersucht werden.



S. 4–5: Rapiscan Systems Ltd/Eagle® M60

Hightech schützen

Ohne IT-Unterstützung geht in militärischen Operationen nichts mehr. Das Gefechtsfeld wird immer vernetzter und digitaler. Hier im Bild bedient ein Soldat das neue Battle Management System im Kampfpanzer Leopard 2. Das Führungssystem ermöglicht es, Informationen interoperabel und in Echtzeit zwischen Gefechtsständen und Kampfeinheiten auszutauschen. Die Vorteile liegen auf der Hand: Wenn alle Einheiten auf ein ständig aktualisiertes Lagebild zugreifen können, dann können sie schneller, präziser und effektiver kämpfen. Vorausgesetzt, die Systeme werden nicht gezielt vom Feind gestört. Je komplexer Technologien sind, desto wichtiger sind ihr Schutz und ihre Durchhaltefähigkeit.



Schwachstelle Mensch

Smartphones, Smartwatches und Co. zeichnen unsere Standortdaten auf. Eine Recherche des Bayerischen Rundfunks und netzpolitik.org brachte zutage, wie leicht staatliche Einrichtungen durch die Bewegungsprofile der Beschäftigten ausspioniert werden können. Koordinaten, Zeitangaben und Gerätekennungen – viele App-Anbieter verkaufen die erhobenen Standortdaten, zum Beispiel an die Werbeindustrie. Die Informationen sind aber auch für ausländische Nachrichtendienste sehr interessant. Vom Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) in Koblenz wurden bei der Recherche 7.356 Standortdaten von 220 Werbe-IDs ausgewertet. Die Daten zeigen, wo die Soldatinnen und Soldaten sowie Zivilbeschäftigten besonders häufig aufeinandertreffen und sich austauschen.



Sicherheit für uns alle

Editorial

Die Bundeswehr ist ein wichtiger Faktor für die Sicherheit Deutschlands. Rund 260.000 Soldatinnen und Soldaten sowie Zivilbeschäftigte tragen mit dazu bei, dass die Menschen in Frieden und Freiheit leben können. In einer Zeit, in der Deutschland und seine Partner mit vielen äußeren Bedrohungen konfrontiert sind, braucht es gute Streitkräfte. Sie müssen einsatzbereit und kriegstüchtig sein, um äußere Feinde abzuschrecken und Gefahren von Deutschland und seinen Bündnispartnern fernzuhalten.

Damit die Bundeswehr ihren Kernauftrag, die Landes- und Bündnisverteidigung, erfüllen kann, muss sie selbst sicher sein. Seit Russlands völkerrechtswidrigem Angriff auf die Ukraine im Februar 2022 haben die Zwischenfälle in militärischen Liegenschaften und im Cyber- und Informationsraum deutlich zugenommen. Das ist kein Zufall: Der Militärische Abschirmdienst, kurz MAD, schreibt in seinem Jahresbericht 2023, dass die Bundeswehr im Fokus ausländischer Nachrichtendienste steht, allen voran aus Russland, aber auch aus China. Spionagefälle, Drohnenüberflüge, Einbrüche und hybride Angriffe – die Hintergründe und Drahtzieher lassen sich oft nicht herausfinden. Was man aber sagen kann: Autoritäre Staaten interessieren sich sehr für die Bundeswehr

und ihre Fähigkeiten. Viele Menschen in Uniform und Zivil sorgen deshalb tagtäglich dafür, dass die Bundeswehr geschützt wird. Ihre genaue Zahl dürfen wir nicht nennen, das würde den Falschen in die Hände spielen. Aber klar ist: Vom IT-Schutz über die Abwehr von Spionage und Cyberangriffen bis zur Abschirmung schutzbedürftiger Räume – die Menschen schützen unsere Truppe.

In der neuen Ausgabe widmen wir uns dem Thema Sicherheit in der Bundeswehr. Wir wollen die Akteure und Instrumente beleuchten, die dazu beitragen. Unser Ziel zeigt sich bereits auf dem Cover: Wer genau hinsieht, der erkennt, dass sich die ersten Seiten spiegelverkehrt auch auf dem Cover wiederfinden. Wie bei einem Röntgenbild könnt ihr hier einen ersten Blick ins Heft werfen. Wir wollen damit zum Ausdruck bringen, dass wir ein Thema, das sich der allgemeinen Wahrnehmung häufig entzieht, sichtbar und transparent machen – soweit, wie es die Sicherheitslage zulässt.

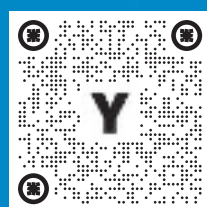
Die Zeiten haben sich verändert. Das betrifft auch die Informationsarbeit der Truppe. Y trägt – wie die anderen Kanäle der Redaktion der Bundeswehr – dafür Sorge, dass unsere Protagonistinnen und Protagonisten geschützt sind. Deshalb haben wir in dieser Ausgabe erstmals alle

Personennamen anonymisiert. Ausgenommen sind davon nur Führungskräfte, die aufgrund ihrer Funktion mit ihrem Klarnamen in der Öffentlichkeit stehen. Wir tun dies nicht, um etwas zu verbergen, sondern zur Sicherheit der Menschen, die uns von ihrer Arbeit erzählen und von deren Erfahrung und Expertise wir leben.

Zurück zum Heft: Wir sind in Litauen gewesen, um der Frage nachzugehen, wie die ersten Angehörigen der neuen Brigade an der NATO-Ostflanke für ihre Sicherheit sorgen. In unserem Infoklapper veranschaulichen wir die Sicherheitsmaßnahmen in Kasernen in Deutschland. Den obersten Cyberschützer der Bundeswehr haben wir gefragt, wie unsere IT und Kommunikation geschützt werden. Außerdem erfahrt ihr im Heft, wie der MAD gegen Spionage vorgeht und warum die Sicherheitsüberprüfung keine lästige Angelegenheit ist, sondern zu unser aller Schutz durchgeführt wird.

Jeder Einzelne kann zur Sicherheit der Bundeswehr ein kleines Stück beitragen. Das gilt auch für Y und dieses Heft. Viel Spaß beim Lesen!

Die Y-Redaktion



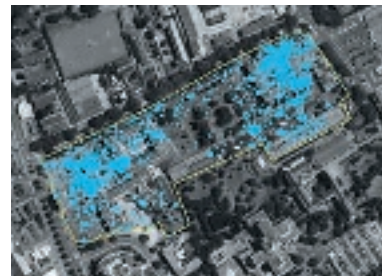
Hol dir die digitale Y!

Für alle Bundeswehrangehörigen mit einem Yinside-Zugang gibt es hier das Y-Magazin digital: browseroptimiert und an alle Bildschirme angepasst. Dazu gibt es viele Extras wie animierte Infografiken und zusätzliche Inhalte. Probiere die digitale Y jetzt aus!

Das ganze Heft in 15 Minuten

Eine eigene Ausgabe zum Thema Sicherheit? Ist die Bundeswehr nicht selbst Garant für die Sicherheit Deutschlands und seiner Bürgerinnen und Bürger? Ja, und trotzdem oder gerade deswegen muss auch der Eigenschutz der deutschen Streitkräfte auf dem neuesten Stand sein. Y erklärt die Sicherheitsarchitektur der Bundeswehr und beleuchtet die wichtigsten Aspekte.

Intro



Zum Schutz der Truppe

Die Bundeswehr ist für die Sicherheit Deutschlands zuständig und muss sich dabei auch selbst schützen.

- Fahrzeugdurchleuchtungsanlagen sorgen für die Absicherung von Bundeswehrliegenschaften.
- Auf dem Gefechtsfeld sorgt moderne Informationstechnik für Schutz und Durchhaltefähigkeit.
- Ein Bewusstsein für potenzielle Schwachstellen, wie leicht zu trackende Smartphones oder Smartwatches, sorgt für mehr Vorsicht im Umgang mit IT-Technik.

So ist die Bundeswehr rundum sicher – sowohl im hochagilen Gefechtsszenario als auch im Friedensbetrieb.

Seite 04–09

S. 12: Rapiscan Systems Ltd/Eagle M60 (c); Bundeswehr/Marco Dorow (m); ©BR/MapTiler/OpenStreetMap contributors; in Lizenz der BMedia Service GmbH (u); S. 13: Bundeswehr/Diorg Huttenlocher (ES-1-4); Bundeswehr/Arne Weyand (Z-So.unt); Y/C3 Visual Lab; Infografik (Z.S.u.); Y/C3 Visual Lab; Infografik (D.S.1-3)

Kapitel 1 – Brennpunkte



Im Fokus des Gegners

Wie wappnen sich Soldatinnen und Soldaten der Brigade Litauen gegen mögliche Ausspähung durch Russland? Y hat einen Stabsfeldwebel einen Tag lang begleitet.

- Worauf muss er bei der Nutzung seines Smartphones achten – dienstlich und privat?
- Worauf müssen er und seine Kameraden in der Öffentlichkeit Rücksicht nehmen?
- Wie schützt er seine mitgereiste Familie am besten?

Seite 19–26

Unter Kontrolle

Die Spionage- und Sabotageversuche gegen Liegenschaften der Bundeswehr nehmen zu. Auf welche Gefährdung in welcher Weise reagiert wird, ist individuell festgelegt.

- Abhängig von den jeweiligen sicherheitsrelevanten Gegebenheiten werden die Liegenschaften in Bewachungskategorien eingeteilt.
- Außerdem sind die Gefährdungsstufen wichtig, die sich aus der jeweils aktuellen Bedrohungslage ergeben.

Welche Maßnahmen ergriffen werden können, liest du hier.

Seite 28–35



Gefährdungsstufen	
Alpha	Bravo
Charlie	Delta



Halt, stehen bleiben!

Die Infografik zeigt, welche Maßnahmen zur Sicherung der Liegenschaften in welcher Gefährdungsstufe greifen.

- Alpha: Die allgemeine Gefährdungslage gilt seit 2002 für alle Liegenschaften.
- Bravo: Sich verdichtende Erkenntnisse lassen auf erhöhte Gefährdung schließen.
- Charlie: Ein Zwischenfall tritt auf oder eine erkennbare Bedrohung steht bevor.
- Delta: Eine unmittelbare Bedrohung mit gesicherten Erkenntnissen liegt vor.

Auf welche Gefährdung wie reagiert werden soll, zeigt die Infografik.

Seite 36–37

Kapitel 2 – Cyberraum ▶

**Sicher auf allen Ebenen**

Die Bundeswehr hat aufgrund ihrer einzigartigen Aufgaben ganz besondere Fähigkeiten und Befugnisse, die ein erhöhtes Sicherheitsbewusstsein erfordern.

- Auch bei der Bundeswehr gelten Arbeits- und Betriebsschutzgesetze.
- Darüber hinaus fordert der Umgang mit Waffen seine eigenen Schutzmaßnahmen.
- Als staatliches Sicherheitsorgan ist die Bundeswehr besonderen Gefahren ausgesetzt.

Einen Überblick zur Sicherheitsarchitektur der Bundeswehr findest du hier.

Seite 38–42

**Angriffe im Netz**

Der Kommandeur des Zentrums für Cyber-Sicherheit der Bundeswehr (ZCSBw), Oberst Andreas Kubitz, erklärt ...

- welchen Angriffen und Gefahren die Bundeswehr im Cyberraum ausgesetzt ist,
- wie sein Kommando diesen Attacken begegnet
- und wer die Akteure des neuen digitalen Gefechtsraums sind.

Das vollständige Interview gibt es hier.

Seite 45–50

CYBERCRIME GRUPPEN
FANCY BEAR,
VELVET CHOLIMA,
DARKHOTEL & CO.



Sicherheitsvorfälle
hat das ZCSBw 2023 bearbeitet.

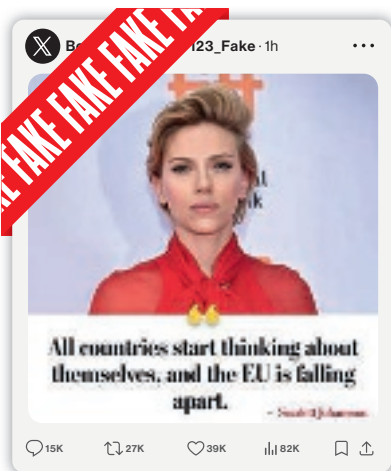
**Krieg mit Lügen**

Falschinformationen aus Russland sollen die Öffentlichkeit in westlichen Ländern verunsichern und beeinflussen.

- Wie geht Russland dabei vor?
- Welche besonders dreisten Falschinformationen werden verbreitet?
- Wie unterscheidest du seriöse Nachrichten von Falschmeldungen?

Antworten zu diesen und weiteren Fragen zu den Hintergründen kannst du hier nachlesen.

Seite 52–57



S. 14: Bundeswehr/Tom Twardy (E.S.o.); Bundeswehr/Marco Dorow (E.S.m.u.); Bundeswehr/Alf Ramana (E.S.o.); Shutterstock/Phil. Pickface (E.S.u.); Picture Alliance/Associated Press (E.S.o.); Shutterstock/Phil. Pickface (E.S.u.); Picture Alliance/Associated Press (E.S.o.); Shutterstock/Phil. Pickface (E.S.u.); S. 18: 2 Agenten/Jülich-Nachrichten (E.S.1–4); Marie Saathoff, Illustration (E.S.1–3); Y/C3 Visual Lab, Infografik (E.S.1–3)

**7 Lifehacks für mehr Sicherheit**

Gegen Sicherheitsbedrohungen bist du der erste Schutzwall. Y gibt dir Tipps, wie du mithelfen kannst, die Truppe noch sicherer zu machen:

- Melde Auffälligkeiten und unbekannte Menschen in der Dienststelle.
- Nutze keine private Soft- oder Hardware am Arbeitsplatz.
- Achte in der Öffentlichkeit darauf, mit wem du sprichst.

Mehr zu diesen Tipps und noch mehr findest du hier.

Seite 58–61

Kapitel 3 – Abwehr ▶

**Gefahr durch Spionage**

Der Militärische Abschirmdienst (MAD) ist von zentraler Bedeutung für die Sicherheit der Bundeswehr – und ganz Deutschlands. Mitarbeitende des Geheimdienstes berichten über ...

- einen Soldaten, der sich von einem russischen Luftwaffenattaché anwerben ließ,
- einen anderen Soldaten, der Russland von sich aus Informationen aus der Truppe angeboten hat,
- ihre Arbeitsweise bei der Spionageabwehr, um solchen Fällen auf die Spur zu kommen.

Seite 63–71



„EINE PERSON, DIE MIT EINER SICHERHEITS-EMPFINDLICHEN TÄTIGKEIT BETRAUT WERDEN SOLL (...), IST VORHER EINER SICHERHEITSÜBERPRÜFUNG ZU UNTERZIEHEN.“

(Paragraf 2, Sicherheitsüberprüfungsgesetz)

Sicheres Umfeld

Die Sicherheitsüberprüfung sorgt dafür, dass alle Angehörigen der Bundeswehr in einem vertrauensvollen Miteinander arbeiten können. Y erklärt, was du alles dazu wissen musst.

- Wer und was wird überprüft?
- Welche Bedeutung haben dabei die Risikostufen?
- Welche Stufen der Geheimhaltung gibt es?

Antworten auf diese und weitere Fragen findest du hier.

Seite 72–75

Outro ▶



Vorsprung durch Wissen

Die Arbeit des Militärischen Nachrichtensystems (MilNW) schützt die eigene Truppe.

- Das MilNW dokumentiert alle sicherheitsrelevanten Informationen von den Einsatzgebieten bis zu den Kasernen in Deutschland.
- Dabei greift es auf Quellen zurück wie Medienberichte, Aufklärungsergebnisse durch Satelliten- oder Luftbildaufnahmen und abgefangene elektronische Kommunikation.

Mehr über das MilNW und wie auch unsere Partner von seiner Arbeit profitieren, erfährst du hier.

Seite 76–83

Rückblick

Wie sich Angehörige der Bundeswehr vor Bespitzelung schützen können, war und ist Gegenstand zahlreicher Kampagnen, Plakate und Broschüren. Eine kleine Zeitreise von den 1950er-Jahren bis heute:

- Die Sicherheitsfibel sensibilisierte die Soldaten während des Kalten Krieges für Spionage.
- Die „10 Grundregeln für die Militärische Sicherheit“ waren lange Zeit die zentrale Dienstvorschrift. Einige Formulierungen erscheinen heute aus der Zeit gefallen.
- Mit dem Aufkommen von E-Mail und Smartphone in den 2000er-Jahren wurden Schulungen gegen Phishing wichtig.

Seite 84–89



Dranbleiben

Sicherheit in der Bundeswehr ist ein weites Feld. Wer sich für noch mehr Inhalte interessiert, als in dieser Ausgabe Platz fanden, bekommt hier spannende Empfehlungen:

- zu Artikeln auf bundeswehr.de und Ynside,
- zu Videos auf dem Youtube-Kanal der Bundeswehr
- und zu Museen und Büchern, die sich mit dem Thema beschäftigen.

Unsere Auswahl an weiterführenden Beiträgen findest du auf diesen Seiten.

Seite 90–94

S. 16: Bundeswehr/Sheriff Kästner (E.S.o.), IMAGO/SNA (E.S.m.); Picture-Alliance/Associated Press/Satellite Image © 2022 Maxar Technologies (E.S.u.); BAMAD (Z.S.o.u.); Bundeswehr/PIZ C/R/Andreas Wiemer (Z.S.m.); Erik Sharar (D.S.e.); Deutsches Spionagemuseum Berlin (D.S.z.); Bundeswehr/Sebastian Wilke (D.S.d.); BND/photothek/Thomas Trutschel (D.S.v.)

Hilf uns, sie zu schützen!



Militärischer
Abschirmdienst

#mad
#infos
#sicherheit





S. 18: Y/C3 Visual Lab, Kollage
S. 19: Bundeswehr/Jörg Hüttenhölcher

Verantwortungsbewusst
Stabsfeldwebel Heinrich Erkner
war bereits 2023 in Litauen –
damals bei der eFP-Battlegroup.
Seit September 2024 ist er Teil
der Brigade Litauen.

BRENNPUNKTE

TEXT Beate Schöne
FOTO Jörg Hüttenhölcher

Im Fokus des Gegners

**Wo gegnerische Staaten direkt aneinandergrenzen,
ist die Spionagetätigkeit besonders hoch.**

Y hat einen Stabsfeldwebel der Brigade Litauen einen Tag
lang begleitet. Wie schützt sich der Soldat vor Ausspähung
durch Russland, das nur wenige Kilometer entfernt liegt?



Gesichertes Gebäude

Heinrich Erkners Truppenausweis allein reicht nicht. Der Zugang zu den Büros der derzeit 150 deutschen Soldatinnen und Soldaten ist speziell gesichert.



BRENNPUNKTE

Hauptstadt Vilnius

Die bevölkerungsreichste Stadt Litauens ist für seine Barockarchitektur bekannt. Eines der bekanntesten historischen Gebäude ist die Kirche der heiligen Katharina.

Grenzgebiet

Die russisch-litauische Grenze ist zwar relativ kurz und besteht ausschließlich über die Exklave Kaliningrad, im Südosten teilt Litauen jedoch auch eine rund 680 Kilometer lange Grenze mit Russlands Verbündetem Belarus.

Es ist ein eiskalter Morgen. Minusgrade in der Nacht haben einen Frostfilm auf den Fahrzeugen hinterlassen. Für Heinrich Erkner* beginnt der Arbeitstag mit Scheibenfreikratzen. Einige Minuten später fährt er mit seinem Auto aus der Stadt und durch einen großen Wald. Sein Ziel: der Standort des Aufstellungs-

stabs der Brigade Litauen. Der Stabsfeldwebel ist seit Anfang September 2024 als Informationsfeldwebel Teil des Stabs. Neben der Begleitung von Pressevertreterinnen und -vertretern und Koordinierungsaufgaben hält er vor allem seinem Presseoffizier den Rücken frei. Erkner war schon von August bis Dezember 2023 bei der damaligen eFP-Battlegroup in Rukla eingesetzt, also kurz nachdem Verteidigungsminister Boris Pistorius die dauerhafte Stationierung einer Brigade in Litauen angekündigt hatte.

Für Erkner war schnell klar, dass ein Dienstposten in der Brigade eine große Chance bietet. „Nicht nur, um hier Pionierarbeit zu leisten, sondern auch für uns als Familie sind diese Erfahrungen unbezahlbar“, sagt der 52-Jährige. Ein knappes Jahr später zog Erkner mit seiner Frau Steffi und den beiden Töchtern Charly (12) und Lilie-Marleen (11) nach Bukčiai, einen Vorort von Vilnius.

*Alle Namen zum Schutz der Soldaten und ihrer Angehörigen geändert.

„Litauen steht durch seine direkte Grenze zu Russland und Belarus besonders im Fokus.“ Heinrich Erkner, Informationsfeldwebel

Im Autoradio laufen die Nachrichten: „Ein Frachtflugzeug, das im Auftrag von DHL in Leipzig gestartet war, ist beim Anflug auf Vilnius über einem Wohngebiet abgestürzt. Mindestens ein Mensch kam ums Leben.“ Die Ursache für den Flugzeugabsturz ist zu diesem Zeitpunkt noch unklar. Da es bereits im Juni zu Paketbränden in DHL-Luftfrachtzentren, unter anderem in Leipzig, kam, kommt Erkner unweigerlich kurz der Gedanke, dass es sich vielleicht um einen Sabotageakt handeln könnte. Spätere Auswertungen des Flugschreibers konnten dies ausschließen. „Natürlich haben wir uns im Vorfeld auch Gedanken über mögliche Bedrohungen gemacht“, sagt er. „Litauen steht durch seine direkte Grenze zu Russland und Belarus besonders im Fokus.“ Regelmäßig erfährt er aus den Medien von Sabotage- und Spionagevorfällen in Litauen. Im September 2024 wurde ein litauischer Anwalt zu neun Jahren Haft wegen Spionage verurteilt. Anfang November kam es zur Festnahme von Verdächtigen, die ➤



Verantwortlich für die Sicherheit

Neben dem militärischen Nachrichtenwesen und der Beratung des Kommandeurs berät Major Christian Friedmann (l.) mit der G2-Abteilung die Soldatinnen und Soldaten im Umgang mit Smartphones und Social Media.

im Zusammenhang mit den Paketbrand-sätzen stehen sollen. Angst hat der Stabsfeldwebel aus Niedersachsen aber nicht: „Natürlich kann jederzeit etwas passieren, aber das kann es theoretisch auch in Deutschland – und wir werden hier sehr gut vorbereitet.“ Erkner und seine Kameradinnen und Kameraden haben Einweisungen und Tipps für ihre Sicherheit bekommen. Litauen ist ein hoch digitalisiertes Land. Neben dem dienstlichen Umgang mit vertraulichen Informationen werden sie deshalb auch darin geschult, wie sie sich privat schützen können. Dazu gehört auch der bewusste Umgang mit dem Smartphone.

Sicherheit durch Selbstreflexion

Erkner fährt vorbei an Wohnhäusern. Immer wieder sieht man wehende litauische und ukrainische Flaggen. Über eine Brücke kreuzt er die Neris, den zweitgrößten Fluss Litauens. Kurz dahinter ist derzeit der Aufstellungsstab der Bundeswehr stationiert. Überall sind Schranken und Schleusen, die nur mit Zugangskarte geöffnet werden können – selbst für den Fahrstuhl braucht man eine Karte. In der siebten Etage sitzen zwei bewaffnete litauische Soldaten. Sie kontrollieren, wer Zugang zu den Kameradinnen und Kameraden aus Deutschland erhält.

Für die Sicherheit der Bundeswehrkräfte ist Major Christian Friedmann aus der G2-Abteilung zuständig. „Wir kümmern uns um alles, was die Sicherheit der Truppe betrifft“, erklärt Friedmann, Dezernatsleiter Nachrichtenlage. Alle Truppenteile sollen ihren Auftrag trotz der möglichen Bedrohung durch Spionage, Sabotage, Subversion, Terrorismus oder organisierte Kriminalität erfüllen können. „Um die Soldatinnen und Soldaten zu sensibilisieren, bitten wir sie als Allererstes, eine persönliche Risikoanalyse zu machen“, so der 38-Jährige. Die Analyse beinhaltet Fragen wie: Wie schütze ich mich und mein Umfeld? Wer braucht



Vielfältiger Aufgabenbereich

Als Informationsfeldwebel koordiniert Erkner nicht nur Pressebesuche und sucht Gesprächspartner für Journalistinnen und Journalisten, sondern schreibt manchmal auch selbst Artikel.

Sichere Kommunikation

Es gibt drei verschiedene Verschlüsselungsmethoden, um Daten vor Spionage zu schützen. Die sicherste ist, den Schlüssel im Vorfeld auszutauschen – beispielsweise durch gegenseitiges Abfotografieren eines QR-Codes.

besonderen Schutz? „Wir wollen, dass sich jeder ehrlich einschätzt, wie gefährdet er ist und welche Informationen er hat, die für andere von Interesse sein könnten“, sagt Friedmann. Für ausländische Nachrichtendienste sind zum Beispiel Verschlusssachen, die Einblicke in den Aufstellungsstab liefern, besonders interessant.

„Außerdem sollte man reflektieren, welche Angriffsfläche man bietet, also welches mögliche Kompromat“, so der Major. Der Begriff stammt vom früheren sowjetischen Geheimdienst KGB. Schulden, eine Affäre, Unzufriedenheit im Job – was ist geeignet, um eine Person zu erpressen, ein Amtsgeheimnis preiszugeben oder die eigenen Kräfte zu sabotieren? Hier setzen die Sicherheitsvorschriften und Sensibilisierungstipps der G2-Abteilung an. „Natürlich sind das Aspekte, die auch in Deutsch-

land beachtet werden sollten, denn auch da kam es bereits zu Vorfällen“, so Friedmann. „In Litauen zeigt sich, was im Inland gepredigt wird.“

Gefahrenquelle Smartphone

Stabsfeldwebel Erkner hat einen Termin mit Major Friedmann. Er geht den Gang entlang, vorbei an Bürotüren und einer Druckerstation. Im Besprechungsraum wartet Friedmann bereits auf ihn. Erkner hat sich ein neues Smartphone gekauft und braucht nun Unterstützung bei der Verschlüsselung. Das ist wichtig, denn vieles läuft in Litauen nur noch übers Smartphone – sei es beim Bezahlen im Geschäft, beim Parken per App oder beim Mieten eines Fahrrads. Auch als Übersetzungshilfe ist das Smartphone Gold wert, zum Beispiel für die Kommunikation mit dem Vermieter ➤



Per Smartphone bezahlen

Bei der Mittagspause im Schnellrestaurant bezahlt Erkner auf digitalem Weg. Innerhalb weniger Minuten wird das bestellte Essen auf einem Transportband geliefert.

oder diversen Dienstleistern. So hilfreich das Smartphone ist, es ist auch immer ein Einfallstor für Spionage. „Heutzutage sind fast alle Menschen gläsern“, erklärt Friedmann. „Mit einigen wenigen Tricks kann man seinen Schutz aber maßgeblich erhöhen.“

Einer der Tricks: ein neues Handy mit litauischer SIM-Karte kaufen. Jedes Smartphone hat eine International Mobile Station Equipment Identity (IMEI), das ist eine eindeutig zuordenbare 15-stellige Seriennummer. Wenn diese bereits in Deutschland im Mobilfunknetz aufgetaucht ist und dann in Litauen, wird man schnell als Deutscher identifiziert. Sollte diese Nummer zusätz-

lich auf dem Truppenübungsplatz Pabradė oder Gaižiūnai getrackt werden, ist es klar, dass es sich um einen deutschen Soldaten handeln muss, und man kann in den Fokus eines Spions rücken. Mit einer litauischen SIM-Karte und bestenfalls einem günstigen neuen Telefon, dem sogenannten Burner Phone, schützt man sich davor. „Wir beraten die Soldatinnen und Soldaten, was sie tun können. Die Entscheidung, was sie davon umsetzen, liegt im privaten Bereich bei ihnen selbst“, so Friedmann. Zusätzlich ist es wichtig, ein virtuelles privates Netzwerk (VPN) zu nutzen, um seine Daten zu schützen. „Bei einer unverschlüsselten

Kommunikation kann jeder, der zwischen Absender und Empfänger in einem Funkmast ist, leicht mithören“, sagt der Major.

Eine Methode, um Daten zu schützen: einen Schlüssel mit Beginn der Kommunikation austauschen. Hierbei hat nur derjenige die Möglichkeit, auf die Informationen zuzugreifen, der auch im Besitz des passenden Schlüssels ist. Dieser kann zwar unter Umständen auch abgegriffen werden, aber nur einmal – ganz am Anfang beim Austausch. Das reduziert das Risiko eines Mithörers oder Mitlesers bereits erheblich. Bei einer weiteren Verschlüsselungsmethode wird der Schlüssel im Vorfeld ausgetauscht.

S. 24–25: Bundeswehr/Jörg Hüttenhölischer (3)

BRENNPUNKTE

„Das Restaurant ist öffentlich zugänglich. Man sollte sich bewusst sein, dass jemand zuhören könnte. Es ist wichtig, sich genau zu überlegen, worüber man spricht.“

Heinrich Erkner, Informationsfeldwebel

Eine Messenger-App, bei der dies möglich ist, ist beispielsweise Threema. Erkner ist genau hierfür heute bei Major Friedmann. Er zückt sein Smartphone und fotografiert einen vorher generierten QR-Code von Friedmanns Display ab. „Danach fotografiere ich noch seinen Code und dann haben wir ausgetauschte Schlüssel“, erläutert Friedmann. „Das nutzen wir alle in der Abteilung G2 für die private Kommunikation über Chats – das ist der sicherste Weg.“ Wichtig sei aber auch, die dienstliche Kommunikation von der privaten zu trennen.



Nur scheinbar unter sich

Erkner und sein Team sprechen beim Mittagessen nie über Dienstliches. Das wäre ein unnötiges Risiko.

Hört jemand mit?

Mittlerweile ist es mittags. Auf den Gängen im Aufstellungsstab herrscht reges Treiben. Viele der rund 150 deutschen Soldatinnen und Soldaten sind auf dem Weg zum Mittagessen. Erkner und seine Presseabteilung gehen in das Schnellrestaurant im Erdgeschoss. Auch hier ist alles digital: An fünf Terminals wird per Touchpad das Essen bestellt. Erkner wählt einen Salat, Sparerips mit Pommes und eine Cola. Die Preise für eine Mahlzeit belaufen sich auf knapp unter zehn Euro. Beahlt wird direkt am Terminal – mit dem Smartphone. „Bevor ich in Litauen war, habe ich nie mit dem Smartphone bezahlt“, sagt Erkner. „Aber es ist einfach und schnell.“

Der Stabsfeldwebel achtet darauf, dass die Bezahlungsfunktion NFC nur aktiv ist, wenn er sie braucht. „Wenn ich mit dem Smartphone bezahle, schalte ich die Funktion ein und danach direkt wieder aus.“ Die Umstellung aufs mobile Bezahlen ist in Litauen zwingend: Nicht nur in Restaurants und Bars, auch in vielen Geschäften sowie beim Busfahren gibt es gar nicht mehr die Möglichkeit, in bar zu zahlen. Das Schnellrestaurant ist im Übrigen ein öffentlicher Ort. Man weiß nie, wer am Nebentisch sitzt. Deshalb gilt für Erkner und sein Team: Über dienstliche Themen zu reden, ist ein unnötiges Risiko. „Alles, was unsere Arbeit betrifft und sogar eingestuft sein könnte, hat nichts in der Öffentlichkeit zu suchen“,



Persönliche Leidenschaft

Um bei Bedarf auch fotografisch unterstützen zu können, hat sich Erkner selbst und mithilfe von Kameraden den Umgang mit der Kamera beigebracht.



Busfahren mit Smartphone

Die Busse in Litauen schauen zwar recht altertümlich aus, im Inneren sind sie jedoch modern. Das Ticket kann nur per Smartphone oder Karte bezahlt werden.

sagt der Stabsfeldwebel. Auch Debatten und Meinungsverschiedenheiten gehören hier nicht hin: „Nach außen sollten wir uns immer als eine Einheit präsentieren.“

Nach dem Essen geht es in die Stadt. Erkner soll für einen Onlineartikel seiner Abteilung Sehenswürdigkeiten von Vilnius fotografieren. Auf dem Weg zum Kathedralenplatz fallen die vielen Sicherheitskameras in der Stadt auf. Am Anfang sei es etwas befremdlich gewesen, überall gefilmt zu werden. Mittlerweile interessiere es ihn nicht mehr. „Das ist ähnlich wie bei meiner Verwendung in Sizilien. Da haben wir in der Nähe des Vulkans Ätna gewohnt. Anfangs waren wir noch ängstlich, wenn die Erde bebte und der Vulkan ausbrach. Irgendwann war es nichts Besonderes mehr. Man gewöhnt sich an alles“, erzählt Erkner. Am Ende ist es auch eine Frage der Perspektive: Die vielen Kameras in der Innenstadt sind ein Eingriff in die Privatsphäre, aber sie bieten auch einen gewissen Schutz.

Als Soldat fällt Erkner in der Stadt auf und wird auch ab und zu freundlich angesprochen. Er fühlt sich in Litauen sehr willkommen. „Als Informationsarbeiter weiß ich natürlich, was ich über meine Arbeit sagen darf und was nicht.“ Informationen, die von der Bundeswehr selbst aktiv an die Medien gegeben werden, kann man jederzeit preisgeben. Diese Informationen sind öffentlich, zum Beispiel die künftige Größe der Brigade Litauen mit rund 5.000 Soldatinnen und Soldaten. Oder wie viele deutsche Kräfte bereits vor Ort sind. „Informationen, die tiefer in die Materie gehen, Interna, Namen oder Dienstgrade, lasse ich komplett weg“, so Erkner.

Verschwiegenheit auch im Privaten

Nach knapp einer Stunde sind alle Fotos im Kasten und es geht zurück ins Büro zur Nachbereitung. Um 15 Uhr hat Erkner heute Dienstschluss. Mit seinem Auto fährt er zur AISV, die American International School of Vilnius. Hier gehen seine beiden Töchter zur Schule, die Erkner heute abholt. Die Einrichtung ist sehr modern: Die Schülerinnen und Schüler nutzen Tablets, und für die Eltern läuft alles über eine App – von der Kommunikation mit der Schulleitung bis zur Krankmeldung der Kinder. Da ist Deutschland noch weit hinterher. Auch bei der Schulwahl der Kinder war das Thema Sicherheit für Erkner und seine Frau wichtig. In die AISV gehen auch einige Diplomatinkinder und Kinder deutscher Partnernationen. Für deren Sicherheit sorgen neben Schranken, Kameras und einer Wache am Eingang auch ein Sicherheitsdienst.

Am Abend sitzen Erkner und seine Familie oft zusammen und sprechen über den Tag. „Wir sehen es als Privileg und Chance, andere Länder kennenzulernen“, sagt Ehefrau Steffi. „Die Kinder haben dadurch die Möglichkeit, weltoffen aufzuwachsen und ihre Sprachfähigkeiten zu verbessern.“ Für den Stabsfeldwebel gilt auch zu Hause, dass man nicht alles erzählen muss, was auf der Arbeit passiert. „Abgesehen davon, dass eingestufte Informationen zu Hause sowie so nichts zu suchen haben, dient es auch dem Schutz meiner Familie, dass ich nicht zu viel erzähle“, so der Stabsfeldwebel.

Erkner schwärmt von Litauen: Kein Bundeswehrangehöriger müsse Angst haben, hierher zu kommen. Einiges laufe hier sogar besser, und die Menschen seien oft entspannter. Für die eigene Sicherheit und die der Bundeswehr sei es natürlich wichtig, sensibilisiert zu sein und achtsam mit Informationen umzugehen. Aber das sollten alle Bundeswehrangehörigen auch in Deutschland. ●



Die Familie ist mit dabei Für Erkner ist es bereits die zweite integrierte Verwendung. Nach vier Jahren Sizilien wird er die nächsten Jahre in Litauen verbringen – auch diesmal wieder gemeinsam mit Frau und Kindern.

S. 26: Bundeswehr/Jörg Hüttenhölischer (3)

SICHERHEITSKAMPAGNE

BMVg



SEI KEINE BEUTE!



Du bist die erste Verteidigungslinie, wenn es um Sicherheit geht. Achte darauf, wie Du Online und im Chat mit Deinen persönlichen und dienstlichen Daten umgehst und schütze damit unsere Bundeswehr!



bpaq.de/krake



BUNDESWEHR

Kasernen-sicherheit

Nicht nur im Auslandseinsatz oder im Feld muss der Eigenschutz sichergestellt werden. Auch am Heimatstandort gilt es, mögliche Bedrohungen abzuwehren. Hierauf muss sich jede Liegenschaft vorbereiten.

Unter Kontrolle

Drohnenüberflüge, Löcher in Zäunen:
Die Liegenschaften der Bundeswehr sind zunehmend Ziel
von Ausspähungs- und Sabotageversuchen.
Y erklärt, wie die Truppe ihre Liegenschaften schützt.

TEXT Ole Henckel

A

Alarm! Gefährdungsstufe Bravo! Ob Spione, Saboteure oder Terroristen die Kaserne der Bundeswehr im Fadenkreuz haben, ist noch unklar. Trotzdem muss jetzt alles schnell gehen. Für den verantwortlichen Kasernenkommandanten läuft die Zeit. Er muss schnellstmöglich alle Maßnahmen zur Absicherung treffen.

Solch eine Situation kommt alle paar Wochen an einem Standort der Bundeswehr in Deutschland vor – auch wenn gar keine Gefahr droht. Der Grund: die Übungsserie „Starke Sicherung“ des Höheren Offiziers Militärische Sicherheit der Bundeswehr (HöhOffzMilSich Bw). Für den betroffenen Kasernenkommandanten bedeutet das zwei Tage voller Anspannung – wenn alles gut läuft. Ansonsten heißt es: Absicherungskonzept und Durchführungsbefehle überarbeiten. „Die entsprechende Liegenschaft erhält einen echten Alarmbefehl über das Alarmierungssystem der Bundeswehr“, erklärt Hauptmann Kai Heuer*,

*Name zum Schutz des Soldaten geändert.

Gefahrenstelle

Wer darf rein und wer nicht? Die Zufahrt zu einer Liegenschaft ist besonders gefährdet und muss entsprechend abgesichert werden. Stacheldraht, Fahrzeugsperren und bewaffnete Kräfte sorgen für zusätzlichen Schutz.



Wachaufgaben

Bei erhöhter Gefährdung übernehmen zunehmend Soldatinnen und Soldaten die Wachaufgaben der zivilen Wache. Eine starke Bestreifung der Liegenschaft ist eine wichtige Maßnahme.



Stehen bleiben

Greift die Streife unbefugte Personen auf, werden diese festgesetzt, durchsucht und später der Polizei übergeben.



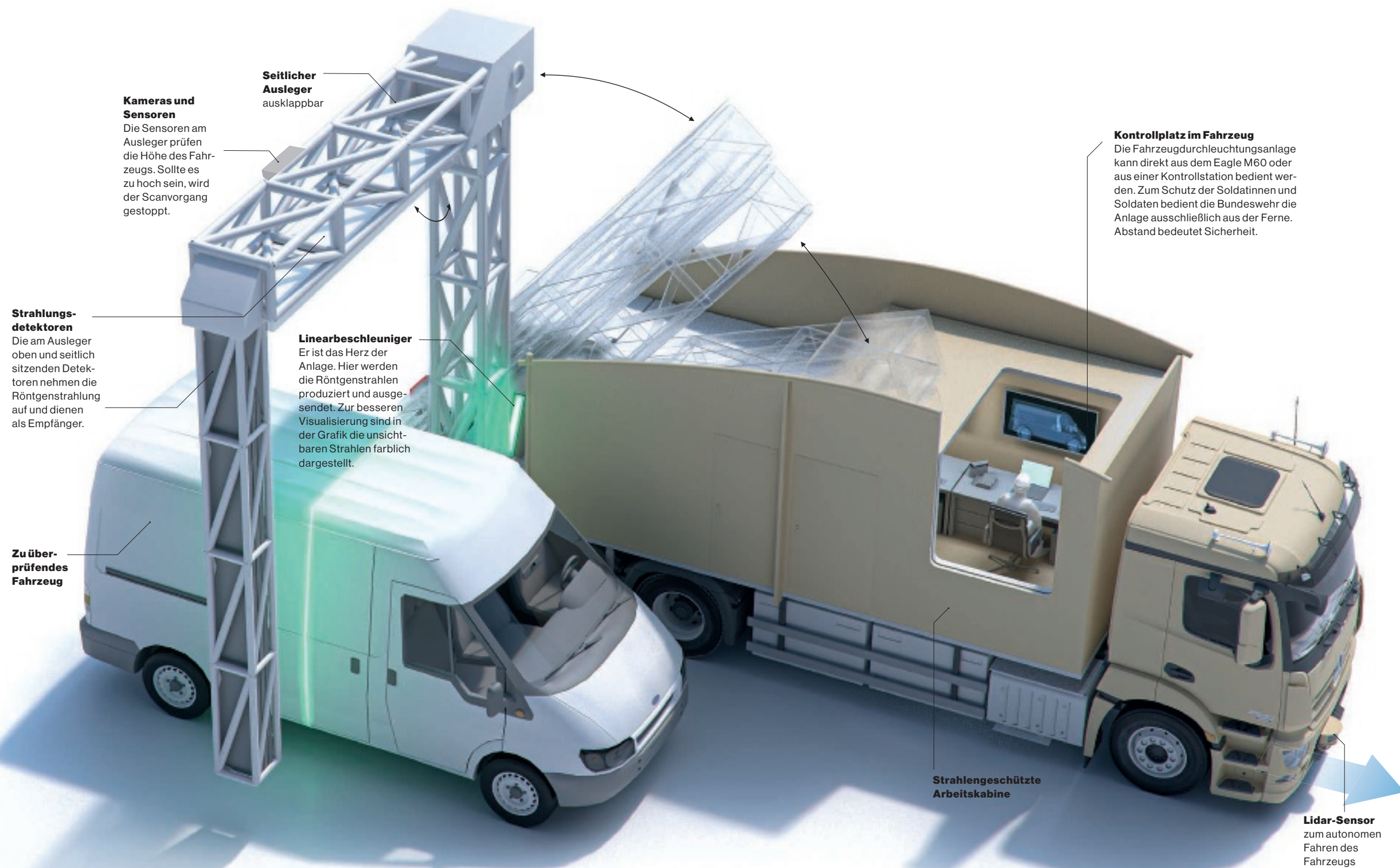
Fahrzeugkontrolle

Nicht nur der Laderaum, sondern auch Unterboden, Fahrerkabine und Motorraum müssen bei unbekannten Fahrzeugen kontrolliert werden.

Mitarbeiter im Referat des HöhOffzMilSich Bw. „Der ist zwar mit einem Hinweis auf die Übung ‚Starke Sicherung‘ versehen, was aber nichts daran ändert, dass alle Maßnahmen wie im Ernstfall ausgeführt werden müssen.“

Der Kasernenkommandant ist dafür verantwortlich, die im Absicherungskonzept enthaltenen Maßnahmen zur Erhöhung der Gefährdungsstufen umzusetzen. Das Konzept selbst ist allerdings so formuliert,

dass es im Fall der Fälle jeder Soldat und jede Soldatin umsetzen könnte. Die Maßnahmen wurden für jede Liegenschaft individuell erarbeitet und dienen dem Schutz von Personal sowie sicherheitsempfindlichen Punkten und Anlagen. Das können zum Beispiel eine Operationszentrale, ein technischer Bereich mit eingestufte Fernmeldetechnik, eine Waffenkammer oder eine Verschlusssachen (VS)-Registratur sein. ➤



Fahrzeugdurchleuchtungsanlage

Nichts bleibt unentdeckt für die Fahrzeugdurchleuchtungsanlage mit dem Lkw Eagle M60. Ursprünglich beschafft zur Absicherung von Feldlagern im Auslandseinsatz, kann die mobile Röntgenanlage auch im Inland zur zusätzlichen Absicherung besonders gefährdeter Liegenschaften eingesetzt werden. Insgesamt wurden drei Systeme beschafft.

Kameras und Sensoren

Die Sensoren am Ausleger prüfen die Höhe des Fahrzeugs. Sollte es zu hoch sein, wird der Scanvorgang gestoppt.

Seitlicher Ausleger ausklappbar

Strahlungsdetektoren

Die am Ausleger oben und seitlich sitzenden Detektoren nehmen die Röntgenstrahlung auf und dienen als Empfänger.

Zu überprüfendes Fahrzeug

Linearbeschleuniger

Er ist das Herz der Anlage. Hier werden die Röntgenstrahlen produziert und ausgesendet. Zur besseren Visualisierung sind in der Grafik die unsichtbaren Strahlen farblich dargestellt.

Kontrollplatz im Fahrzeug

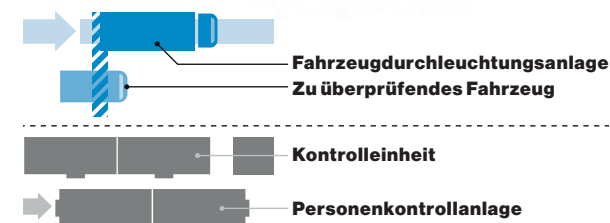
Die Fahrzeugdurchleuchtungsanlage kann direkt aus dem Eagle M60 oder aus einer Kontrollstation bedient werden. Zum Schutz der Soldatinnen und Soldaten bedient die Bundeswehr die Anlage ausschließlich aus der Ferne. Abstand bedeutet Sicherheit.

Strahlengeschützte Arbeitskabine

Lidar-Sensor zum autonomen Fahren des Fahrzeugs

Objektzugangskontrolle

Die Fahrzeugkontrollanlage wird durch die Kontrolleinheit und die Personenkontrollanlage ergänzt.



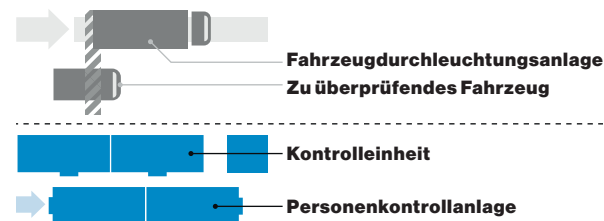
Die Wachkategorien von A bis D

Doch wer entscheidet, welche Liegenschaft in welche Bewachungskategorie eingestuft wird? „Dafür ist die Kommission Bewachung und Absicherung, kurz KomBA, verantwortlich“, berichtet Hauptmann Heuer. „Diese besteht aus einem Vertreter der vorgesetzten Kommandobehörde des jeweiligen Kasernenkommandanten, des BAMAD, des Kompetenzzentrums Baumanagement und des Bundesamts für Infrastruktur, Umweltschutz und Dienstleistungen sowie den Leitern der KomBA.“ Entsprechend der Einschätzung der KomBA werden die Liegenschaften dann in die Bewachungskategorie A bis D einsortiert, wobei A die höchsten Absicherungsmaßnahmen erfordert und D die niedrigsten.

Die Bundeswehr kombiniert die Maßnahmen zur Absicherung von Liegenschaften in vier großen Bereichen. Hauptmann Heuer erklärt: „Als Erstes sind das bauliche Maßnahmen wie Zäune, besondere Härtung von Räumen oder Gebäuden sowie Tore und Sicherheitstüren. Zweitens sind das technische Maßnahmen wie Einbruchmeldeanlagen, Zutrittskontrollanlagen, Videoüberwachung sowie Erschütterungs- und Bewegungssensoren. Zu Drittens zählt die personelle Absicherung, also Sicherheitsüberprüfungen des eigenen Personals, das Wachpersonal, Diensthunde oder die Vorhaltung von Eingreifreserven. Und Viertens gibt es noch die organisatorische Absicherung, also beispielsweise die Einrichtung von militärischen Sicherheitsbereichen, Film- und Fotografierverboten, Zutrittsbeschränkungen oder Sperrzonen.“

Objektzugangskontrolle

In Kombination der drei Einzelanlagen ist eine umfassende Zugangskontrolle aus sicherer Entfernung möglich.

**Bedrohung bestimmt Gefährdungsstufe**

Nicht zu verwechseln sind die Bewachungskategorien mit den Gefährdungsstufen. Hier steht entgegengesetzt Alpha für die niedrigste und Delta für die höchste Stufe. Die Grundlagen für eine Heraufsetzung der Gefährdungsstufe liefert das Militärische Nachrichtenwesen. Anhand seiner Quellen erstellt es fortlaufend eine Bedrohungslage für die Bundeswehr. Gefährdungsstufe Bravo bedeutet, dass es konkretere Erkenntnisse über eine Gefahr gibt, diese aber räumlich und zeitlich noch nicht genau zugeordnet werden kann. Als Reaktion muss der Kasernenkommandant beispielsweise die zivile Wache durch Soldatinnen und Soldaten ergänzen. Auch kann in Absprache mit den zivilen Sicherheitsbehörden der Militärische Sicherheitsbereich um die Kaserne ausgeweitet und beispielsweise die Zufahrtskontrolle zum Haupttor 200 Meter vorverlegt werden. Material zur Absicherung ist dabei ständig vorzuhalten, zum Beispiel Spanische Reiter, Stacheldraht oder Durchbruchhindernisse.

Während der Übung bleibt es aber nicht bei der Gefährdungsstufe Bravo. Die Erhöhung auf Charlie folgt sehr bald. „Das bedeutet, dass die Gefahr nun räumlich und zeitlich eingegrenzt werden kann“, erklärt Hauptmann Heuer. „Die höchste Gefährdungsstufe Delta, also die konkrete und unmittelbare Bedrohung, wird nur theoretisch durchgespielt. Durch starke personelle Bindungen bis hin zu Gebäuderäumungen würde eine reale Durchführung den Dienstalltag zu sehr beeinflussen.“

Während einer Übung nimmt das Team des Referats HöHOffzMilSich Bw die Maßnahmen vor Ort in Augenschein und lässt sich auch an der Zufahrt zur Liegenschaft kontrollieren. Bei vielen Liegenschaften sei er beeindruckt davon, wie die Verantwortlichen die Maßnahmen umsetzen, sagt Heuer. „Es gibt keine Übung, auf die wir fahren und auf der wir nicht selbst noch etwas dazulernen. Jede

Liegenschaft ist anders und die gewählten Maßnahmen müssen immer an die Gegebenheiten vor Ort angepasst werden.“ Dass jede Liegenschaft den Test bestehe, sei aber nicht der Fall, betont Heuer. Insgesamt sieht er die Bewachung und den Schutz der Liegenschaften der Bundeswehr auf einem soliden Niveau – auch im Vergleich zu den internationalen Partnern. ●

Kontrolleinheit

Sie ermöglicht die Steuerung der Fahrzeugdurchleuchtungsanlage und der Personenkontrollanlage aus sicherer Entfernung.

Arbeitsplätze

In diesem Bereich der Kontrolleinheit befinden sich die Arbeitsplätze zur Bedienung der Personenkontrollanlage. Am ersten Platz sitzt der Sprachmittler. Am zweiten Platz werden Sektor 1 und 2 und auf dem letzten Platz Sektor 3 überwacht.

Kameras und Scheinwerfer**Zu überprüfende Person****Sektor 1**

Vereinzelungsschleuse zur Identitätserfassung (Scanner ID-Karte, Handvenenscanner)

Sektor 2

Dokumentenscanner, Gepäck-Röntgenanlage, Metalldetektor, Waage

Sektor 3

Millimeterwellenscanner, Gepäckentgegennahme, Ausgang

Metalldetektor und Waage**Millimeterwellenscanner****Kameras und Gegensprechanlage****Kameras und Scheinwerfer****Generator zur Stromerzeugung****Klimaanlage****Scanner für Dokumente****Röntgenanlage zur Gepäcküberprüfung****Wartungsklappe für Röntgenanlage****Zugangstüren zur Entnahme potenziell gefährlicher Gegenstände****Gepäckentnahme nach Freigabe****Personenkontrollanlage**

Die zu kontrollierenden Personen werden einzeln mithilfe von Anzeigen, Lautsprechern und Kameras durch die Kontrollsektoren geleitet. Die Anlage stellt sicher, dass ausschließlich berechnete Personen ohne verbotene Gegenstände und mit den korrekten Papieren Zugang zum Feldlager oder einer Liegenschaft erhalten.

Servercontainer
Unterbringung des Datenservers

Halt, stehen bleiben!

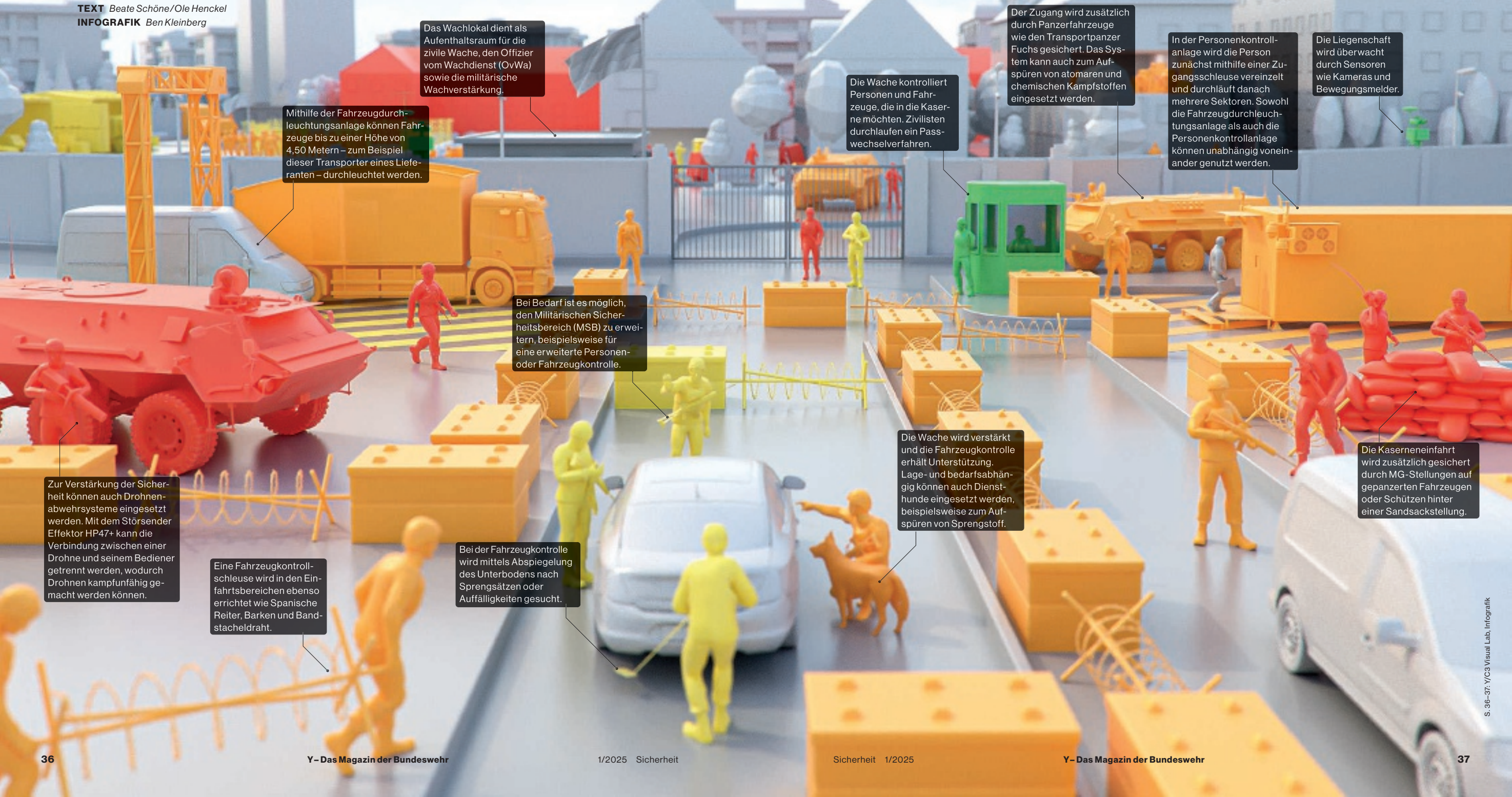
Der Eingangsbereich einer Kaserne oder Liegenschaft ist durch unbefugten Zutritt besonders gefährdet und wird daher speziell gesichert. Beim Schutz der Kasernen werden die Gefährdungsstufen Alpha bis Delta unterschieden. Y zeigt schematisch, welche Maßnahmen jeweils getroffen werden können.

TEXT Beate Schöne/Ole Henckel
INFOGRAFIK Ben Kleinberg

Gefährdungsstufen

Die einzelnen Stufen geben einen Mindeststandard erforderlicher Maßnahmen vor. Diese Vorgaben können liegenschaftsbezogen erweitert und lagebezogen angepasst werden. Man unterscheidet die Gefährdungsstufen:

- Alpha
- Bravo
- Charlie
- Delta



Das Wachlokal dient als Aufenthaltsraum für die zivile Wache, den Offizier vom Wachdienst (OvWa) sowie die militärische Wachverstärkung.

Mithilfe der Fahrzeugdurchleuchtungsanlage können Fahrzeuge bis zu einer Höhe von 4,50 Metern – zum Beispiel dieser Transporter eines Lieferanten – durchleuchtet werden.

Bei Bedarf ist es möglich, den Militärischen Sicherheitsbereich (MSB) zu erweitern, beispielsweise für eine erweiterte Personen- oder Fahrzeugkontrolle.

Die Wache kontrolliert Personen und Fahrzeuge, die in die Kaserne möchten. Zivilisten durchlaufen ein Passwechselverfahren.

Der Zugang wird zusätzlich durch Panzerfahrzeuge wie den Transportpanzer Fuchs gesichert. Das System kann auch zum Aufspüren von atomaren und chemischen Kampfstoffen eingesetzt werden.

In der Personenkontrollanlage wird die Person zunächst mithilfe einer Zugangsschleuse vereinzelt und durchläuft danach mehrere Sektoren. Sowohl die Fahrzeugdurchleuchtungsanlage als auch die Personenkontrollanlage können unabhängig voneinander genutzt werden.

Die Liegenschaft wird überwacht durch Sensoren wie Kameras und Bewegungsmelder.

Zur Verstärkung der Sicherheit können auch Drohnenabwehrsysteme eingesetzt werden. Mit dem Störsender Effektor HP47+ kann die Verbindung zwischen einer Drohne und seinem Bediener getrennt werden, wodurch Drohnen kampfunfähig gemacht werden können.

Eine Fahrzeugkontrollschleuse wird in den Einfahrtbereichen ebenso errichtet wie Spanische Reiter, Barken und Bandstacheldraht.

Bei der Fahrzeugkontrolle wird mittels Abspiegelung des Unterbodens nach Sprengsätzen oder Auffälligkeiten gesucht.

Die Wache wird verstärkt und die Fahrzeugkontrolle erhält Unterstützung. Lage- und bedarfsabhängig können auch Diensthunde eingesetzt werden, beispielsweise zum Aufspüren von Sprengstoff.

Die Kaserneneinfahrt wird zusätzlich gesichert durch MG-Stellungen auf gepanzerten Fahrzeugen oder Schützen hinter einer Sandsackstellung.

Sicherung in vier Phasen

Das Ausrufen einer Gefährdungsstufe

ist abhängig von einer potenziellen Gefährdung und kann sowohl räumlich als auch zeitlich begrenzt ausgerufen werden. Die Umsetzung der befohlenen Maßnahmen trägt zur Erhöhung der Militärischen Sicherheit bei, beispielsweise gegenüber terroristischen Bedrohungen und Sabotageversuchen.

Alpha

Ausrufung bei allgemeiner Gefährdungslage mit möglicher abstrakter Bedrohung

Die Absicherungsmaßnahmen werden in den Liegenschaften mit dem zur Verfügung stehenden Personal und Material eigenverantwortlich umgesetzt. Sie müssen dauerhaft durchhaltet sein. Ziel ist, die Bundeswehrangehörigen und das Wachpersonal zu sensibilisieren. Kraftfahrzeuge, Personen und Gebäude sind regelmäßig zu kontrollieren. Die ständige Bereitschaft zur Erhöhung der Gefährdungsstufen muss sichergestellt sein. Aufgrund der Erhöhung der militärischen Sicherheit gegen terroristische Bedrohung und Sabotage herrscht seit 2002 bundeswehrgesamt Gefährdungsstufe Alpha.

Bravo

Ausrufung bei Verschärfung der Bedrohungslage mit sich verdichtenden Erkenntnissen

Die Absicherungsmaßnahmen werden in den Liegenschaften eigenverantwortlich umgesetzt. Sie müssen längerfristig durchhaltet sein, ohne den Grundbetrieb zu beeinträchtigen. Dafür können gegebenenfalls Personal und Material aus anderen Liegenschaften hinzugezogen werden. Ziel ist, mittels der erhöhten Sicherheitsmaßnahmen mögliche Anschläge zu erschweren und abzuschrecken. Dies kann durch die Ausweitung des militärischen Sicherheitsbereiches, Wachverstärkung sowie erhöhte Kontrollmaßnahmen erfolgen.

Charlie

Ausrufung bei Auftreten eines Zwischenfalls oder erkennbar bevorstehender Bedrohung

Die Absicherungsmaßnahmen werden in der Regel regional begrenzt in den Liegenschaften umgesetzt. Ohne zusätzliche Wachverstärkung werden sie voraussichtlich nicht durchhaltet sein. Einschränkungen im Grundbetrieb werden in Kauf genommen. Ziel ist, die Bewachungs- und Absicherungsmaßnahmen weiter zu erhöhen, um einen Anschlag möglichst zu verhindern oder die Folgen zumindest zu minimieren. Um auf eventuelle Schadensereignisse reagieren zu können, werden Maßnahmen für eine weitere Erhöhung der Gefährdungsstufe vorbereitet.

Delta

Ausrufung bei unmittelbarer Bedrohungslage mit gesicherten Erkenntnissen

Die Absicherungs- und Objektschutzmaßnahmen werden örtlich begrenzt umgesetzt und führen zu erheblichen Einschränkungen im Grundbetrieb. Die Maßnahmen sind so vorzubereiten, dass eine grundsätzliche Durchhaltetätigkeit von mehreren Tagen sichergestellt ist, sofern eine Liegenschaft nicht vorübergehend geschlossen werden soll. Ziel ist, das Personal vor Ort auf das absolut notwendige Maß zu reduzieren. Das bedeutet, dass nur so viel Personal eingesetzt wird, wie für die Aufrechterhaltung und Wiederherstellung der militärischen Sicherheit erforderlich ist.

Der erweiterte Militärische Sicherheitsbereich (MSB) wird abgesichert, zudem werden öffentliche Straßen innerhalb des MSB gesperrt.

Bei Bravo wird die Zufahrt ausschließlich für den militärischen Zugangsverkehr genutzt. Ab Charlie wird dieses Tor geschlossen.

Für besonders schutzbedürftige Bereiche wie Technik und Munitionslager gilt erhöhte Aufmerksamkeit und verstärkte Absicherung.

Die Wache wird durch eigene Kräfte verstärkt. Gebäudezugänge werden verschlossen, Türen und Fenster regelmäßig überprüft.

Absicherung und Bewachung können noch weiter verstärkt werden, etwa durch Heimatschutzkräfte.

Die Liegenschaft wird durch verschiedene Sensoren wie Kameras und Bewegungsmelder überwacht.

Regelmäßig bestreifen der Offizier vom Wachdienst (OvWa) und sein Kraftfahrer den Kasernenzaun.

Ein zusätzlicher Bereich wird festgelegt, der etwa zur Fahrzeugabstellung oder als Dekontaminierungsplatz genutzt werden kann.

Zusätzliche und nicht notwendige Zugänge werden geschlossen, zum Beispiel Personendrehkreuze.

Ein Bereich zur Fahrzeugkontrolle wird gesondert eingerichtet.

Die Poststelle kann ein Anschlagziel sein und wird daher besonders geschützt. Die Schutzausrüstung (Schutzhelm, Handschuhe, FFP2-Maske) ist griffbereit zu halten. Ab Bravo wird ein gesonderter Bereich für die Bearbeitung der Post eingerichtet. Ab Charlie wird dieser auch bezogen. Bei Delta kann es zu einer vorübergehenden Schließung kommen.

Sicherheitsempfindliche Dokumente und Materialien wie Waffen und Munition, die nicht abgesichert werden können, werden zur alternativen Lagerung an einen anderen Ort abtransportiert.

Ein gemeinsames Lagezentrum, in dem alle Maßnahmen durch den Kasernenkommandanten koordiniert werden, wird eingerichtet.

Ein gepanzertes Fahrzeug mit MG-Schützen dient als Verstärkung und Aufstellung für möglicherweise durchbrechende Fahrzeuge.

Die Daten der Fahrzeugdurchleuchtungsanlage und der Personenkontrollanlage werden an die Kontrolleinheit übermittelt und dort ausgewertet. Von den fünf Arbeitsplätzen aus lässt sich die gesamte Kontrolle aus sicherer Entfernung durchführen.

Wach- und Sicherungspersonal zeigen verstärkte Präsenz. Soldatinnen und Soldaten, teilweise auch anderer Verbände, übernehmen Wachaufgaben. Die Streifenaktivität wird erhöht.

Alle nicht notwendigen Zugänge und Nebentore werden gesperrt.

Wenn möglich werden die direkt an die Liegenschaft angrenzenden öffentlichen Bereiche gesperrt. Grundlage dafür ist das Gesetz über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen (UZwGBW).

Abgestimmte Evakuierungsmaßnahmen für besonders gefährdete sowie entbehrliche Bereiche der Liegenschaft werden durchgeführt.

Zusätzliche und nicht notwendige Zugänge werden geschlossen, zum Beispiel Personendrehkreuze.

Die Wache wird verstärkt und die Bestreifung des Kasernenzauns erhöht.

Der erweiterte Militärische Sicherheitsbereich (MSB) wird verstärkt, zudem werden öffentliche Straßen innerhalb des MSB gesperrt.

Zoom

SICHER AUF ALLEN EBENEN

Die Truppe hat aufgrund ihrer einzigartigen Aufgaben ein besonderes Sicherheitsbedürfnis. Y verschafft einen Überblick über die **Sicherheitsarchitektur der Bundeswehr**.

TEXT Frank Buchstein

ARBEITS- UND BETRIEBS-SCHUTZ

Arbeitsschutz soll für funktionierende Abläufe sorgen, Risiken minimieren und Unfällen vorbeugen. In der Bundeswehr hat er viele Gesichter:

Oberste Anlaufstelle ist der Leitende Sicherheitsingenieur Bundeswehr, der die Zentrale Stelle für Arbeitsschutz der Bundeswehr im Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr leitet. In den Dienststellen

sind es die Fachkräfte für Arbeitsschutz, die im technischen Arbeitsschutz ausgebildet sind, und die Betriebsärzte und Truppenpsychologen, die den medizinischen Arbeitsschutz sicherstellen. Die Fachleute in den Wehrtechnischen Dienststellen übernehmen die technische Überwachung des Materials. Dazu kommen Brand-schutzhelferinnen und -helfer, Beauftragte für Strahlenschutz, Unfallvertrauenspersonen, das Personal des Sozialdienstes und viele mehr. Sie alle leisten einen Beitrag zum Schutz am Arbeitsplatz und für die Betriebssicherheit in der Truppe. Hinzu kommen die spezifischen militärischen Arbeitsschutzvorschriften, zum Beispiel bei der Schieß-

Lärmschutzmaßnahmen gehören zum Bundeswehralltag dazu, etwa auf der Schießbahn. Die Schießaufsicht misst den Lärmpegel, Gehörschutz ist Pflicht.



Bei der Schießausbildung wird besonderes Augenmerk auf den sicheren Umgang mit der Waffe gelegt.

sicherheit oder im Lärm- und Explosionsschutz. Und wo das Ablaufdatum an Gefechtschirm, Schießbrille und ABC-Schutzmaske steht, sollte auch jeder Soldat und jede Soldatin wissen. In Zeiten, in denen die Landes- und Bündnisverteidigung im Fokus steht, muss Arbeitsschutz aber auch gut ausbalanciert sein. Im Verteidigungsfall können Arbeitsschutzvorschriften und Arbeitszeitregelungen für Soldatinnen und Soldaten außer Kraft gesetzt werden, wenn sie der Einsatzfähigkeit der Truppe im Wege stehen.



Zum Brandschutz sind Feuerlöscher in Fahrzeugen vorgeschrieben. In Kasernen müssen sie schnell erreichbar sein.

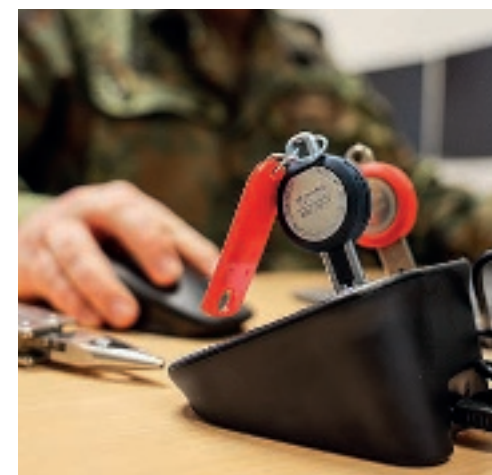
MILITÄRISCHE ABSICHERUNG

Absicherungsmaßnahmen bestimmen die Bundeswehr – in der Organisation, beim Personal sowie bei Infrastruktur und Material.

ORGANISATORISCHE ABSICHERUNG

Vom Operativen Führungskommando über das Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen bis zum Kasernenkommandanten und dem Wachdienst vor Ort: Die Absicherung von militärischen Bereichen und militärischen Sicherheitsbereichen ist auf viele Schultern verteilt. Zudem hat immer nur der Personenkreis Zugriff auf Informationen, Materialien und Ver-

Zu sensiblen Bereichen ist der Zugang nur mit bestimmten Schlüsseln möglich, die von IT-Kräften digital kodiert werden.



schluss-sachen, der diese benötigt und über die entsprechende Befugnis verfügt. Jede Person, die für die Bundeswehr tätig ist, muss eine Verpflichtungserklärung unterschreiben, dass sie die Regeln der Militärischen Sicherheit befolgt. Je nach

Tätigkeit gehören auch Sicherheitsbelehrungen oder eine Sicherheitsausbildung dazu. In sicherheitsempfindlichen Bereichen greift der Geheim-schutz. Dieser umfasst unter anderem Zutrittsbeschränkungen zu Dienstgebäuden, Geheimhaltungsstufen für Dokumente oder spezielle abhörsichere Arbeitsumgebungen.

PERSONELLE ABSICHERUNG

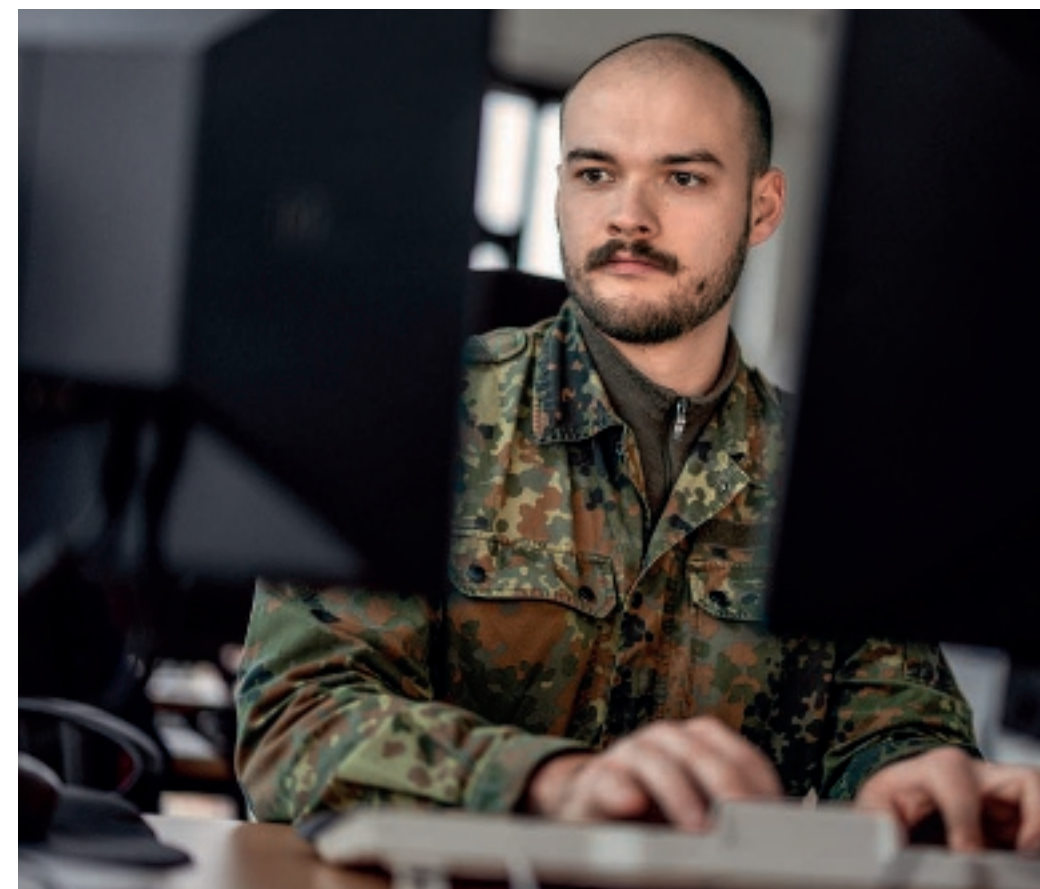
Für ihren Auftrag ist die Bundeswehr auf Menschen angewiesen, die zuverlässig sind und sich der freiheitlichen demokratischen Grundordnung verpflichtet

fühlen. Die Truppe wählt ihr Personal genau aus und überprüft es regelmäßig. Alle Soldatinnen und Soldaten durchlaufen eine Sicherheitsüberprüfung (SÜ), Gleiches gilt für Zivilbeschäftigte in sicherheitsempfindlichen Tätigkeiten. Dadurch soll unter anderem verhindert werden, dass Extremisten militärisch ausgebildet werden oder Spione Einblick in sicherheitsrelevante Bereiche erhalten. Gleichzeitig sorgt die Bundeswehr dafür, dass ihre Angehörigen bei der Ausübung ihres Jobs geschützt sind. Bei einem Einsatz im Ausland etwa greifen für die Soldatinnen und Soldaten je nach

Region gezielte Absicherungsmaßnahmen, Zivilbeschäftigte werden vorab in Sicherheitsfragen geschult. Auch werden Personen, die von der Bundeswehr in Einsatzgebieten betreut werden, im Vorfeld belehrt und vor Ort begleitet.

MATERIELLE ABSICHERUNG

Vom Munitionsdepot und dem Kasernengelände am Standort über den Übungsplatz bis hin zum Feldlager im Ausland: Die Liegenschaften der Bundeswehr sind entsprechend ihrer Sicherheitseinstufung durch bauliche und technische Absicherungsmaßnahmen geschützt. ➤



Die Geheimhaltungsstufen für Dokumente regeln, wer mit welcher Freigabestufe Zugriff hat. Auf Vertrauenswürdigkeit hin wird das Personal der Bundeswehr in der Sicherheitsüberprüfung untersucht.



privaten Videos in den sozialen Medien die Operationsfähigkeit der Truppe gefährden. Daher gelten hier klare Verhaltensregeln, die alle kennen und einhalten müssen.

MILITÄRISCHES NACHRICHTENWESEN (MILNW)

Im MilNW sind bundeswehrweit alle Fähigkeiten vereint, Erkenntnisse für Entscheidungsträger in den Streitkräften aufzubereiten und auszuwerten. Die dafür notwendigen Informationen erhalten sie zum einen über Schnittstellen zu den Nachrichtendiensten,

OPERATIVE SICHERHEIT (OPSEC)

Diese schließen nicht nur das Gelände selbst, sondern auch das komplette militärische Material und die Infrastruktur des Standorts mit ein. Denn Unbefugte sollen keine Einblicke in militärische Bereiche erhalten oder in diese eindringen können – etwa um Sabotageakte zu verüben oder Waffen und Munition zu stehlen. Zum Objektschutz gehören die Bewachung der Liegenschaften und Zugangskontrollen. Jeder Standort hat sein eigenes Absicherungskonzept – abhängig von den zu schützenden Objekten. Die aktuelle Bedrohungslage einer Liegenschaft gibt die Gefährdungsstufe an: von Alpha für niedrig bis Delta für hoch. Steigt die Bedrohung, wird auch die Absicherung verstärkt.

Unter OpSec werden alle Sicherheitsmaßnahmen zusammengefasst, die dafür sorgen, dass die Truppe ihre Aufträge erfüllen kann. Dazu gehört etwa die Kontrolle darüber, was öffentlich über die Aktivitäten einzelner Einheiten und Dienststellen bekannt sein darf und was nicht. Das gilt insbesondere für sensible Bereiche wie die Spezialkräfte oder die Einsatzgebiete. Dem Gegner sollen keine wichtigen Erkenntnisse über die eigenen Kräfte und Fähigkeiten gegeben werden. Als sicheren Kommunikationskanal nutzt die Bundeswehr daher das sogenannte Rote Netz, das unabhän-

gig von den herkömmlichen IT- und Telekommunikationswegen, dem Schwarzen Netz, funktioniert. Auch Geheimschutz und Abschirmung spielen hier eine große Rolle. OpSec schließt aber auch das Verhalten jedes Soldaten und jeder Soldatin mit ein. Vor allem im Einsatz können Standortdaten des privaten Smartphones, zu freizügige Kontakte mit Personen außerhalb der Bundeswehr oder das unbeachtete Posten von

Feldjäger sind zur operativen Absicherung immer mit dabei, wenn Einheiten sich im öffentlichen Raum bewegen.

Zum Erfolg auf dem Gefechtsfeld trägt bei, mit Informationen über das eigene Vorgehen sorgfältig umzugehen und eine gegnerische Einflussnahme abzuwehren. Operative Sicherheit und eine effektive Abschirmung schützen das Leben von Soldatinnen und Soldaten.



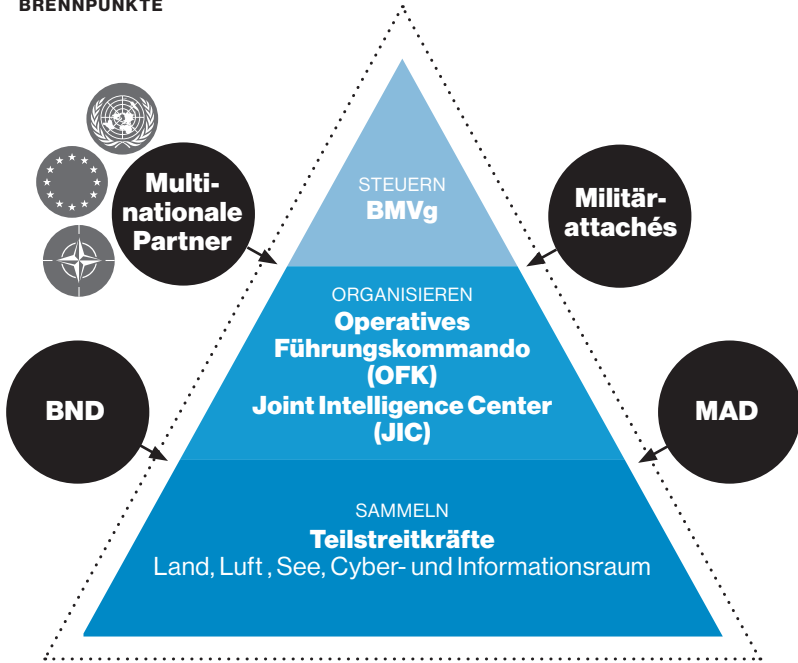
S. 40: Bundeswehr/Marco Dorow (l.o.); S. 40–41: Bundeswehr/Maximilian Schütz (u.); 41: Bundeswehr/BAA/NBW (l.); YCS Visual Lab, Infografik (r.)



den deutschen Militärattachés im Ausland sowie den multinationalen Partnern der Bundesrepublik. Zum anderen können die Teilstreitkräfte nach Bedarf Aufklärungsergebnisse zuliefern. Im Operativen Führungskommando laufen die Fäden zusammen. Das Joint Intelligence Center, das Teil des Kommando CIR ist, steuert die Bedarfsanfragen und den Informationsfluss. Die so entstehenden Analysen und

Das Abzeichen mit der Eule tragen Soldatinnen und Soldaten an ihrer Uniform, die im Militärischen Nachrichtenwesen aktiv sind.

Lagebilder dienen als Grundlage für die militärische Führung und strategische Ausrichtung der Bundeswehr. Zudem laufen sie in die operativen Planungen, in die taktische Entwicklung der Bundeswehr und in die Aufrechterhaltung der Militärischen Sicherheit ein.



Das System MilNW besteht aus drei Ebenen und den Schnittstellen zu den Nachrichtendiensten (BND, MAD), den Militärattachés und multinationalen Partnern (UN, EU, NATO).

ABSCHIRMUNG UND ABWEHR

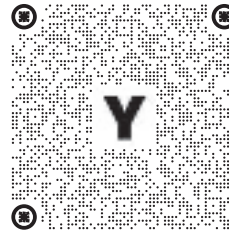
Jede Dienststelle der Bundeswehr wird ihrer Sicherheitsstufe entsprechend mit Abschirmungsmaßnahmen geschützt. Um zu verhindern, dass digitale Kommunikation abgehört wird oder Unbefugte auf sensible Informationen zugreifen können, wird zum Beispiel IT-Hardware auf ihre elektromagnetische Abstrahlung geprüft. Auch die Kräfte der Elektronischen Kampfführung verfügen über vielfältige Abschirmfähigkeiten – vor allem im mobilen Einsatz bei der Truppe. Für die Abwehr von Gefahren für die Bundeswehr ist der Militärische Abschirmdienst (MAD) zuständig – von Extremismus über Spionage bis hin zu Sabotage. So untersucht er Verdachtsfälle gegen

Bundeswehrangehörige, zum Beispiel ob ein Soldat sich extremistisch betätigt oder eine Reservistin militärische Geheimnisse verraten haben könnte. Der MAD schützt auch die Einsatzkontingente der Bundeswehr im Ausland. Deshalb erhält auch die Brigade Litauen eine MAD-Stelle. ➤

2.131

Dienstposten beim MAD gab es 2024.

Du interessierst dich für die Arbeit des MAD? Hier findest du mehr Informationen:



SICHERHEITS-MANAGEMENT

Zum Schutz der Bundeswehr müssen die Bereiche Cyber- und Informationssicherheit, Militärische Sicherheit und Datenschutz eng zusammenarbeiten. Um dem Schutzbedarf für die Bundeswehr ganzheitlich gerecht zu werden, sind diese Aufgaben daher im Organisationselement Sicherheitsmanagement zusammengeführt.

CYBER- UND INFORMATIONSSICHERHEIT

In einer zunehmend digitalen Welt, in der neben hybriden Bedrohungen der Cyber- und Informationsraum (CIR) zunehmend als mögliches Kriegsgelände verstanden wird, ist Sicherheit umso wichtiger – ein Grund, warum CIR inzwischen die vierte

Teilstreitkraft der Bundeswehr geworden ist. Ihre wichtigste Aufgabe ist der Schutz der IT-Systeme der Truppe. Der Chief Information Security Officer Bundeswehr steuert und überwacht dabei alle operativen Aufgaben zur Gewährleistung der Informationssicherheit in der Bundeswehr. Zwei zentrale Akteure dabei sind das Zentrum Cyber-Operationen in Rheinbach und das Zentrum für Cyber-Sicherheit in Euskirchen. Letzteres überwacht rund um die Uhr die IT-Systeme und Netzwerke, wehrt Cyberangriffe ab, richtet Firewalls ein und schützt vor Hackern. Zu ihm gehören auch die Kryptologen, die Spezialistinnen und Spezialisten für die Verschlüsselung des Datenverkehrs in der Bundeswehr. Auch in Auslandseinsätzen

sind die IT-Sicherheitsexpertinnen und -experten unverzichtbar – egal ob als Teil des Einsatzkontingents oder über das sogenannte Reach-Back-Verfahren von Deutschland aus. Im Nationalen Cyber-Abwehrzentrum, das die Arbeit aller deutschen Sicherheitsbehörden im Cyberraum koordiniert, ist die Bundeswehr mit dem Kommando CIR und dem MAD vertreten.

MILITÄRISCHE SICHERHEIT

Damit all die verschiedenen Sicherheitsmaßnahmen ineinandergreifen und einheitlich sind, wird militärische Sicherheit bundesweit abgestimmt und weiterentwickelt. Oberster Sicherheitsbeauftragter ist der Höhere Offizier Militärische Sicherheit Bundeswehr, ab April 2025 ist dieser

BRENNPUNKTE

483

308

Rechtsextremismus

65

Auslandsbezogener Extremismus

(etwa Unterstützung des russischen Angriffskriegs gegen die Ukraine)

35

Reichsbürger

34

Islamismus

24

Delegitimierung des Staates

(etwa in Bezug auf Corona-Maßnahmen)

16

Linksextremismus

1

Scientology

neue Verdachtsfälle auf Extremismus in der Bundeswehr 2023 (Quelle: MAD-Report 2023)

im Kommando CIR verortet. Auch die Teilstreitkräfte und Organisationsbereiche der Bundeswehr haben Sicherheitsoffiziere, die in Fragen der Militärischen Sicherheit zusammenarbeiten. In den einzelnen Dienststellen koordinieren Sicherheitsbeauftragte viele Absicherungsmaßnahmen – vom Absicherungskonzept bis zu Sicherheitsübungen. Sicherheitsbeauftragte für die Militärische Sicherheit einer Dienststelle führen dabei auch das Sicherheitstagebuch, in dem Sicherheitsvorkommnisse eingetragen werden. Sie kontrollieren zudem jährlich, wie die verschiedenen Absicherungsmaßnahmen wirken.

DATENSCHUTZ

Der Administrative Datenschutzbeauftragte (ADSB) unterstützt die Leiterinnen und Leiter der Dienststellen bei der Umsetzung des Datenschutzes. Er begleitet sämtliche Vorgänge, bei denen es um personenbezogene Daten geht. Weitere wichtige Akteure im Fachstrang sind der ADSB der Bundeswehr, die ADSB der Organisationsbereiche sowie die Fachaufsicht im BMVg. ●

S. 42: Bundeswehr/Marco Dorow

RADIO ANDERNACH

Soldaten senden für Soldaten

Das Einsatzradio

Auch im **Inland** verfügbar!

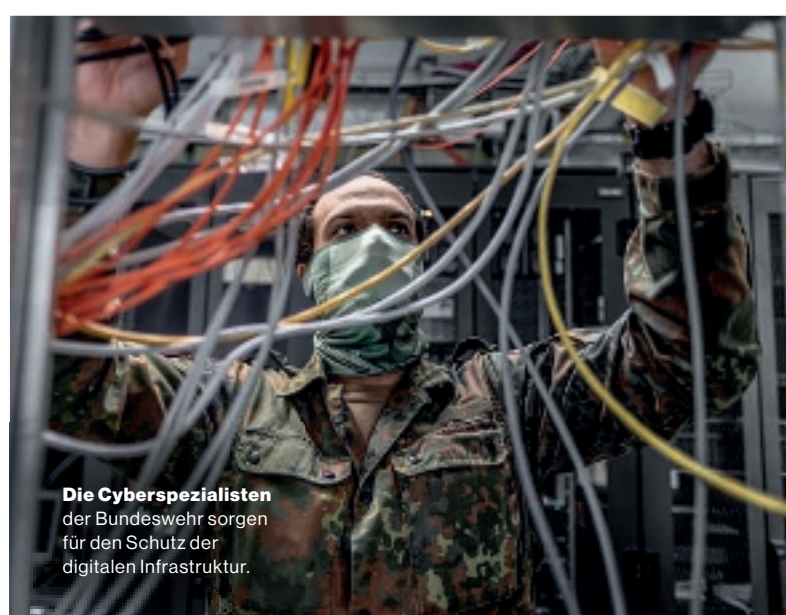
Eine für Alle!



Die **Radio Andernach App** ganz einfach auf ihrem Handy.



Mehr Infos auf **radio-andernach.de**



Die Cyberspezialisten der Bundeswehr sorgen für den Schutz der digitalen Infrastruktur.

2

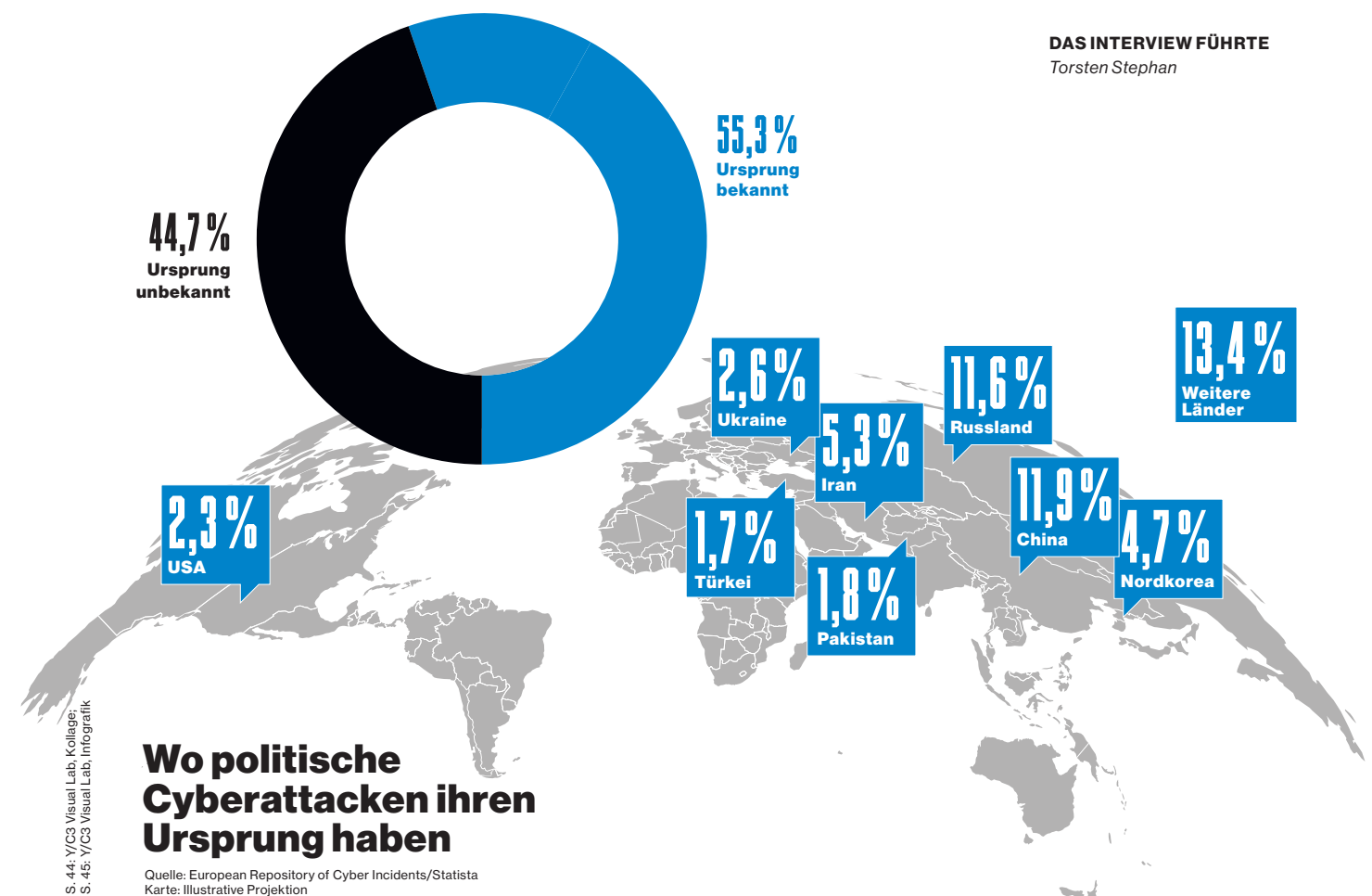
Kapitel

Cyberraum

Angriffe im Netz

Tagtäglich wird deutsche IT-Infrastruktur aus dem Internet heraus angegriffen – auch die der Bundeswehr. Wie sich die Truppe dagegen wehrt, erklärt **im Interview Oberst Andreas Kubitz**, Kommandeur des Zentrums für Cyber-Sicherheit der Bundeswehr.

DAS INTERVIEW FÜHRTE
Torsten Stephan





Oberst Andreas Kubitz
ist seit September 2024 Kommandeur
des Zentrums für Cyber-Sicherheit
der Bundeswehr.

Immer öfter hört und liest man von Cyberangriffen auf staatliche Institutionen, Behörden und Unternehmen in Deutschland. Ist die Bundeswehr auch davon betroffen?
Oberst Andreas Kubitz: Ja, die Bundeswehr ist regelmäßig Ziel von Cyberangriffen. Die Auswirkungen waren aber aufgrund unserer technischen Vorkehrungen und unseres Fachpersonals bisher eher gering.

Was wird bei der Bundeswehr angegriffen?
Ein häufiges Angriffsziel ist unsere Bürokommunikationsinfrastruktur. Über 200.000 Mitarbeitende in der Bundeswehr erhalten täglich E-Mails und nutzen das Internet. Es gibt also eine dauerhafte Verbindung nach draußen in den Cyberraum, wo sich Angreifer frei bewegen können. Die Informationstechnik der Bundeswehr umfasst natürlich wesentlich mehr: Waffen- und Führungssysteme oder auch Haustechnik wie zum Beispiel Überwachungskameras und Zugangskontrollanlagen können vom Gegner für einen Angriff, Spionage oder Störung genutzt werden.

In welcher Form wird die Truppe angegriffen?
Wir beobachten vielfältige Angriffe. Sie reichen von Phishing-Attacken über Malware-Infektionen bis zu gezielten Spionageversuchen durch Advanced Persistent Threats, kurz APT. Für Ransomware-Angriffe ist die Bundeswehr nicht attraktiv. Kriminelle können sich sicher sein, dass die Bundeswehr kein Lösegeld bezahlen würde. Gefährlicher ist ein Datendiebstahl, bei dem Kriminelle versuchen, in unsere Systeme einzudringen und die dort abgefishchten Daten an andere Staaten zu verkaufen.

Wie schützt sich die Bundeswehr gegen Cyberangriffe?
Jeder in der Truppe ist ein potenzielles Einfallstor für einen Angriff. Daher konzentrieren wir uns nicht nur auf die technische Absicherung, sondern betrachten Informationssicherheit als Gesamtsystem. Die Verantwortlichkeiten sind dezentral organisiert: In allen Dienststellen, Organisationsbereichen und Teilstreitkräften gibt es Personal, das technische und

organisatorische Maßnahmen etabliert, prüft und berät. Wichtig sind auch die Einrichtungen, die den IT-Betrieb sicherstellen. Die Technikerinnen und Techniker müssen oft kreativ sein und unter Zeitdruck arbeiten – und dürfen dabei die Informationssicherheit nie aus dem Blick verlieren.

Welche Rolle spielt dabei das Zentrum für Cyber-Sicherheit der Bundeswehr?
Das Zentrum für Cyber-Sicherheit der Bundeswehr, kurz ZCSBw, wurde 2017 aufgestellt. Unser Name ist Programm: Es geht nicht nur um IT-Sicherheit, also technische Schutz- und Überwachungsaufgaben, sondern um einen umfassenden operativen und taktischen Auftrag. Fast 600 militärische und zivile Mitarbeitende arbeiten hier, viele sind hochspezialisierte IT-Expertinnen und -Experten. Wir überwachen den gesamten Cyberraum der Bundeswehr. Dazu gehört, neu eingeführte IT-Systeme zu prüfen, allgemeine Vorgaben zu machen und bei Sicherheitsvorkommnissen zu unterstützen. Bei Cyberangriffen sind unsere mobilen Teams schnell vor Ort. Wir führen auch Penetrationstests von Systemen durch und prüfen die Abstrahlungen von IT. Wir sind also breit aufgestellt. Wichtig ist, dass wir unsere Fähigkeiten stets an die Angriffsmethoden im Cyberraum anpassen. Ein Beispiel dafür ist der Einsatz von künstlicher Intelligenz: Die Zunahme von KI stellt uns vor enorme Herausforderungen, aber sie kann unsere Cyberabwehr auch stärken. Eine gute KI, die von Fachpersonal trainiert und kontrolliert wird, kann Phishing-Mails, Deep Fakes oder ungewöhnliche Verhaltensmuster in Bundeswehrnetzwerken frühzeitig identifizieren und bei der Abwehr unterstützen.

Wie oft passieren solche Angriffe?
Ich bin bei konkreten Zahlen und Beispielen sehr zurückhaltend. Generische Kräfte könnten daraus Rückschlüsse auf unsere Sensoren und Methoden erhalten. Ein weiterer Grund: Was ist ein Cyberangriff? Ist ein Computervirus, der an einer Phishing-E-Mail angehängt ist, aber an unserer Peripherie erkannt und isoliert wurde, ein Angriff oder ein „Abklopfen“ unserer Systeme auf potenzielle Schwachstellen?

S. 46: Bundeswehr/All Rahmama
S. 47: Y/C3 Visual Lab, Infografik (2), Shutterstock/PM, Pick&Place (Z.Z.r.)

**CYBERCRIME
GRUPPEN
FANCY BEAR,
VELVET
CHOLLIMA,
DARKHOTEL & CO.**

Das BSI zählte für 2024 22 APT-Gruppen, die sich auf die Verwaltung, Verteidigung und Sicherheitsbereiche des deutschen Staates eingeschossen haben.

Fünf Arten von Angriffen



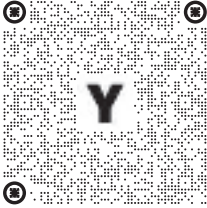
- Malware**
Computerprogramme, die schädliche Operationen ausführen, werden als Schadprogramme (englisch: Malware) bezeichnet. Zum Beispiel durch E-Mail-Anhänge oder Links, auf die geklickt wird, kann sich ein Schadprogramm installieren.
- Ransomware**
Als Ransomware werden Schadprogramme bezeichnet, die dem Opfer den Zugriff auf ein angegriffenes System verwehren und erst gegen eine Lösegeldzahlung wieder freigeben.
- APT (Advanced Persistent Threat)**
APT-Angriffe sind langfristig und aufwendig geplante Angriffe auf ausgewählte herausgehobene Ziele. Sie dienen häufig der Beschaffung von Informationen über das Ziel und gegebenenfalls der Sabotage.
- Phishing**
Beim Phishing nutzen Betrüger gefälschte E-Mails oder Websites, die vertrauenswürdige Unternehmen imitieren. Sie fordern die Empfänger auf, sensible Daten wie Zugangsdaten oder Zahlungsinformationen preiszugeben.
- DDoS (Distributed Denial of Service)**
Durch das Überfluten von (Web-)Servern mit Anfragen sind zum Beispiel Webseiten nicht mehr erreichbar. Das Ziel der Angreifer besteht darin, die angegriffenen Dienste so weit zu überlasten, dass diese lahmgelegt werden.

Zentrum für Cyber-Sicherheit der Bundeswehr
Das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) ist die zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der IT-Systeme und -Services der Bundeswehr.



Wir bearbeiten jedes Informationssicherheitsvorkommnis auf einer eigens dafür entwickelten Plattform. 2023 wurden mehr als 3.500 Tickets bearbeitet. Das gibt ein grobes Gefühl über die Menge, wobei die Komplexität und der Aufwand pro Ticket sehr unterschiedlich sind. Was ich sagen kann: Wir erleben seit der russischen Vollinvasion in der Ukraine im Februar 2022 einen erheblichen Anstieg von Distributed-Denial-of-Service (DDoS)-Ereignissen gegen öffentliche Portale der Bundeswehr. Gegnerische Gruppen fluten unsere Server mit Anfragen und stören unsere öffentlichen Schnittstel-

len und Webseiten. Auswirkungen auf operative Fähigkeiten der Bundeswehr haben sie aber nicht. Wir stellen unsere Architekturen und Prozesse auf die Bedrohungslage ein, damit unsere Systeme noch resilienter werden. Es geht aber nicht nur um die Bundeswehr. Cybersicherheit ist eine gesamtstaatliche Aufgabe. Ich würde mir wünschen, dass mehr Bürgerinnen und Bürger wüssten, was jeder privat und beruflich dagegen tun kann. Prävention beginnt bei jedem Einzelnen. Wir müssen uns bewusst werden, dass unser digitales Handeln Auswirkungen auf die Sicherheit aller haben kann. ➤



„Die Lage der IT-Sicherheit in Deutschland 2024“
Der Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) erläutert unter anderem die Bedrohungslage im Cyberraum, verschiedene Angriffsarten und Gegenmaßnahmen. Du findest ihn als PDF-Download unter dem QR-Code.

„Die Bedrohungslage für die deutsche Wirtschaft verschärft sich.“

Aus dem **BSI-Report 2024**

Was weiß man über die Drahtzieher und ihre Hintergründe?

Das ZCSBw nimmt grundsätzlich keine Attribution, sprich Zuordnung von Angriffen zu Akteuren, vor. Aber wir sammeln Beweise und leiten sie den Strafverfolgungsbehörden weiter. Manchmal ist es offensichtlich, woher ein Angriff kommt. Gerade Hackingaktivisten bekennen sich häufig öffentlich, um einen vermeintlichen Erfolg für sich zu verbuchen. Viele Gruppen haben bestimmte Methoden und Werkzeuge, die wir wiedererkennen und auf die wir unsere Abwehr passgenau abstimmen. Für Staaten sind Cyberangriffe günstige Möglichkeiten, um geopolitische und wirtschaftliche Ziele zu erreichen – ohne in einen militärischen Konflikt einzutreten. Russland hat hochentwickelte Fähigkeiten. Staatlich unterstützte Hackergruppen wie APT28 oder APT29 nutzen Schwachstellen in Netzwerken aus. Die Angriffsmöglichkeiten reichen von APT und Ransomware bis zu Phishing-Kampagnen. Dazu kommen Botnets und die Manipulation sozialer Medien. China geht es auch um Zugang zu sensiblen Daten und ökonomische Interessen. Als führende Industrienation sind wir ein attraktives Ziel, um geistiges Eigentum, technologische Innovationen und Produktionsdaten auszuspähen. Spezialisierte Hackergruppen wie APT41 oder Hafnium könnten auch unsere kritischen Infrastrukturen stören. Auch Nordkorea verfügt mit Hackergruppen wie Lazarus über gute Fähigkeiten zu Cyberangriffen, inklusive Nutzung von Malware und Social-Engineering-Techniken.

Tauschen Sie sich mit anderen Stellen über ihre Erfahrungen aus?

In der EU, der NATO und innerhalb Deutschlands sowie mit Österreich und der Schweiz arbeiten wir sehr eng zusammen. Wir haben gute Austauschprozesse über erkannte Angriffsverfahren und -muster etabliert und führen gemeinsame Übungen durch.

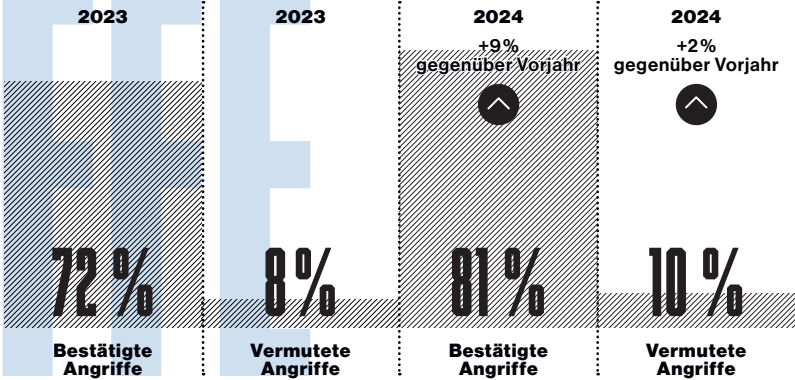
Die nationale Zusammenarbeit ist genauso wichtig. Denn innere und äußere Sicherheit lassen sich nicht trennen. Deshalb wurde das Nationale Cyber-Abwehrzentrum aufgebaut, in dem unter anderem das Innen- und das Verteidigungsministerium vertreten sind. Für ein gemeinsames Lagebild und um Aktionen zu planen, unterhalten wir vom ZCSBw auch enge Kontakte zum CERT-Bund, der zentralen Anlaufstelle für Bundesbehörden bei IT-Sicherheitsvorfällen, zu Telekommunikationsanbietern sowie vielen anderen Akteuren.

Das unberechtigte Eindringen in fremde IT-Systeme ist in Deutschland verboten. Was macht das ZCSBw bei einem akuten Cyberangriff?

Es ist unser Kernauftrag, die Informationssicherheit in der Bundeswehr zu schützen und wiederherzustellen, wenn diese gestört wurde. Das ist eine Dauereinsatzaufgabe, die rund um die Uhr durch das Cyber Security Operations Centre (CSOCBw) erfüllt wird. Unsere Sensorik liefert das technische Lagebild dafür. Die Daten über IT-Systeme, Übergänge in andere Netzwerke und registrierte Veränderungen werden weitgehend automatisiert ausgewertet. Wenn ein Angriff auf die Bundeswehr erkannt wird, beheben unsere Spezialistinnen und Spezialisten den Schaden schnellstmöglich. Sie werten ihn aus und sichern Beweise, um einen vergleichbaren Angriff in Zukunft auszuschließen. Neben der akuten Reaktion suchen wir auch nach Spuren, die auf die Anwesenheit von Eindringlingen in den Bundeswehrnetzen schließen lassen. Man nennt das „Cyber Threat Hunting“, also das Aufspüren von Cyber-Bedrohungen. Das gleicht oft der sprichwörtlichen Suche nach der Nadel im Heuhaufen. Je nach Aufwand kann ein Vorfall in wenigen Minuten entdeckt, dokumentiert und abgeschlossen sein oder sich über Wochen hinziehen, bis alles gesichert ist und Funktionen wiederhergestellt sind.

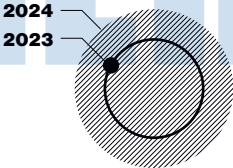
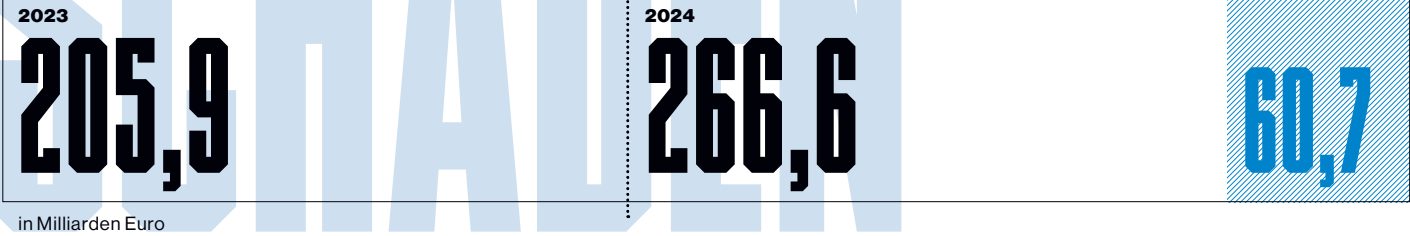
Anstieg der Fälle

Bei einer jährlich durchgeführten Umfrage des Branchenverbands Bitkom gaben 2024 81 Prozent der Unternehmen an, in den vergangenen zwölf Monaten vom Diebstahl von Daten und IT-Geräten sowie von digitaler und analoger Industriespionage oder Sabotage betroffen gewesen zu sein. Weitere zehn Prozent vermuteten dies.



Hohe finanzielle Verluste

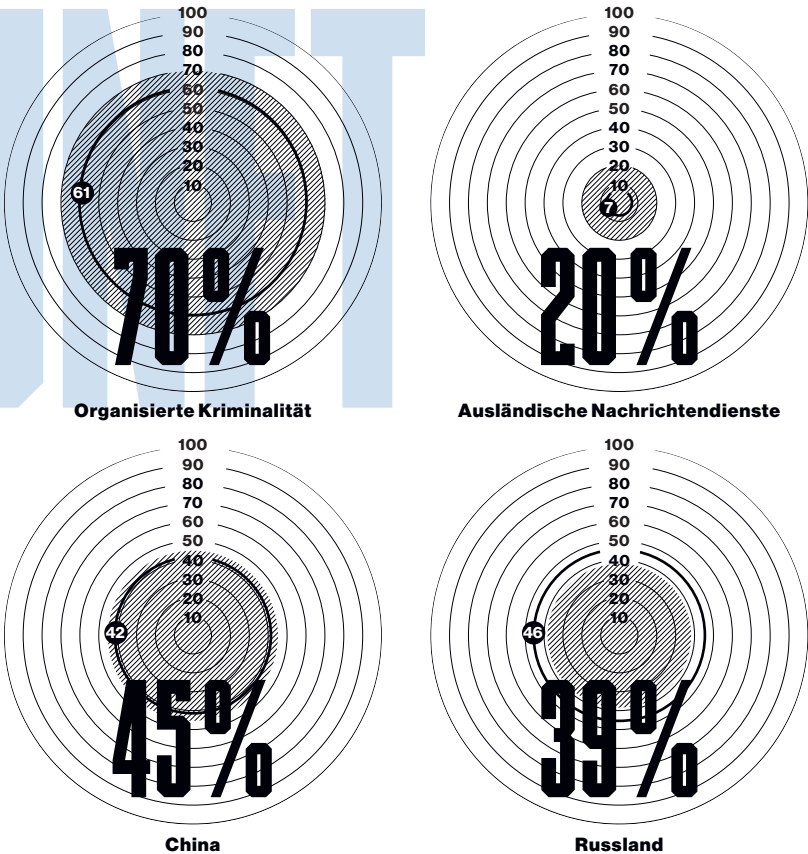
Der Bitkom-Umfrage zufolge sind die Schäden durch analoge und digitale Angriffe auf die deutsche Wirtschaft 2024 im Vergleich zum Vorjahr deutlich gestiegen.



Zunahme der Angriffe aus Osteuropa

70 Prozent der Unternehmen, die Opfer wurden, konnten Angriffe der organisierten Kriminalität zuordnen. Zur wichtigsten Ausgangsbasis für Angriffe auf die deutsche Wirtschaft hat sich China entwickelt.

Zugenommen haben zugleich Angriffe aus osteuropäischen Staaten außerhalb der EU. Rückläufig sind Angriffe aus Deutschland selbst sowie aus Russland.



Sie entsenden auch mobile Teams, die bei Cyberangriffen unterstützen. Wer fragt die Bundeswehr an und wie läuft das ab?

Grundsätzlich verlegen unsere Kräfte selten an den Ort des Geschehens. Unsere hochgradige Vernetzung ermöglicht es uns, Aktionen an IT-Systemen verzugslos und standortunabhängig durchzuführen. Im Reach-Back-Verfahren können unsere IT-Expertinnen und -Experten aus Euskirchen unterstützen. Unsere flexiblen Incident Response Teams können bei Bedarf auch vor Ort – weltweit und sogar unter Gefechtsbedingungen – ihren Auftrag erfüllen. Bei Bedarf können sie auch Amtshilfe leisten, wie im Juli 2021, als wir den Landkreis Anhalt-Bitterfeld nach einem schweren Angriff auf dessen IT-Infrastruktur unterstützten. Wir haben Fachleute entsandt, die die Lage begutachteten und bei der Behebung der Schäden halfen. Abschließend gaben wir dem Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, unsere Erkenntnisse weiter. Wir wollen nicht in Konkurrenz zu zivilwirtschaftlichen Anbietern treten, sondern setzen auf Zusammenarbeit. Beim Cyberangriff im August 2020 auf die BwFuhrpark-Service GmbH konzentrierten wir uns auf die Suche nach kompromittierten Verbindungen zum Bundeswehrnetz. Mit der Analyse und Behebung des Schadens wurde ein ziviles Unternehmen beauftragt.

Das ZCSBw unterstützt Bw-Dienststellen auch im Umgang mit der Abstrahlung der dienstlichen IT. Worum geht es dabei genau?

Jedes technische Gerät gibt bei seiner Nutzung elektromagnetische Strahlen frei, genauso wie ein Auto. In diesen Emissionen können unter Umständen sicherheitsempfindliche Informationen enthalten sein. Diese „kompromittierte Abstrahlung“ kann durch elektromagnetische Wellen – zum Beispiel über das WLAN – in die Umwelt übertragen werden. Ein Angreifer kann diese Wellen mit einer Antenne empfangen und die enthaltenen Informationen auswerten. Der Schutz unserer IT vor elektromagnetischer Abstrahlung ist unerlässlich. Unsere Abstrahlprüferinnen und

-prüfer sind mit einer speziellen Sensorik ausgestattet, um die Strahlung von technischen Geräten zu prüfen und Dienststellen der Bundeswehr über mögliche Sicherheitslücken zu informieren. Es geht uns vor allem um Prävention und Beratung.

Wie läuft so eine Prüfung ab und was kann man gegen Abstrahlung tun?

Wir beraten die jeweiligen Verantwortlichen von IT-Systemen, zum Beispiel die Informationssicherheitsbeauftragten einer Dienststelle, in allen Fragen der Abstrahlsicherheit. Das umfasst sowohl die Planung und Implementierung neuer Systeme und Infrastrukturen als auch die Absicherung bestehender Strukturen, Räume oder Gebäude, in denen eingestufte Informationen verarbeitet werden. Für ein gutes Schutzkonzept können bautechnische Maßnahmen notwendig sein, um Systeme zu „härten“, damit von ihnen keine oder nur eine sehr geringe kompromittierende Abstrahlung ausgeht. Diese Maßnahmen werden in der Regel bereits von den Herstellern umgesetzt. Die bautechnische Härtung von Räumen und Gebäuden sowie die technische Absicherung kompletter Waffensysteme sind sehr wichtig. Ein Beispiel: Unsere Prüferinnen und Prüfer sind fester Bestandteil bei der Einführung des neuen F-35-Kampfflugs ab 2027. Sie stellen sicher, dass von den Jets und der Infrastruktur keine kritische Abstrahlung ausgeht. Erst dann können die F-35 an die Bundeswehr übergeben werden. Grundsätzlich werden die Abstrahlprüfungen bei Geräten alle sechs Jahre wiederholt. Wir prüfen, ob die Grenzwerte etwa zur Verarbeitung von VS-Dokumenten noch eingehalten werden oder die Technik erneuert werden muss. Dafür hat unser Zentrum vier Abstrahlprüflabore an verschiedenen Standorten. Um Infrastrukturen und Waffensysteme zu vermessen, nutzen wir zehn Mess- und Prüffahrzeuge, die im In- und Ausland eingesetzt werden können.

Zum Abschluss:

Ist der Cyberraum noch aus den Streitkräften wegzudenken?

Nein, der Cyberraum ist zu einem entscheidenden Faktor in der modernen Kriegführung geworden. Eine gute

„Der Cyberraum ist zu einem entscheidenden Faktor in der modernen Kriegführung geworden.“

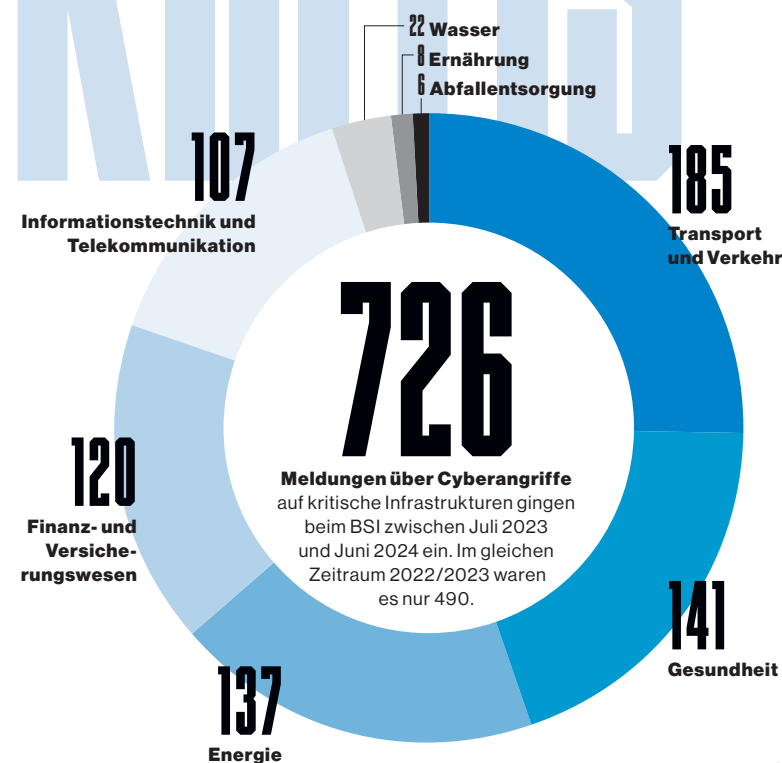
Oberst Andreas Kubitz,
Kommandeur ZCSBw

Cyberverteidigung ist deshalb unerlässlich. Sie schützt kritische Infrastrukturen, Kommunikationssysteme und die eigene Waffensteuerung vor Angriffen. Ohne Informationssicherheit könnte die eigene operative Handlungsfähigkeit massiv beeinträchtigt werden. In asymmetrischen Konflikten und hybriden Bedrohungsszenarien spielen Cyberangriffe heute eine Schlüsselrolle, um Gegner zu destabilisieren, Spionage zu betreiben oder Desinformation zu verbreiten. Eine gute Cyberabwehr verhindert Datenverluste, bewahrt die Integrität und Verfügbarkeit von Systemen und stärkt die Handlungsfähigkeit von Streitkräften. Am Ende geht es auch um Abschreckung: Eine robuste Verteidigung im Cyberraum signalisiert potenziellen Angreifern, dass ihre Aktionen wirkungslos sind und sehr kostspielig werden könnten. ●

S. 50: Y/C3 Visual Lab, Infografik

Cyberangriffe auf kritische Infrastrukturen nach Sektoren

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltige Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Zu den KRITIS-Sektoren gehören Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung. In Deutschland waren Ende September 2024 1.127 Betreiber mit 2.086 Anlagen registriert.



BUNDESWEHR INTRAPRENEURSHIP BOOTCAMP



INNOVATION IN UNIFORM

DAS IST INTRAPRENEURSHIP

Bundeswehr Intrapreneurship ist eine neuartige Methode des Innovationsmanagements bei den Streitkräften, die innovative Menschen dazu befähigt und dabei unterstützt, ihre Ideen eigeninitiativ voranzutreiben.

DAS IST DAS BOOTCAMP

Mit dem Bootcamp vom Cyber Innovation Hub der Bundeswehr möchten wir Dir das Handwerkzeug eines Intrapreneurs in der Bundeswehr geben.

WER KANN MITMACHEN?

Alle Angehörigen der Bundeswehr. Melde Dich einfach mit einer offiziellen Bundeswehr E-Mail an und werde Teil des Netzwerks von innovativen Vordenker:innen.

WIE IST DER ABLAUF?

In fünf kurzen Modulen über sieben Wochen erfährst Du die Grundlagen des Innovationsmanagements kennen:

1_Was ist eigentlich Innovation?

2_Innovation in Organisationen

3_Intrapreneurship

4_Digital Innovation Unit (DIU) im militärischen Kontext

5_Bundeswehr Intrapreneurship

Du lernst wie Deine Idee zu einer Innovation entwickelt werden kann und welche Rolle der Cyber Innovation Hub der Bundeswehr dabei spielt. **Und das alles ganz unkompliziert und flexibel online.**

KOMM' MIT INS BOOTCAMP!

Jetzt QR-Code scannen, mit Deiner Bundeswehr E-Mail anmelden **und kostenlos mitmachen.**
www.cyberinnovationhub.de/innovation/innovationskultur/boot-camp



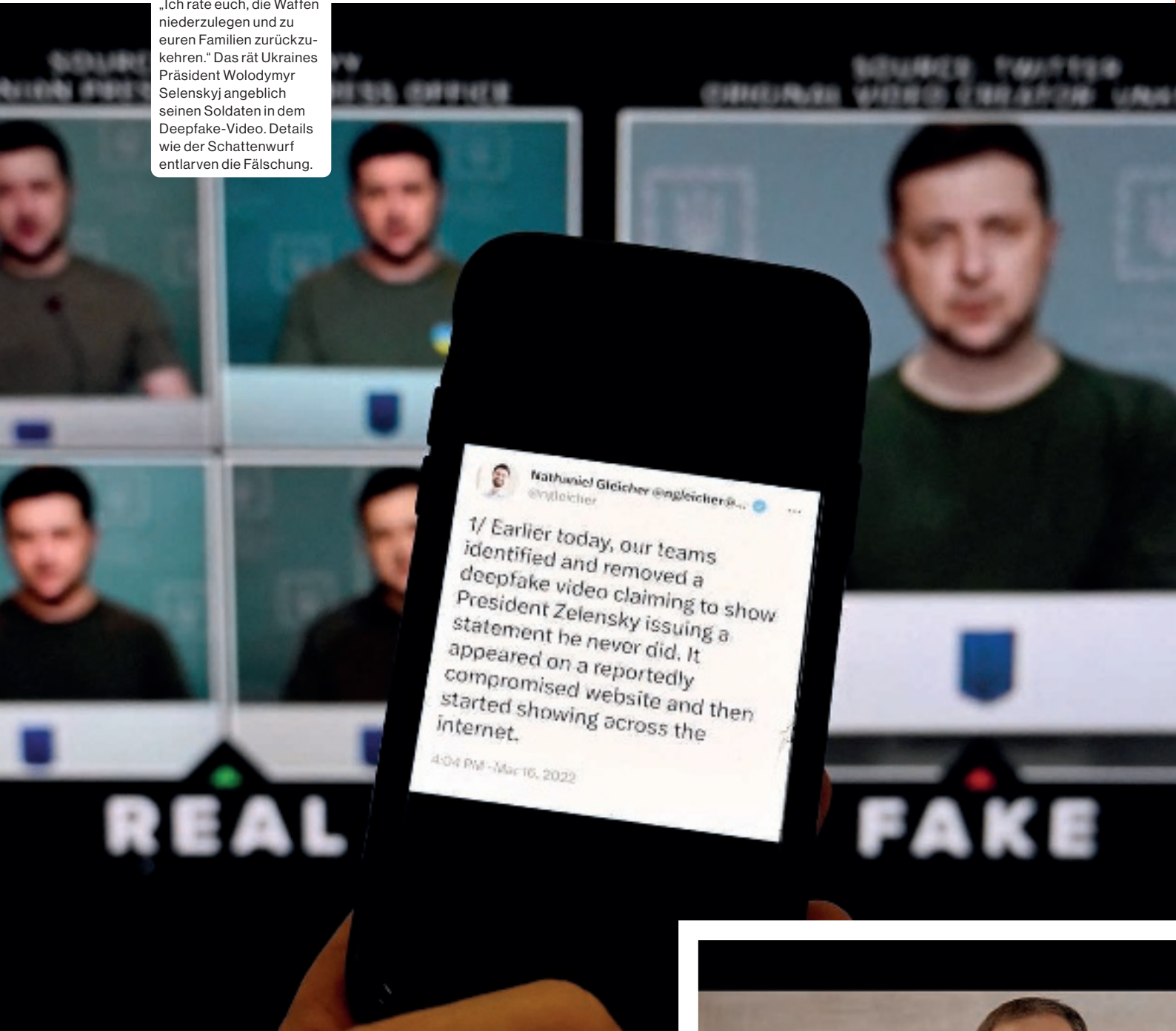
Russland bedroht die NATO und nutzt dafür Formen der hybriden Kriegführung. Ein wichtiger Bestandteil ist Desinformation, um die Öffentlichkeit in den westlichen Ländern zu verunsichern und zu beeinflussen. Wie geht Russland dabei vor – und wie lassen sich Falschmeldungen erkennen?

TEXT Ronald Rogge

Die Biolab-Verschöörung
Am 16. Mai 2022 wiederholte Russlands Präsident Wladimir Putin in einer Fernsehansprache die Behauptung, man habe in der Ukraine US-amerikanische Biowaffenlabore gefunden. Mit dieser und anderen Falschinformationen rechtfertigt Russland seinen völkerrechtswidrigen Angriffskrieg gegen das Nachbarland.

Deutschland habe gemeinsam mit den USA und der Ukraine an Biowaffen geforscht. Das hat nicht irgendjemand in den sozialen Medien gepostet, das hat kein selbsternanntes Online-Nachrichtenportal geschrieben und das hat auch niemand anonym per Video auf einer Internetplattform verbreitet. Es war die russische Regierung selbst, die diese gezielte Falschinformation im März 2022 in einer Dringlichkeitssitzung der Vereinten Nationen vortragen hatte. Ein Beispiel für Desinformation, die ganz offiziell von einem autokratischen Staat verbreitet wird.

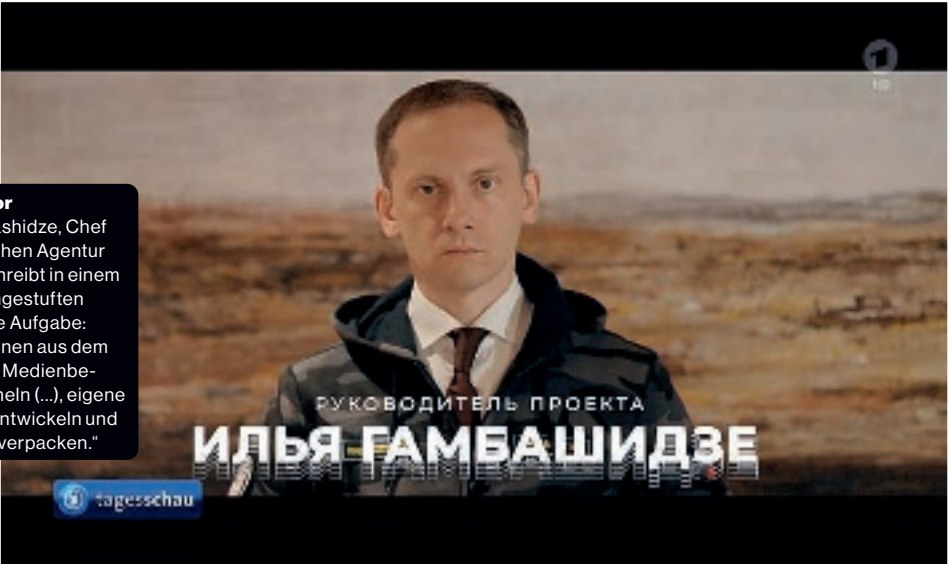
Fingierte Kapitulation
„Ich rate euch, die Waffen niederzulegen und zu euren Familien zurückzukehren.“ Das rät Ukraines Präsident Wolodymyr Selenskyj angeblich seinen Soldaten in dem Deepfake-Video. Details wie der Schattenwurf entlarven die Fälschung.



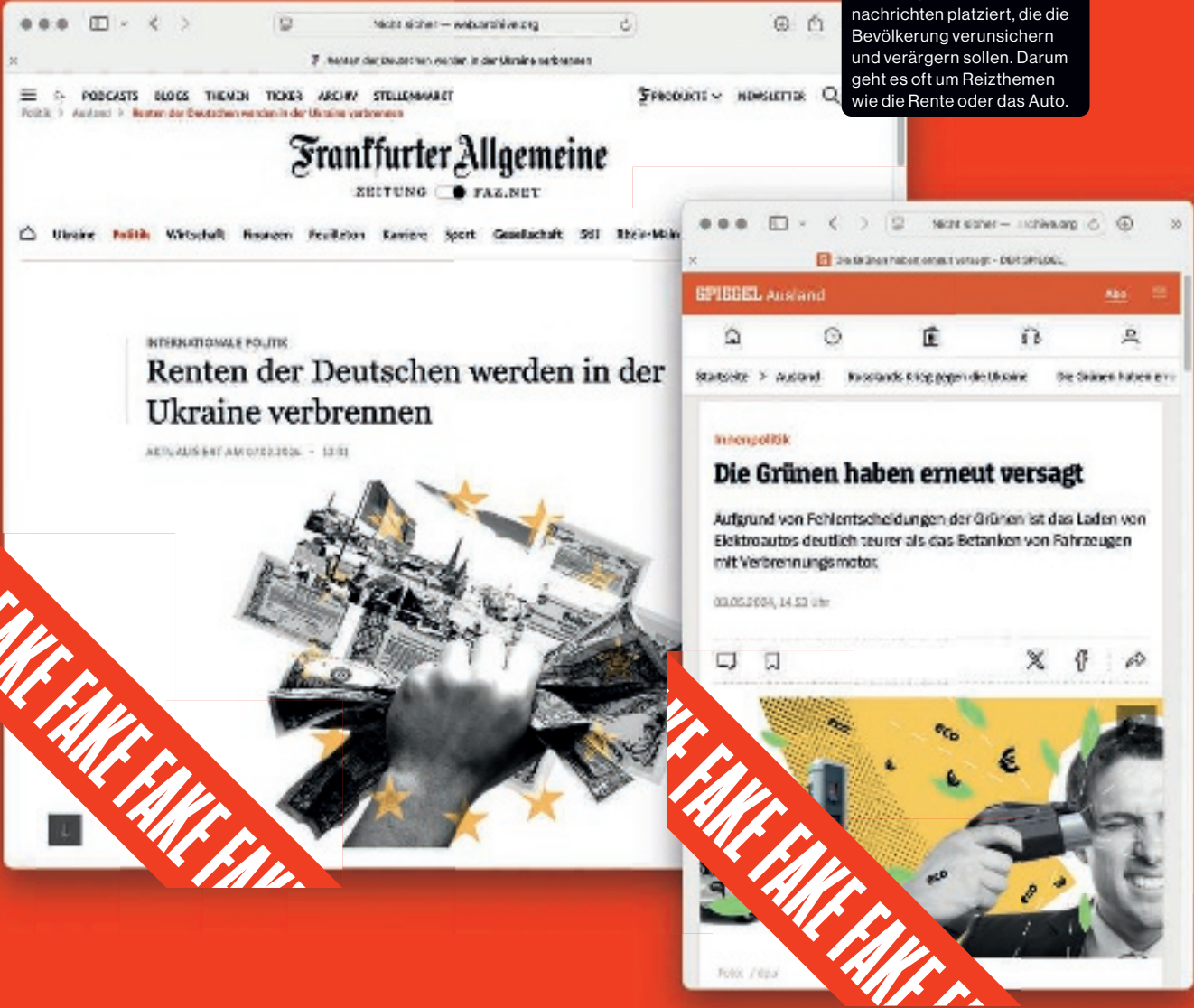
Längst nicht immer ist der Absender von Desinformation so klar erkennbar wie im Fall der Biowaffen-Verschwörung. Gerade auf Social-Media-Plattformen verbreiten sich Falschmeldungen schnell und kaum kontrollierbar, wie etwa Fotos von prominenten Personen, die mit grob verkürzten oder sogar gefälschten Zitaten versehen sind. Kurz nach Beginn des russi-

schen Angriffskriegs gegen die Ukraine wurde eine vermeintliche Video-botschaft des ukrainischen Präsidenten Wolodymyr Selenskyj verbreitet, in der dieser die Armee zur Kapitulation aufrief. Dazu hatten sich Hacker Zugriff auf die Webseite des ukrainischen Nachrichtensenders Ukraine 24 verschafft und dort den Deep Fake veröffentlicht.

Spindoktor
Ilya Gambashidze, Chef der russischen Agentur SDA, beschreibt in einem als echt eingestuften Video seine Aufgabe: „Informationen aus dem westlichen Medienbereich sammeln (...), eigene Narrative entwickeln und in Content verpacken.“



Aufregung erzeugen
Auf gefälschten Websites, die bekannte und vertrauenswürdige Nachrichtenportale imitieren, werden Falschnachrichten platziert, die die Bevölkerung verunsichern und verärgern sollen. Darum geht es oft um Reizthemen wie die Rente oder das Auto.



Gefechtsfeld Internet

Natürlich ist Russland nicht der einzige Akteur, der gezielt Desinformation betreibt. Auch andere autokratische Staaten, nicht-staatliche Organisationen oder Privatpersonen verbreiten Falschinformationen. Klar ist aber: Russland ist in Deutschland sehr aktiv, wie auch die Doppelgänger-Kampagne gezeigt hat, über die prorussische Meinungen massenweise verbreitet wurden. Im Zentrum der Aktion standen gefälschte Nachrichtenseiten sowie tausendfache Postings auf Social-Media-Plattformen. Bekannte

und vertrauenswürdige Nachrichtenportale wurden nachgebaut und darüber Falschmeldungen verbreitet. Zudem wurden neue deutschsprachige Portale ins Netz gestellt, die sich als unabhängige Nachrichtenseiten ausgaben. Die Leserinnen und Leser wurden unter anderem über Social Media auf die Seiten gelockt. Hier spielten insbesondere die Plattformen X (ehemals Twitter) und Facebook eine Rolle. Das Auswärtige Amt identifizierte allein von Mitte Dezember 2023 bis Ende Januar 2024, innerhalb von nur sechs Wochen, mehr als

50.000 gefälschte Nutzerkonten auf X, die über 1,8 Millionen deutschsprachige Tweets absetzten. Ziel war es, Unwahrheiten zu verbreiten, um beispielsweise Unmut gegen die Bundesregierung zu schüren und die deutsche Unterstützung für die Ukraine zu verunglimpfen. Zentral gesteuert wurde diese Kampagne nach Angaben der US-Regierung von der Kreml-nahen Social Design Agency (SDA). Im September 2024 warf die US-Regierung der SDA auch vor, die US-Präsidentenwahlen im November beeinflussen zu wollen.

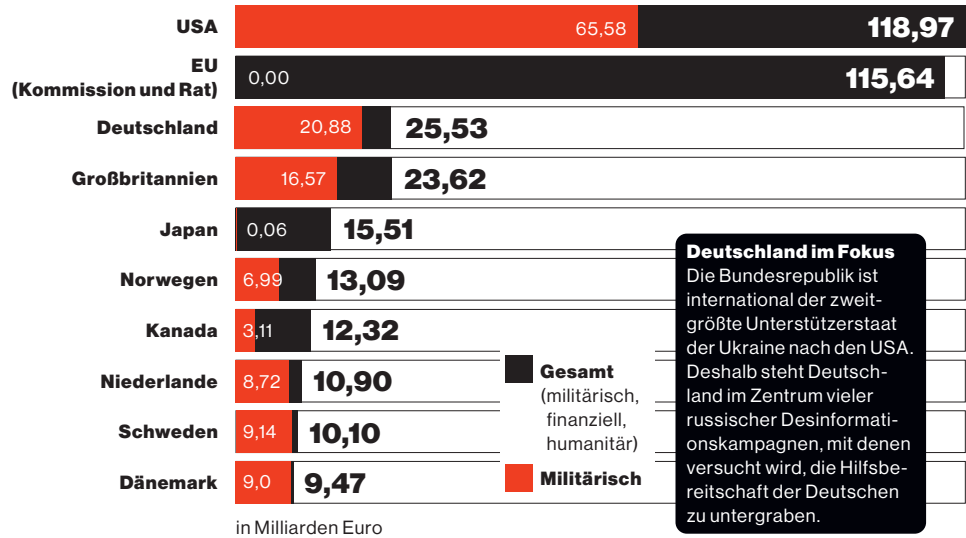


Hilfe für die Ukraine
Deutschland unterstützt die Ukraine im Kampf gegen Russland mit militärischen und zivilen Mitteln. Ein Schwerpunkt der Rüstungslieferungen ist die Luftverteidigung, hier das Flugabwehr-raketensystem Patriot.

Russlands Beweggründe

Was erhofft sich Russland von den Aktivitäten? Seit Jahren baut es die NATO als Feindbild auf. Präsident Wladimir Putin behauptet, das westliche Verteidigungsbündnis bedrohe sein Land. Dabei ist Russland selbst die Gefahr – vor allem für seine Nachbarn, wie der Angriffskrieg gegen die Ukraine oder innen-

politische Einmischungen in Moldau und Georgien zeigen. Um die NATO-Staaten politisch zu schwächen, bedient sich Russland Formen der hybriden Kriegführung, insbesondere eines Informationskriegs. Deutschland steht dabei besonders im Fokus. Nach den USA trägt Deutschland den zweitgrößten Anteil an den internationalen Militärhilfen für die Ukraine und hat mehr als eine Million ukrainische Flüchtlinge aufgenommen. Gegen Russland trägt die Bundesregierung zahlreiche internationale Sanktionen mit. Zudem unterstützt Deutschland die Ermittlungen des Internationalen Strafgerichtshofs gegen Russland wegen vielfacher Kriegsverbrechen und Menschenrechtsverletzungen.



Die Waffen des Aggressors

Russische Desinformation richtet sich an bestimmte Zielgruppen, bei denen die Falschmeldungen besonders verfangen sollen. Das kann zum Beispiel die deutsche Bevölkerung im Allgemeinen sein oder einzelne Gruppen wie russischstämmige Deutsche, die vielleicht weniger kritisch gegenüber Russland sind, oder Menschen, die für Verschwörungstheorien empfänglich sind. Falschmeldungen sollen Verunsicherung auslösen oder Meinungen zugunsten Russlands verändern. Häufig werden auch Personen, Institutionen oder Organisationen verunglimpft. Der Bundesregierung wird zum Beispiel vorgeworfen, Geld in der Ukraine zu verschwenden. Oder es werden Lügen über die Bundeswehr verbreitet: Anfang 2017 streute Russland Gerüchte über eine angebliche Vergewaltigung einer jungen Litauerin durch deutsche Soldaten, um die Unterstützung der litauischen Bevölkerung für die NATO-Truppen im Land zu untergraben. Den Hinterleuten geht es darum, mit kontroversen Positionen öffentliche Debatten aufzuheizen und zu radikalisieren. Sie schüren Misstrauen gegenüber anerkannten Medien, politischen Entscheidungsträgern und der demokratischen Ordnung an sich. Es ist der Versuch, einen politischen Gegner von innen heraus zu schwächen. Im Fokus vieler Falschnachrichten in Deutschland steht die Anteilnahme und Unterstützung der Menschen in der Ukraine. Wenn Kyjiw dadurch vielleicht weniger Geld oder weniger Waffen und Munition erhält, hätte Russland einen Vorteil in seinem Krieg. Der virtuelle Informationskrieg und der eigentliche Kriegsschauplatz sind eng miteinander verbunden.

Doppelgänger
Die russische Doppelgänger-Desinformationskampagne nutzt seit 2022 Bilder prominenter Persönlichkeiten. Denen wird dann ein offenbar europakritisches Zitat in den Mund gelegt. Ziel ist es aber, Stimmung gegen eine Unterstützung der Ukraine zu machen.

18K **36K** **41K** **86K**

23_Fake

TILL LINDEMANN

«EUROPA WIRD ZERSTÖRT. DIE FOLGEN DER SINNLOSEN HILFE FÜR DIE UKRAINE»

15K **27K** **39K** **82K**

23_Fake · 1h

Scarlett Johansson

All countries start thinking about themselves, and the EU is falling apart.

Desinformation erkennen

Viele Menschen tragen zur Verbreitung von russischen Falschnachrichten bei, weil sie diese ungeprüft über ihre Social-Media-Accounts teilen. Deshalb ist es wichtig, Falschinformationen zu erkennen und nicht weiterzuverbreiten. Fünf Tipps der Bundesregierung:

- 1**

Textzusammenhang
Stimmen die Überschrift und die eigentliche Meldung überein? Ist der gesamte Text sinnvoll und widerspruchsfrei?
- 2**

Fakten
Passt die Darstellung mit den bekannten und belegbaren Fakten zusammen? Sind die Quellen nachvollziehbar und überprüfbar?
- 3**

Urheberschaft
Wer ist der ursprüngliche Verbreiter der Nachricht? Ist dieser seriös und glaubwürdig? Was veröffentlicht die Person oder Institution sonst noch?
- 4**

Andere Quellen
Können die dargelegten Informationen in anderen Quellen und Medien nachvollzogen werden? Stimmen die Fakten überein?
- 5**

Bilder
Was ergibt die Rückwärts-suche der veröffentlichten Bilder im Internet? Erscheint ein Bild immer im gleichen Zusammenhang?

Nein

Es könnte sich um Desinformation handeln. Verbreiten Sie die Nachricht nicht weiter!

Lifehacks für mehr Sicherheit

Gegen Sicherheitsbedrohungen bist du der allererste Schutzwall.

Hier sind sieben Tipps, um die Bundeswehr für dich und deine Kameradinnen und Kameraden noch sicherer zu machen.

TEXT Sebastian Blum

ILLUSTRATION Jindrich Novotny

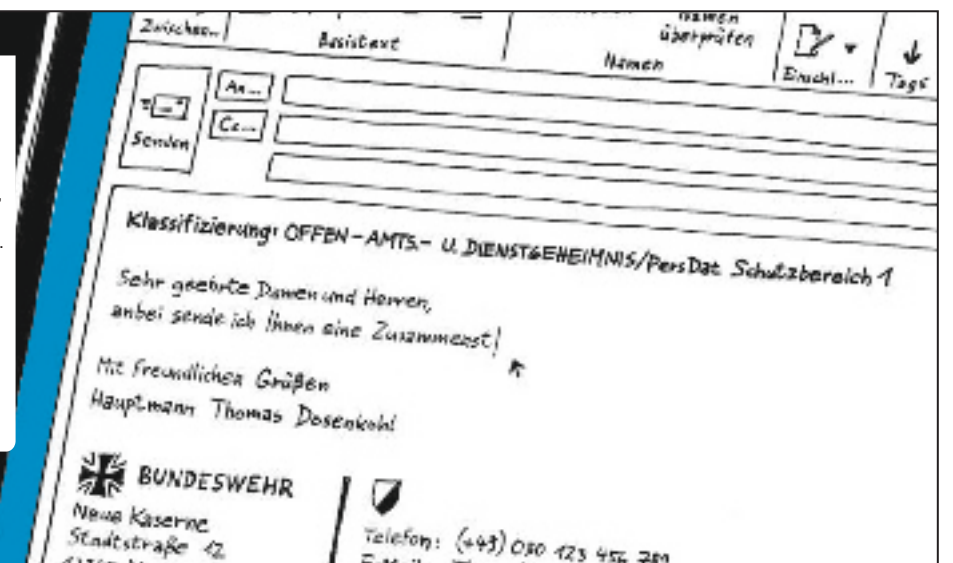
S. 59: 2 Agenten/Jindrich Novotny, Illustration (2)

TIPP 1 In der Öffentlichkeit: Nutze keine ungeschützten Internetverbindungen.

Um ihren mobilen Datenverbrauch zu schonen, nutzen viele öffentliche WLAN-Verbindungen. Aber Vorsicht: Deine Daten sind über offene oder öffentlich zugängliche WLAN-Hotspots nicht sicher und können leicht abgegriffen werden. Lässt es sich nicht vermeiden, einen Hotspot zu verwenden, solltest du die Datei- oder Verzeichnisfreigabe in den Einstellungen deines Endgeräts abschalten. Außerdem schützen VPN-Verbindungen vor ungewolltem Zugriff. Und schließlich solltest du offene WLAN-Zugänge nicht speichern, damit sich dein Gerät nicht ohne dein Wissen von alleine verbindet.



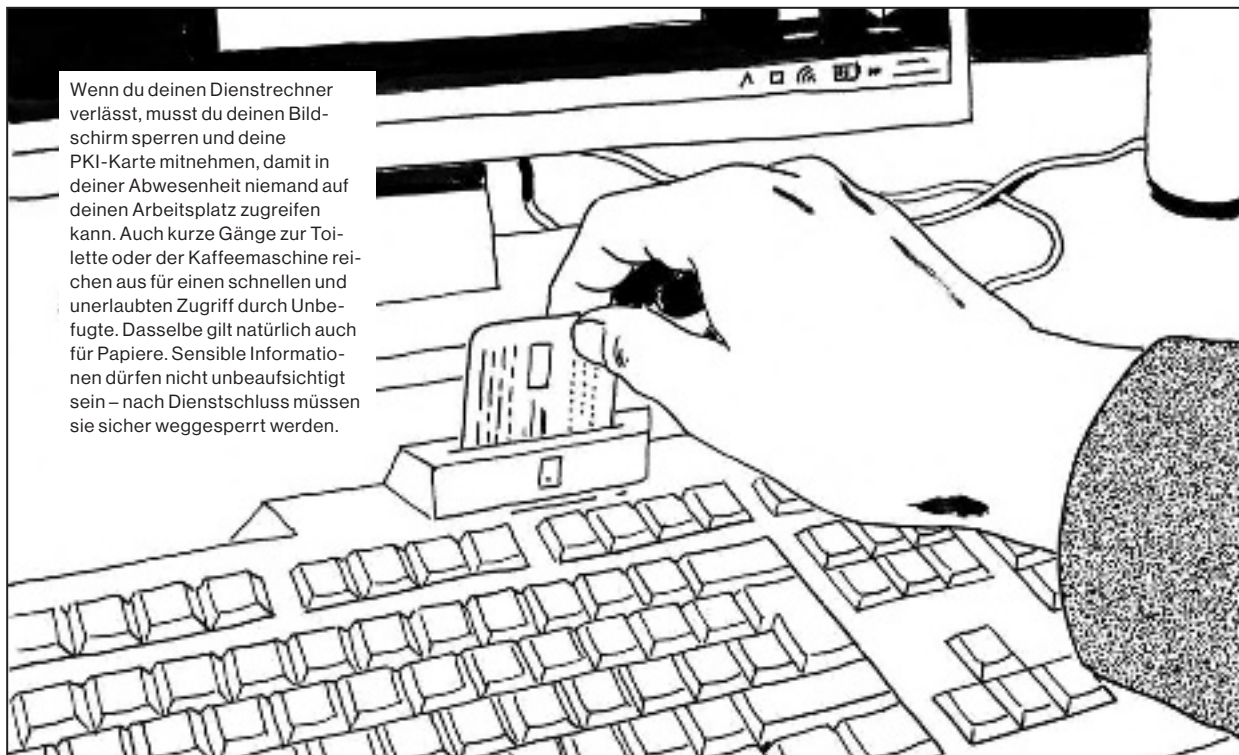
Die Verschlusssachenanweisung des Bundesinnenministeriums unterscheidet vier Stufen der Geheimhaltung für Informationen: 1. Streng geheim, 2. Geheim, 3. VS-Vertraulich und 4. VS-Nur für den Dienstgebrauch. Die richtige Klassifizierung sorgt dafür, dass Bundeswehrinterne geschützt sind und nicht in falsche Hände geraten – und bei der internen Kommunikation wissen alle Beteiligten, wer welche Information erhalten darf.



TIPP 2 Im Dienst: Denk daran, deine Dienstmails und Dokumente richtig zu klassifizieren.

TIPP 3 Am Arbeitsplatz: Sperre deinen Rechner, wenn du gehst.

Wenn du deinen Dienstrechner verlässt, musst du deinen Bildschirm sperren und deine PKI-Karte mitnehmen, damit in deiner Abwesenheit niemand auf deinen Arbeitsplatz zugreifen kann. Auch kurze Gänge zur Toilette oder der Kaffeemaschine reichen aus für einen schnellen und unerlaubten Zugriff durch Unbefugte. Dasselbe gilt natürlich auch für Papiere. Sensible Informationen dürfen nicht unbeaufsichtigt sein – nach Dienstschluss müssen sie sicher weggesperrt werden.



Jede Dienststelle in der Bundeswehr hat ihren eigenen Informationssicherheitsbeauftragten (ISB). Lerne deine Ansprechpartner oder -partnerinnen kennen und sprich sie bei Unklarheiten, Problemen oder Sicherheitsvorfällen sofort an. Denk immer daran: Fehler können jedem passieren. Wenn du dich frühzeitig meldest, lassen sie sich oft noch korrigieren.

TIPP 4 Im Dienst: Kenne deine Sicherheitsbeauftragten.

Auf dem Dienstrechner darf keine private Software installiert und keine private Hardware angeschlossen werden. Außerdem dürfen keine privaten Accounts wie Amazon, Instagram oder Ähnliches geöffnet werden. Das private Handy gehört stets ausgeschaltet und weggeschlossen. Denn verschiedene Apps stehen im Verdacht, die Umgebung des Handys heimlich auszuspionieren.



TIPP 5 Am Arbeitsplatz: Nutze keine private Soft- oder Hardware.

S. 60–61: 2 Agenten Jindrich Novotny, Illustration (5)

TIPP 6 In der Dienststelle: Melde Auffälligkeiten und unbekannte Menschen.



Hast du diesen Kollegen noch nie gesehen? Oder kommt dir etwas anderes komisch vor? Melde Auffälligkeiten und fremde Personen, damit diese nicht unbehelligt bleiben. Oft reicht auch schon eine kurze Frage, ob man weiterhelfen kann, um ungebetene Gäste abzuschrecken. Aber auch Kameraden oder Kameradinnen, die in der Kaserne etwas filmen oder fotografieren, was nicht an die Öffentlichkeit gehört, solltest du ansprechen und auf das hohe Schutzbedürfnis der Truppe aufmerksam machen.



Sei vorsichtig, mit wem du über deine Arbeit redest. Wirst du manchmal angesprochen und nach deiner Tätigkeit in der Bundeswehr befragt? Das kann gefährlich sein. Oft reichen kleine Informationssplitter, aus denen Spione ein größeres Gesamtbild zusammensetzen können. Welches unverfängliche Puzzleteil ihnen fehlt, kannst du nicht wissen. Achte auch auf ungebetene Zuhörer, wenn du dich mit einer Kameradin oder einem Kameraden außerhalb der Dienststelle unterhältst.

TIPP 7 In der Öffentlichkeit: Achte darauf, mit wem du sprichst.

3

Kapitel

Abwehr

Gefahr durch Spionage

Der Militärische Abschirmdienst der Bundeswehr schützt die Truppe und muss dabei vielen Bedrohungen begegnen – von Anbahnungsversuchen ausländischer Nachrichtendienste bis zum Selbstanbieter aus persönlichen Motiven.

TEXT Florian Stöhr
ILLUSTRATION Marje Saathoff

Es fing ganz harmlos an. Oberstleutnant Ralph G. besuchte im Februar 2014 den Ball der Luftwaffe in Bonn. Der Reserveoffizier aus Erkrath arbeitete damals für eine US-amerikanische Firma in Deutschland und übte häufig im Landeskommando Nordrhein-Westfalen. Fast 2.000 Gäste waren an diesem Abend in der altherwürdigen Beethovenhalle, in der früher die Bundespräsidenten gewählt wurden. In feiner Garderobe tanzten sie zu Livemusik, trafen alte Freunde und knüpften neue Kontakte. Unter den Gästen war auch Michail Starow, Russlands Luftwaffenattaché in Berlin. Veranstaltungen wie diese waren für ihn von unschätzbarem Wert. Denn seine Funktion in der Botschaft war nur eine Tarnung, in Wirklichkeit war er Offizier des GRU, Russlands Militärgeheimdienst. Starow sprach Ralph G. an, man kam ins Gespräch. Der Deutsche fühlte sich geschmeichelt, die beiden verabredeten, in Kontakt zu bleiben. Der Anfang einer Beziehung, die schwere Folgen haben sollte.

„Das war eine klassische nachrichtendienstliche Anbahnung“, sagt Major Thorsten Ahrweil* von der Spionageabwehr des MAD, dem Militärischen Abschirmdienst der Bundeswehr. „Öffentliche Veranstaltungen eignen sich sehr gut, um Informationen zu sammeln. Meist bleibt es bei einem einmaligen Ausfragen.“ Im Fall von Ralph G. wurde aus der unauffälligen Gesprächsabschöpfung die gezielte Rekrutierung eines Agenten für den GRU. Was danach folgte, war wie aus dem Lehrbuch: Michail Starow baute ein Vertrauensverhältnis zu Ralph G. auf, das mehrere Jahre andauerte. Er besuchte den Reservisten in Erkrath und lud ihn nach Berlin ein. Gemeinsame Essen, die Ehefrauen lernten sich kennen, dann folgten Einladungen zu exklusiven Reisen nach Russland. Ob Ralph G. von Beginn an wusste, was sein russischer Freund damit bezweckte? Oder war es das eigene Geltungsbedürfnis? In den Medien wurden immer mehr Details bekannt und diskutiert. Als das Oberlandesgericht Düsseldorf im November 2022 sein Urteil sprach, stand fest, dass sich Ralph G. der Spionage schuldig gemacht hatte. Denn er hatte Starow wertvolle Informationen aus dem Innenleben der Bundeswehr geliefert. „Wir gehen davon aus, dass er aus Überzeugung handelte“, sagt Ahrweil. „Ralph G. war sehr russlandfreundlich. Er wollte dem Geheimdienstoffizier gefallen – zum Schaden der Bundeswehr.“ ➤

*Alle Namen zum Schutz der Soldaten geändert.



Anbahnung Oberstleutnant Ralph G. wird beim Ball der Luftwaffe vom russischen Luftwaffenattaché Michail Starow angesprochen. Dabei wird es nicht bleiben, sie vereinbaren, in Kontakt zu bleiben.

Rekrutierung Auf gemeinsame Essen und Besuche folgen Einladungen nach Moskau. Ralph G. wird gezielt umworben, damit er dienstliche Informationen an die russische Botschaft weitergibt.

Spionage In den Medien war zu lesen, dass der Oberstleutnant unter anderem Arbeitsstände wichtiger Dokumente der Bundeswehr weitergegeben haben soll. 2022 wird er vor Gericht verurteilt.





Selbstanbieter Thomas H. arbeitet 2023 beim Beschaffungsamt der Bundeswehr. Er nutzt seine Position, um Informationen von seinem Dienstrechner herunterzuladen. Die Ermittler gehen von persönlichem Frust aus.



Enttarnt Der Hauptmann speicherte dienstliche Daten auf einer CD, die er beim russischen Generalkonsulat in Bonn einwarf. Nur wenige Monate später wird er von den Behörden gefasst.

S. 66–67, Marje Saathoff, Illustration (3)

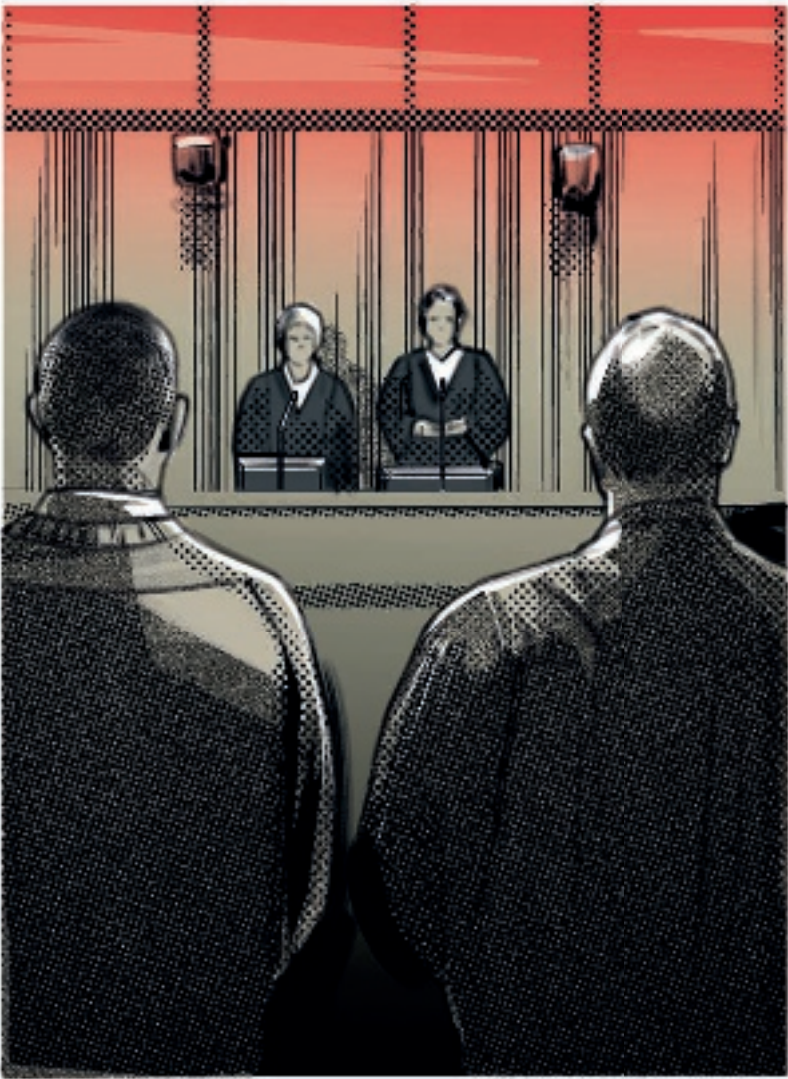
Schuldspruch Thomas H. wird im Mai 2024 für seine Spionagetätigkeit verurteilt. In der Bundeswehr ist er da schon lange nicht mehr. Der frühere Hauptmann muss für drei Jahre und sechs Monate ins Gefängnis.

Der MAD ermittelt

Der MAD wurde über eine Meldung aus der Truppe auf ihn aufmerksam und fing an zu ermitteln. Die Spionageabwehr war alarmiert. „Unsere Aufgabe ist es, Agentinnen und Agenten ausländischer Geheimdienste in der Bundeswehr zu identifizieren und abzuwehren“, erklärt Major Ahrweil. Dafür wertet der MAD alle Informationen aus, die er gewinnen kann. Neben eigenen Ermittlungen werden Erkenntnisse anderer inländischer Dienste wie dem Verfassungsschutz sowie ausländischer Partner eingeholt. „Wir können bei einem ausreichenden Verdacht und nach unabhängiger juristischer Mitprüfung eine Person beobachten, ihre Telefonate mithören und Briefe lesen“, erklärt Ahrweil. Ralph G. war auffallend häufig in Russland. Der MAD kam zu eindeutigen Erkenntnissen: Der Reserveoffizier hatte interne Informationen weitergegeben. In den Medien hieß es, dass es sich um Dokumente zum Reservistenwesen, zur Cyberabwehr und zur Zivil-Militärischen Zusammenarbeit der Bundeswehr gehandelt haben soll. Nicht alles davon sei eingestuft gewesen, manches aber schon, wie frühe Arbeitsstände des Weißbuchs zur Sicherheitspolitik oder zur Strategie der Reserve. Als der russische Geheimdienstoffizier Starow Deutschland 2017 verließ, habe der Reservist seine Dienste dessen Nachfolgern angeboten.

„Wir haben unsere Erkenntnisse dem Generalbundesanwalt übergeben. Das Bundeskriminalamt nahm Ralph G. schließlich fest“, sagt der Major. Das Oberlandesgericht Düsseldorf folgte der Anklage und sprach eine Bewährungsstrafe von einem Jahr und neun Monaten aus. Der ehemalige Reservist kam glimpflich davon. „Wenn man überführt wird, heißt das oft Gefängnis“, erklärt der Experte vom MAD. So wie im Fall von Thomas H., der im August 2023 festgenommen wurde. Der Hauptmann arbeitete im Beschaffungsamt der Bundeswehr (BAAINBw) in einer Einheit, die sich mit Mitteln der elektronischen Kampfführung beschäftigt. Wenige Monate vor sei-

ABWEHR



„Ralph G. war sehr russland-freundlich. Er wollte dem Geheimdienstoffizier gefallen.“

Major Thorsten Ahrweil, Spionageabwehr MAD

ner Festnahme hatte er sich an russische Stellen gewandt. Dem russischen Generalkonsulat in Bonn übergab der Berufsoffizier eine CD mit Daten, die er von seinem Dienstrechner heruntergeladen hatte. Zwei Fälle, zwei unterschiedliche Motive: „Thomas H. wurde nicht rekrutiert, sondern war ein Selbstanbieter. Nach unseren Ermittlungen war es bei ihm ein Motivationsmix aus privatem, beruflichem und politischem Frust“, so Ahrweil. Auch hier arbeitete der MAD eng mit den anderen Sicherheitsbehörden zusammen. Im Mai 2024 folgte das Urteil des Oberlandesgerichts Düsseldorf: drei Jahre und sechs Monate Gefängnis. ➤

„Unsere Aufgabe ist es, Agentinnen und Agenten zu identifizieren und abzuwehren.“

Major Thorsten Ahrweil, Spionageabwehr MAD

Nachrichtengewinnung
Der MAD kann unter anderem die Kommunikationsgeräte eines Verdächtigen abhören. Neben eigenen Ermittlungen werden auch Erkenntnisse anderer Dienste ausgewertet.



Lagebild

Recherchen, Ermittlungen und Fallanalysen – in der Zentrale des MAD in Köln laufen alle Fäden zusammen. Der Nachrichtendienst der Bundeswehr registriert aktuell vielfach Spionageversuche aus Russland und China.

Spionage hat viele Gesichter

Die deutschen Geheimdienste beobachten erhebliche Spionagetätigkeiten Russlands. Mit dem Angriffskrieg auf die Ukraine ist die Zahl seit Februar 2022 noch weiter gestiegen. Als zweitgrößter Unterstützer der Ukraine nach den USA steht Deutschland besonders im Fokus. Immer wieder versuchen russische Geheimdienste wie der GRU oder der SVR, der Auslandsgeheimdienst, die Bundeswehr aufzuklären. Das Spektrum geht über die Anbahnung bei öffentlichen Veranstaltungen und Selbstanbieter hinaus. Angehörige der Bundeswehr und anderer staatlicher Institutionen wer-

den ausspioniert oder auf Social Media angeschrieben. Wer sich nicht freiwillig bereit erklärt, kann unter Druck gesetzt werden, warnt der MAD. Besonders wenn man eine Schwäche hat, die sich ausnutzen lässt. Alkoholismus, Spielsucht, Schulden oder Affären – Zielpersonen, die erpressbar sind, sind schneller zu Gegenleistungen bereit. Ein Kompromat, wie es früher beim KGB hieß. Der Vorgänger der heutigen russischen Dienste war dafür berüchtigt, kompromittierende Lagen gezielt herbeizuführen. „Gefährdet sind auch Bundeswehrangehörige mit russischen Wurzeln“,

S. 68–69: Marie Saathoff, Illustration (2)

erklärt Oberst Marcus Deckert. Auch Deckert arbeitet bei der Spionageabwehr des MAD. Wie sein Kollege möchte er über seine Identität nicht mehr verraten. Die beiden Offiziere bleiben lieber im Hintergrund. Wer Familienangehörige in Russland hat und diese besucht, muss damit rechnen, bei der Einreise von den Grenzbehörden befragt zu werden. „Russlands Inlandsgeheimdienst FSB erfährt von der Einreise über den Visumsantrag. Dort muss man angeben, wo man arbeitet“, sagt der Oberst. Spätestens dann wird man als Bundeswehrangehöriger erkannt. Wer eine

deutsche und eine russische Staatsbürgerschaft hat, läuft sogar Gefahr, zum Militärdienst eingezogen zu werden. „Wir raten deshalb dringend von Reisen nach Russland ab. Auf jeden Fall sind uns die Reisen und alle Auffälligkeiten zu melden“, so der MAD-Mann. Warum interessieren sich russische Dienste für Bundeswehrangehörige, selbst wenn diese gar keinen Zugang zu geheimen Informationen haben? „Weil jeder Lagesplitter über das innere Gefüge der Truppe relevant ist. Die vielen kleinen Informationen verdichten sich zu einem Gesamtbild über uns“, sagt Deckert. ➤

Mit 360-Grad-Blick

Der MAD beobachtet neben russischen auch vermehrt chinesische Spionageaktivitäten. Die Vorgehensweisen unterscheiden sich: Chinas Geheimdienste nutzen zum Ausspähen oft die immer größere Menge an technischen Geräten in Deutschland. Erstansprachen zur Rekrutierung von Agentinnen und Agenten erfolgen meist über Social Media. Bundeswehrangehörige werden auch per E-Mail angeschrieben und mit Geldangeboten für Fachaufsätze und Vorträge geködert. „Russland ist der Sturm, China der Klimawandel“, hatte der ehemalige Präsident des Bundesverfassungsschutzes Thomas Haldenwang im Oktober 2022 bei einer Anhörung der deutschen Geheimdienste im Bundestag gesagt. China wird die Dienste künftig noch stärker beschäftigen. „Unsere Lagebilder sind sehr hoch eingestuft und nicht für die Öffentlichkeit bestimmt“, erklärt Oberst Deckert. „Aber man kann sagen, dass wir einen 360-Grad-Blick haben und sehr deutlich aufzeigen, was wir sehen.“ Man muss seine Gegner kennen – jetzt und in Zukunft.

„Unsere Lagebilder sind sehr hoch eingestuft und nicht für die Öffentlichkeit bestimmt.“

Oberst Marcus Deckert
Spionageabwehr MAD



ABWEHR

Verdeckte Ermittlungen

Die Bundeswehr steht im Fokus ausländischer Dienste. Zu ihrem Schutz kann der MAD Verdächtige beobachten. Alle Informationen werden zu einem großen Lagebild verdichtet.

Noch aber hat Russland Priorität. Infolge des Kriegs in der Ukraine hat Deutschland rund 70 russische Botschaftsangehörige zur Persona non grata erklärt. Sie wurden der Spionage beschuldigt und mussten das Land verlassen. „Das hat den russischen Diensten sehr wehgetan. Aber wir gehen davon aus, dass sie ihre Kräfte wieder ersetzen und ihre Methodik anpassen“, sagt Deckert. Geheimdienste nutzen in der Regel eine Toolbox. Wenn es hauptamtliche Spioninnen und Spione schwerer haben, verlagert sich der Fokus auf den Cyberbereich oder auf die Anheuerung informeller Kräfte. Die russischen Dienste setzen deshalb auch auf sogenannte Einwegspione. „Einweg- oder Wegwerfagenten sind kurzfristig angeworbene Kräfte, die einen einmaligen Auftrag ausführen. Oft sind es Kleinkriminelle, die über Mittelsmänner bezahlt werden“, erklärt Oberst Deckert. Der Vorteil liegt auf der Hand: Sie müssen nicht aufwendig rekrutiert und geführt werden, sondern sind schnell einsatzbereit. Die Drahtzieher bleiben derweil im Verborgenen.

Zahlreiche Fälle von Sabotage

Bayreuth, August 2024: Spezialkräfte der Polizei nehmen zwei mutmaßliche Spione fest, die im Auftrag Russlands militärische Liegenschaften und Transportwege ausgespäht haben. Der Verdacht des Generalbundesanwalts: Die beiden Männer mit deutschem und russischem Pass sollen Brand- und Sprengstoffanschläge auf die deutsche Ukrainehilfe geplant haben.

Warschau, März 2023: Polnische Behörden decken einen russischen Spionagering auf. Mehrere ausländische Personen werden festgenommen. Sie werden verdächtigt, Bahnstrecken mit Wildkameras überwacht und Sabotageakte geplant zu haben. Polen ist Dreh- und Angelpunkt für die Versorgung der Ukraine mit Militärgütern. Würden die Transportwege gestört, wäre die Unterstützung nicht mehr gesichert.

London, Februar 2023: Britische Behörden nehmen drei Bulgaren fest, die für Russland spioniert haben sollen. Sie waren im Besitz zahlreicher gefälschter Ausweise unter anderem für Großbritannien, Frankreich, Kroatien, Tschechien und Slowenien.

Die Liste der Vorfälle ist lang und nicht immer können die Sicherheitsbehörden eine Tat im Vorfeld verhindern. 2014 zerstörten zwei Explosionen das Munitionslager Vrbětice im Osten Tschechiens, in dem Munition für die Ukraine hergestellt wurde. Zwei Menschen kamen dabei ums Leben. Die tschechischen Streitkräfte brauchten zwei Jahre, um alle Blindgänger zu entschärfen. Die Behörden sind sich sicher, dass es russische Agenten waren. Weil Russland jegliche Zusammenarbeit ablehnte, mussten die Ermittlungen 2024 letztlich eingestellt werden. „Hier geht es nicht um Informationsgewinnung. Russland versucht, uns und unsere Partner auch direkt zu sabotieren“, erklärt Major Ahrweil.

MAD mahnt zur Vorsicht

Für die Bundeswehr bedeutet das vor allem: wachsam sein. Der MAD rät dazu, ungewöhnliche Vorkommnisse unbedingt zu melden. „Alle Bundeswehrangehörigen sollten stets mit offenen Augen durch die Welt gehen. Wir wollen keine Ängste schüren, aber dafür sensibilisieren, dass jeder einen Beitrag leisten kann“, sagt Ahrweil. Spionageabwehr fängt mit Prävention an. Der MAD hat für jede Dienststelle der Bundeswehr das Risikopotenzial für fremde Geheimdienste bewertet. „Der beste Schutz ist, wenn wir Schwachstellen frühzeitig erkennen und abstellen“, so der MAD-Mann.

Ralph G. und Thomas H. mussten die Truppe verlassen. Sie haben schwere Straftaten begangen und mussten sich dafür vor Gericht verantworten. Soweit müsse es nicht kommen, weiß Ahrweil. Der MAD bietet Bundeswehrangehörigen an, sich auch dann zu melden, wenn sie schon nachrichtendienstlich verstrickt sind. „Es gibt immer die Option, auszusteigen – selbst dann, wenn man schon einen Fehler gemacht hat.“ Wer das nicht tut, der muss mit der Spionageabwehr rechnen. ●

SICHERES UMFELD

1
„EINE PERSON, DIE MIT EINER SICHERHEITSEMPFINDLICHEN TÄTIGKEIT BETRAUT WERDEN SOLL (...), IST VORHER EINER SICHERHEITSÜBERPRÜFUNG ZU UNTERZIEHEN.“
(Paragraph 2, Sicherheitsüberprüfungsgesetz)

Die **Sicherheitsüberprüfung** ist dafür da, die Bundeswehr und ihre Angehörigen zu schützen. Nur wer überprüft worden ist, erhält Zugang zu Waffen, Munition, geschützten Bereichen und vertraulichen Informationen. Y erklärt, wie die Sicherheitsüberprüfung funktioniert.

TEXT Florian Stöhr

2
WER WIRD ÜBERPRÜFT?
Durch die Sicherheitsüberprüfung, kurz SÜ, stellt die Bundeswehr wie andere Institutionen und Behörden fest, ob eine Person geeignet ist, eine sicherheitsempfindliche Tätigkeit auszuüben. Überprüft werden Personen, die (1) Zugang zu Verschlusssachen oder (2) zu Sabotageschutzbereichen haben, oder (3) ein Dienstverhältnis als Soldatin bzw. Soldat, Reservistin bzw. Reservist oder Freiwillig Wehrdienstleistende bzw. Wehrdienstleistender anstreben. Denn alle Personen, die eine Ausbildung an der Waffe erhalten, werden überprüft.



S. 72: Bundeswehr/Jana Neumann
S. 72-73: YCS Visual Lab, Infografik

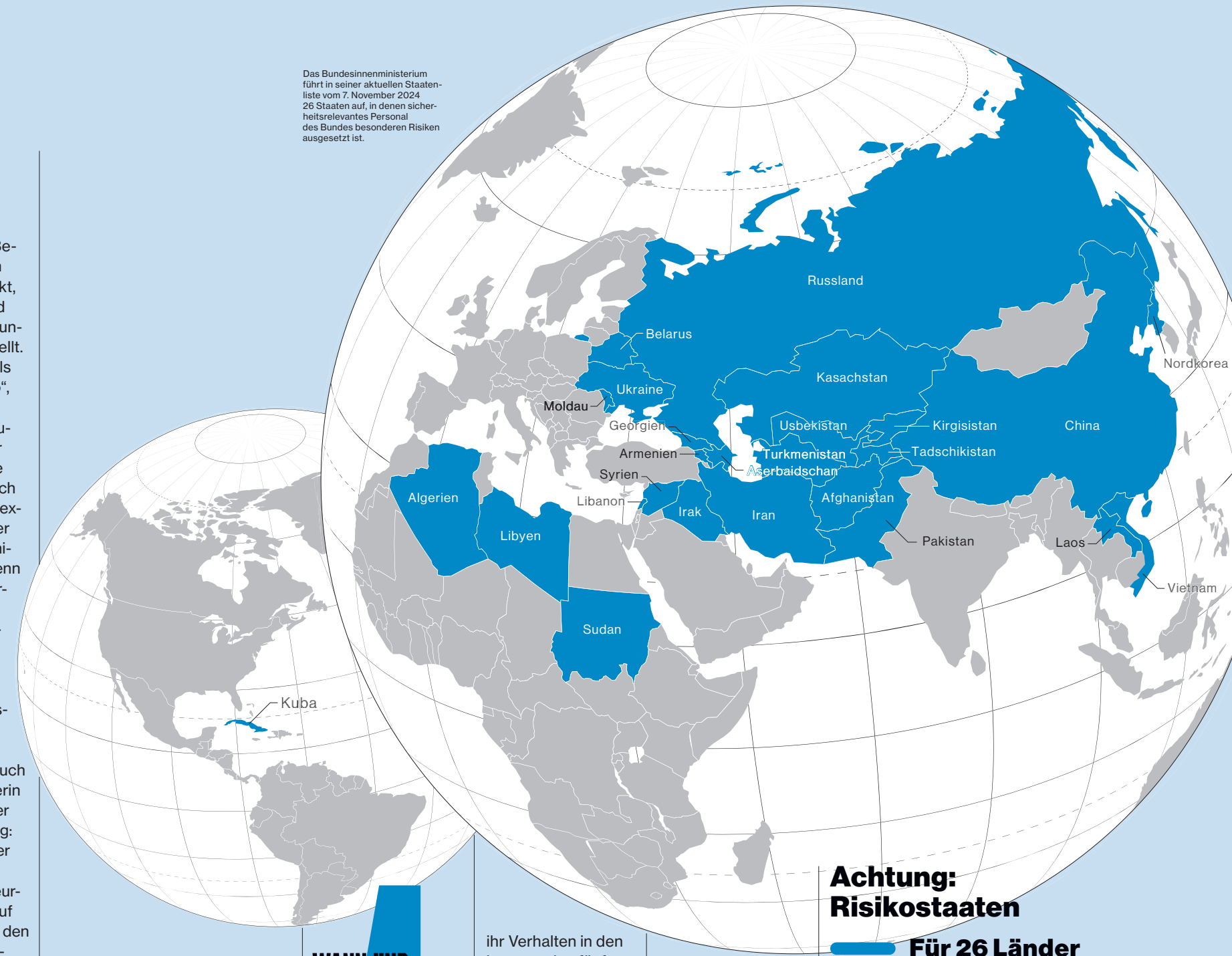
3
WAS WIRD ÜBERPRÜFT?
Die SÜ ist keine Bestrafung, sondern ein Verwaltungsakt, der Vertrauen und Integrität in der Bundeswehr sicherstellt. Eine Person gilt als „Sicherheitsrisiko“, wenn Zweifel bestehen an ihrer Zuverlässigkeit oder Verfassungstreue (zum Beispiel durch Verbindungen zu extremistischen oder kriminellen Vereinigungen). Oder wenn die Person gefährdet ist, aufgrund von Anbahnungs- und Werbungsversuchen durch ausländische Nachrichtendienste erpressbar zu sein. Ein Sicherheitsrisiko kann auch durch eine Partnerin oder einen Partner entstehen. Wichtig: Es entscheidet der Einzelfall und es kommt bei der Beurteilung nicht darauf an, ob die Person den Grund des Sicherheitsrisikos selbst verschuldet hat.

4
WANN UND WIE OFT FINDET DIE SÜ STATT?
Grundsätzlich werden Informationen über eine Person aus den vergangenen fünf Jahren ausgewertet, beispielsweise Auslandsreisen oder Anfragen an Polizei und Staatsanwaltschaften, um eine Prognose über

ihre Verhalten in den kommenden fünf Jahren abzugeben. Dementsprechend muss die SÜ alle fünf Jahre aktualisiert oder wiederholt werden. Die gesetzlichen Bestimmungen sind zuletzt mehrfach angepasst und verschärft worden, um die Bundeswehr insbesondere vor Extremismus in den eigenen Reihen zu schützen. Seit 2017 gibt es die Soldaten-

einstellungsüberprüfung, bei der alle Soldatinnen und Soldaten schon vor ihrem Dienstbeginn überprüft werden. Seit 2022 erfolgt die SÜ bei Soldatinnen und Soldaten mit besonders hohen Sicherheitsanforderungen, zum Beispiel Spezialeinheiten, noch intensiver und in kürzeren Abständen.

Achtung: Risikostaat
Für 26 Länder in der Welt gilt aufgrund ihrer Sicherheitslage und der Gefährdung durch fremde Nachrichtendienste eine Meldepflicht. Wer in diese Risikostaat reist, muss das in seiner Sicherheitserklärung angeben.



Das Bundesinnenministerium führt in seiner aktuellen Staatenliste vom 7. November 2024 26 Staaten auf, in denen sicherheitsrelevantes Personal des Bundes besonderen Risiken ausgesetzt ist.

5

WELCHE ARTEN DER SÜ GIBT ES?

Eine **Einfache Sicherheitsüberprüfung** erfolgt bei allen Bundeswehrangehörigen, die Zugang zu Informationen bis VS-VERTRAULICH erhalten, bei der Einstellung als Soldatin oder Soldat sowie bei Reservisten. Der MAD überprüft die Angaben in der Sicherheitserklärung und holt auch Auskünfte aus dem Bundeszentralregister ein.

Die **Erweiterte Sicherheitsüberprüfung VS-Schutz** wird durchgeführt bei Zugang zu Informationen, die als GEHEIM eingestuft sind. Gleiches gilt auch für den Zugang zu einer hohen Anzahl von VS-VERTRAULICH-Informationen. Über die Maßnahmen der Ü1 hinaus wird die Polizei an den Wohnorten angefragt und die Partner werden einbezogen.

Die **Erweiterte Sicherheitsüberprüfung Sabotageschutz** zielt auf Bundeswehrangehörige sowie externe Dienstleister ab, die Zugang zu besonders sicherheitsempfindlichen und sabotageanfalligen Einrichtungen der Truppe haben. Im Unterschied zur Ü2 VS wird nur die betroffene Person überprüft.

Die **Erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen** erfolgt bei Zugang zu STRENG GEHEIMEN Informationen oder zu einer hohen Zahl von GEHEIMEN Verschlusssachen. Über die Maßnahmen der Ü2 hinaus werden auch Personen aus dem persönlichen Umfeld befragt.

6

WELCHE STUFEN DER GEHEIMHALTUNG GIBT ES?

STRENG GEHEIM

Die Kenntnisnahme durch Unbefugte kann den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden.

GEHEIM

Die Kenntnisnahme durch Unbefugte kann die Sicherheit Deutschlands gefährden oder ihren Interessen schweren Schaden zufügen.

VS-VERTRAULICH

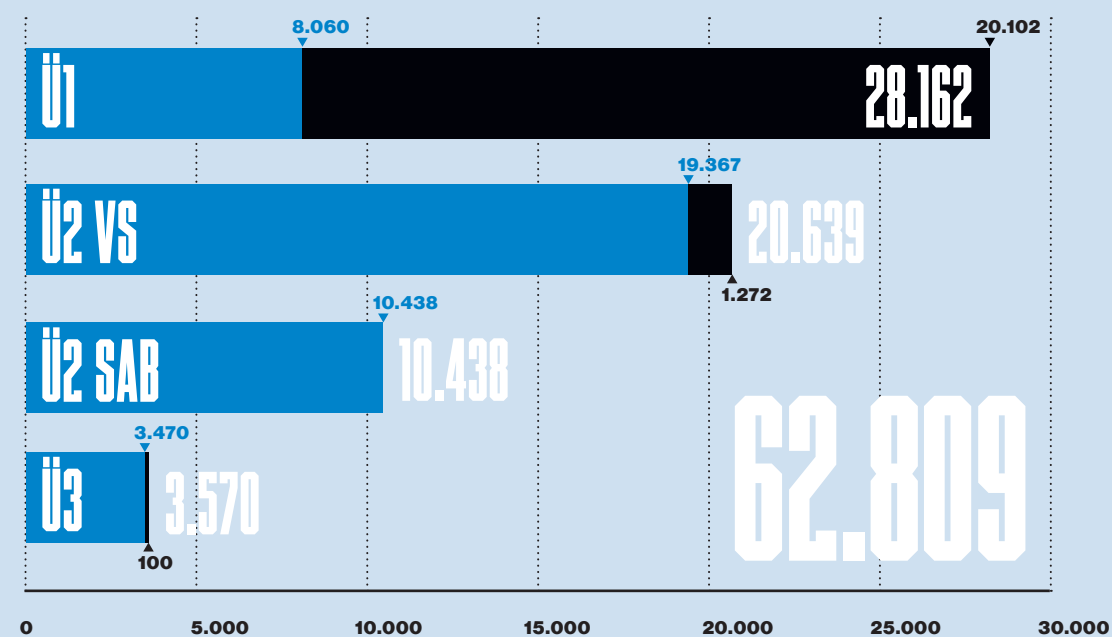
Die Kenntnisnahme durch Unbefugte kann für die Interessen Deutschlands schädlich sein. VS steht für Verschlusssachen.

VS-NUR FÜR DEN DIENSTGEBRAUCH

Die Kenntnisnahme durch Unbefugte kann für Deutschland nachteilig sein.

Beauftragte Sicherheitsüberprüfungen

2023 gab es in der Bundeswehr 62.809 Sicherheitsüberprüfungen. Durch verschärfte gesetzliche Regelungen stieg die Zahl zuletzt immer weiter an.



7

WAS PASSIERT MIT RESERVISTENDIENSTLEISTENDEN?

Auch Reservistinnen und Reservisten benötigen eine SÜ. Wie Soldatinnen und Soldaten können sie nur nach einer abgeschlossenen SÜ eine sicherheitsempfindliche Tätigkeit ausführen,

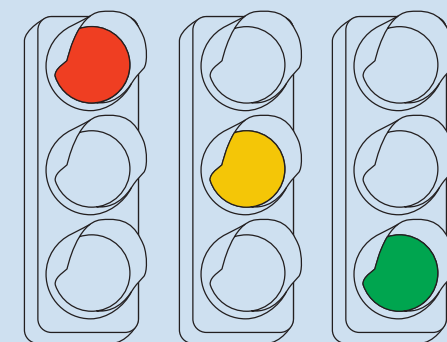
also Zugang zu Waffen, geschützten Bereichen oder vertraulichen Informationen erhalten. Wird bei ihnen eine Neigung zu Gewalt, Extremismus oder Terrorismus ermittelt, werden sie nicht herangezogen und damit auch nicht an der Waffe aus- und weitergebildet. Wer eine Reservistendienstleistung anstrebt und zuvor nicht in der Bundeswehr gedient hat, unterliegt den Vorgaben der Soldateneinstellungsüberprüfung.

S. 74–75: Y/C3 Visual Lab, Infografik
S. 75: Y/C3 Visual Lab, Illustration

8

WIE LÄUFT DIE SÜ AB?

Die rund 1.500 Sicherheitsbeauftragten in den Dienststellen und Karrierecentern der Bundeswehr beauftragen den Militärischen Abschirmdienst (MAD) damit, die SÜ durchzuführen. Im ersten Schritt sind die Bundeswehrangehörigen gefragt:



Sicherheitsrisiken sind erkannt worden. Die Person darf keine sicherheitsrelevante Funktion übernehmen.

Erkenntnisse unterhalb der Schwelle eines Sicherheitsrisikos können Auflagen während der Tätigkeit nach sich ziehen.

Keine Einschränkungen – die Person ist für eine sicherheitsempfindliche Arbeit in der Bundeswehr geeignet.

Sie müssen eine Elektronische Sicherheitserklärung (ELSE) ausfüllen. Die Angaben zur Person und zum privaten Umfeld werden vertraulich behandelt. Der zuständige Sicherheitsbeauftragte überprüft den Datensatz danach auf Vollständigkeit und formale Richtigkeit. Schritt drei ist die eigentliche Prüfung durch den MAD: Die Ermittlungen können je nach Tiefe mehr als 15 Maßnahmen umfassen – von der einfachen Prüfung der angegebenen Daten bis zur Befragung des persönlichen Umfelds. Die Ergebnisse, die der MAD dokumentiert und an den Sicherheitsbeauftragten übermittelt, lassen sich vereinfacht mit einem Ampelsystem vergleichen. Über Auflagen oder andere Maßnahmen entscheiden die Geheimschutzbeauftragten der Bundeswehr.

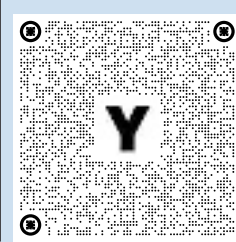
9

WAS MUSST DU TUN?

Die SÜ darf nur mit deiner Zustimmung erfolgen. Deine Aufgabe ist vor allem, die Elektronische Sicherheitserklärung korrekt und wahrheitsgemäß auszufüllen und für Nachfragen bereitzustehen. Hast du alles genannt? Sind deine

SÜ und ELSE erklärt

In einem Video werden alle wesentlichen Informationen kurz und knapp zusammengefasst:



Angaben sinnvoll und logisch? Wenn du dir nicht sicher bist, sprich mit deinem Sicherheitsbeauftragten. Das Programm ELSE findest du auf bundeswehr.de. Viele vergleichen die Menüführung und den Fragebogen mit dem Steuererklärungsprogramm Elster. Den fertigen Datensatz musst du ausdrucken, unterzeichnen und deinem Sicherheitsbeauftragten übergeben. ELSE soll voraussichtlich Mitte 2025 abgelöst werden. Dann sollen alle Schritte der SÜ komplett digital und papierlos erfolgen. Der Prozess wird dadurch einfacher und schneller.

10

WIESO DAUERT DIE SÜ SO LANGE?

Mehrere Hundert Menschen prüfen die Sicherheitserklärungen aller Bundeswehrangehörigen in Uniform und Zivil. Sie stellen Nachforschungen an und führen, wenn nötig, Befragungen durch.

Priorität haben die Soldateneinstellungsüberprüfungen: Sie startet in der Regel drei Monate, bevor Rekrutinnen und Rekruten ihren Dienst antreten, und soll bis zur fünften Woche der Grundausbildung abgeschlossen sein – denn dann beginnt die Schießausbildung. Andere Prüfungen, vor allem die Wiederholungsprüfung, dauern deshalb oft länger. Verzögerungen im Prozess treten zudem meistens auf, wenn Sicherheitserklärungen unvollständig sind und zurückgeschickt werden müssen oder wenn Erkenntnisse weitere Ermittlungen nach sich ziehen. Ein mögliches anschließendes Erörterungsverfahren zwischen Sicherheitsbeauftragten, MAD und Geheimschutzbeauftragten nimmt ebenfalls Zeit in Anspruch. Für die meisten bereits sicherheitsüberprüften Personen ergeben sich während des Prozesses aber keine Auswirkungen. Sie können während der SÜ ihrer Tätigkeit wie gewohnt nachgehen – und werden dies in den allermeisten Fällen auch danach weiterhin tun.



TEXT Florian Stöhr

Vorsprung durch Wissen

Wer den Gegner im Blick hat und viel über ihn weiß, kann vorausschauend handeln, statt nur reagieren.

Die notwendigen Informationen besitzt in der Bundeswehr das Militärische Nachrichtenwesen. Auch Verbündete profitieren davon.

Aufklärung

Satellitenaufnahmen vom 10. Februar 2022 zeigen russische Truppenbewegungen in Belarus. Der Luftwaffenstützpunkt Zyabrovka liegt südlich der Stadt Gomel – und weniger als 25 Kilometer entfernt von der Grenze zur Ukraine.

S. 76: Picture Alliance/Associated Press/Satellite
Image © 2022 Maxar Technologies
S. 77: Picture Alliance/dpa/TASS/Alexei Kononov (o);
Picture Alliance/dpa/TASS/Vitaly Nevar (u)



Getarnt als Übung

Die Truppenbewegungen an der Grenze zur Ukraine wurden als gemeinsames Manöver Russlands und Belarus begründet. In Wirklichkeit war es eine Mobilmachung russischer Streitkräfte für eine Vollinvasion des Nachbarlands. Der völkerrechtswidrige Angriff begann am 24. Februar 2022 und hält bis heute an.





Luftüberwachung

Die NATO veröffentlicht im Februar 2024 Bilder von russischen Militärflugzeugen, die über der Ostsee aufgeklärt wurden, darunter diese beiden Kampffjets SU-30M (im Hintergrund: eine französische Mirage 2000-5). Die Zahl russischer Überflüge am NATO-Grenzgebiet, hier im internationalen Luftraum nördlich von Polen, hat deutlich zugenommen.



Bedrohung der NATO

Die angrenzenden NATO-Staaten sorgen sich über russische Flottenbewegungen im Schwarzen Meer und in der Ostsee. Übungen der russischen Marine, wie hier im Februar 2022 vor der Halbinsel Krim, werden als Bedrohung wahrgenommen.

R

Rukla, Litauen: Der deutsche Kommandeur der Multinational Battle-group erhält täglich Informationen über die Sicherheitslage seiner Truppen. Was macht Russland? Worauf müssen sich die rund 1.000 Bundeswehrkräfte und ihre Partner bei der NATO-Mission einstellen? Gibt es Erkenntnisse über russische Truppenbewegungen, hybride Bedrohungen oder andere Auffälligkeiten an der Grenze zu Litauen? Mit Fragen wie diesen beschäftigt sich das Militärische Nachrichtenwesen der Bundeswehr, kurz MilNW. Was ist das wahrscheinlichste und was das gefährlichste Szenario? Und was heißt das für die Bundeswehr? Nur mit einem guten Lagebild kann die Truppe ihren Auftrag erfüllen – und der militärische Führer in Litauen die richtigen Entscheidungen treffen.

„Das MilNW dokumentiert alle sicherheitsrelevanten Informationen für die Bundeswehr, von den Einsatzgebieten bis zur Kaserne in Deutschland“, sagt Oberstleutnant Daniel Kleinert* vom Joint Intelligence Center (JIC) im rheinländischen Grafschaft. Das JIC ist Dreh- und Angelpunkt des Militärischen Nachrichtenwesens. „Wir sammeln hier sämtliche Informationen, die wir aus unseren Quellen erhalten, und bereiten sie für den jeweiligen Bedarfsträger auf.“ In diesem Fall ist der Bedarfsträger der deutsche Kommandeur in Litauen, dessen Stab Berichte zur Sicherheitslage im Baltikum abfragt. Litauen liegt zwischen der russischen Exklave Kaliningrad und Russlands Verbündetem Belarus. 150 Kilometer südlich vom Standort

S. 78: Picture Alliance/Newscom (o.); Picture Alliance/dpa/TAASS (u.)
S. 79: CG Visual Lab, Infografik

*Alle Namen zum Schutz der Soldaten geändert.

ABWEHR

Der Suwalki-Korridor ist das Grenzgebiet zwischen den NATO-Staaten Polen und Litauen. Er gilt als gefährdet, da Russlands Exklave Kaliningrad und das Staatsgebiet des Verbündeten Belarus hier nur 65 Kilometer voneinander entfernt liegen. Für die NATO ist der Korridor der einzige Versorgungsweg über Land ins Baltikum.



„Wir dokumentieren alle sicherheitsrelevanten Informationen.“

Oberstleutnant Daniel Kleinert,
Joint Intelligence Center

der NATO-Battlegroup befindet sich der Suwalki-Korridor, wo Russland und Belarus nur 65 Kilometer voneinander entfernt sind. Bei einem Angriff könnten die baltischen Staaten vom übrigen NATO-Gebiet abgeschnitten werden. Was hier passiert, kann also schwerwiegende Folgen haben.

Viele Quellen herangezogen

Eine Organisation wie die Bundeswehr hat einen riesigen Informationsbedarf. Wie viele Anfragen das JIC pro Tag erhält, ist geheim. „Die Zahlen sind eingestuft, damit ein Geg-

ner keine Rückschlüsse auf unsere Arbeitsweise ziehen kann. Aber man kann sagen, dass es viele Anfragen sind“, erklärt Kleinert. Das MilNW ist in allen Bereichen und Truppenteilen fest verortet. Man spricht auch vom Führungsgrundgebiet 2, der Sammlung, Verarbeitung und Auswertung von Informationen. Zuständig dafür sind die Abteilungen S2, G2, A2, M2 oder J2 – je nach Teilstreitkraft und Hierarchieebene. Mehrere Hundert Soldatinnen und Soldaten auf allen Ebenen sammeln jeden Tag Daten über gegnerische Kräfte, Aktivitäten und Fähigkeiten.

„Wir greifen zur Erstellung der militärischen Nachrichtenlage auf viele Quellen zurück“, sagt Kleinert. Das Spektrum reicht von offen verfügbaren Quellen (Open Source Intelligence, OSINT), wie zum Beispiel Online- oder Zeitungsartikeln, bis hin zu Personen, die geheime Informationen des Gegners preisgeben (Human Intelligence, HUMINT). Genauso wichtig sind Aufklärungsergebnisse durch Satelliten- oder Luftbildaufnahmen (Imagery Intelligence, IMINT) oder aus abgefangener elektronischer Kommunikation (Signals Intelligence, SIGINT). ➤



Neues Waffensystem

Russland modernisiert sein Raketenarsenal. Zu den neuesten Entwicklungen gehört die Mittelstreckenrakete RS-26 „Oreschnik“, die auf der RS-24 „Jars“ (hier bei einem Test und unten bei einer Parade in Moskau) basiert. Von der „Oreschnik“ gibt es noch keine Bilder.

„Bei jeder Bedarfsanfrage prüfen wir zunächst, was wir dazu schon haben und welche Anfrage besonders wichtig ist“, sagt der Oberstleutnant. Das JIC koordiniert alle Anfragen und managt den weiteren Prozess. „Wenn wir feststellen, dass unsere Daten nicht ausreichen, beauftragen wir Einheiten damit, zusätzliche Aufklärung zu betreiben.“ Das können Satellitenaufnahmen, Luftbilder eines Aufklärungsflugs oder abgehörter Fernmeldeverkehr durch Kräfte der Elektronischen Kampfführung (EloKa) sein. Oder Daten der Bündnispartner: Das MiINW nutzt auch Aufklärungsergebnisse anderer NATO- und EU-Staaten.



Die Sicherheitslage der Bundeswehr hat sich verändert. Russlands Vollinvasion in die Ukraine im Februar 2022 hat die Landes- und Bündnisverteidigung wieder in den Fokus gerückt und damit auch die Frage, wie dessen Streitkräfte im Kampf vorgehen. Ein Beispiel: Im November 2024 beschoss Russland die ukrainische Stadt Dnipro mit einer neuen Mittelstreckenrakete vom Typ RS-26, besser bekannt als „Oreschnik“. Die Expertinnen und Experten beim MiINW beobachten die Entwicklung der Rakete schon länger – neu war ihr Einsatz unter Gefechtsbedingungen.

„Im JIC sammeln wir alle verfügbaren Informationen zur RS-26 und werten sie aus. Wir liefern nicht nur eine Gefahrenanalyse, sondern geben auch Handlungsempfehlungen“, erklärt Kleinert. Welche Auswirkung hat das Waffensystem für die eigenen Verfahren und Taktiken? Kann das deutsche Flugabwehrsystem Patriot die Mittelstreckenrakete erfolgreich bekämpfen? „Unsere Erkenntnisse dienen dazu, die Bundeswehr bestmöglich auf einen feindlichen Angriff einzustellen“, so der Oberstleutnant. Es geht darum, auf den Ernstfall vorbereitet zu sein, zu agieren, statt zu reagieren.

Die Analysen und Bewertungen des russischen Fähigkeitsprofils fließen auch in die Operationspläne der NATO ein. Das gilt auch für Aufklärungsergebnisse, die die Bundeswehr erzielt. Seit Längerem dokumentieren die Fachleute im MiINW erhöhte Aktivitäten der russischen Marine im Ostseeraum. Der Verdacht: Russland beobachtet gezielt die neuen NATO-Mitglieder Schweden und Finnland und klärt deren Militärpotenziale auf.

Frühwarnsystem der Truppe

Neben dem Schutz der NATO-Ostflanke hat das MiINW auch die Sicherheit der Bundeswehr in Deutschland im Blick. Die Nachrichtendienste warnen vor russischer Desinformation, Spionage und Sabotage. Im August 2024 wurden in Köln-Wahn, Geilenkirchen und Mechernich verdächtige Löcher in Kasernenzäunen entdeckt – immer in der Nähe der Trinkwasserversorgung. Die Polizei und der Staatsschutz ermittelten, die Feldjäger und der MAD unterstützten. Der Verdacht auf Sabotageakte ließ sich nicht erhärten. Vorfälle wie diese unterstreichen aber, dass die Bundeswehr auch im Inland Bedrohungen ausgesetzt ist. Eine enge Zusammenarbeit zwischen dem MiINW und den ▶

S.80: IMAGO/SNA (6), Imago Images/TAR-TASS/Stanislav Krasnikov (u.)
S.81: imageBROKER/Foran Bachmeier

Test und Warnung

Russland beschießt die Ukraine täglich mit Raketen. Darunter sind auch Neuentwicklungen wie die RS-26 „Oreschnik“. Moskau spricht von Tests unter Gefechtsbedingungen, zugleich sind sie als Drohung gegenüber den Unterstützerstaaten der Ukraine gemeint. Nach dem „Oreschnik“-Angriff im November 2024 berief die NATO eine Sondersitzung des NATO-Ukraine-Rats ein.





Informationen gewinnen

Das MilNW hat viele Gesichter. Für die Fernmelde- und elektronische Aufklärung nutzt sie etwa den Störpanzer Hummel.

Nah am Gegner

Die EloKa-Truppe versucht, die Kommunikation eines Gegners zu erfassen, um für das MilNW Informationen zu sammeln.



„Das MilNW ist ein Frühwarnsystem, um im Notfall schnell Alarm schlagen zu können.“

Oberstleutnant Marco Felten, Operatives Führungskommando

Sicherheitsbehörden ist daher unerlässlich. „Das MilNW ist dazu da, der militärischen Führung frühestmöglich relevante Informationen zu liefern, damit diese Entscheidungen treffen kann“, erklärt Oberstleutnant Marco Felten vom neu aufgestellten Operativen Führungskommando (OFK) der Bundeswehr. Bevor eine Operation geplant wird, braucht es gute Kenntnisse zur Bedrohungs- und Feindlage. „Rot bestimmt blau: Aus dem Handeln des Feindes leitet sich das eigene Verhalten ab. Deshalb kommt das MilNW in Besprechungen auch zuerst“, sagt Felten. Nur wer die Bedrohungs- und

Feindlage kennt, kann sich darauf strategisch, operativ und taktisch vorbereiten. Jede Information ist wichtig für das Gesamtbild. Ergänzt wird das bundeswehrinterne Netz durch das System MilNW. Es umfasst auch Schnittstellen zum MAD und BND sowie zur EU und NATO. Eine wichtige Rolle spielen zudem die Militärattachés, die regelmäßig aus ihren Ländern berichten.

„Das OFK nutzt die Informationen für die stetige Weiterentwicklung des Operationsplans Deutschland“, sagt Felten. Das Dokument regelt den militärischen Anteil bei der Gesamtverteidigung Deutschlands. „Der OPLAN DEU legt fest, wie wir Deutschland bei der Landes- und Bündnisverteidigung schützen und sichern wollen.“ Die Details sind geheim. Bekannt ist lediglich, dass die erste Fassung vom März 2024 mehrere Hundert Seiten hatte. „Das MilNW ist für uns auch ein Frühwarnsystem. Wir überwachen viele Indikatoren, um Krisen und Gefahren frühzeitig zu erkennen und im Notfall schnell Alarm schlagen zu können“, so der Oberstleutnant.

Felten arbeitet in der J2-Abteilung des OFK. Das Operative Führungskommando hat neben der zentralen und streitkräfteübergreifenden Operationsführung der Truppe auch weite Teile der Gesamtsteuerung des MilNW übernommen. Das JIC bleibt für die Koordination und Umsetzung verantwortlich. Am Aufgabenprofil wird sich aber nichts ändern. „MilNW bleibt eine Querschnittsaufgabe in der Bundeswehr, von der alle beteiligten Akteure profitieren sollen“, erklärt Felten. Alle geben ihre Erkenntnisse weiter und haben leichten Zugang zu den gemeinsamen Daten. Das Ergebnis ist ein detailliertes, streitkräftegemeinsames Lagebild oder spezielle Gefahrenanalysen wie für Litauen.

S. 82: Bundeswehr/Carl Schulze (2);
S. 83: Bundeswehr/Sherrita Kästner



Fernspäher

Sie gelten als Augen des Heeres und operieren tief hinter den feindlichen Linien. Ihre Beobachtungen fließen ebenfalls ins MilNW ein – denn jede Information über einen Gegner ist wichtig.

Geheime Kommunikationskanäle

Um auch Informationen austauschen zu können, die als „GEHEIM“ oder „NATO SECRET“ eingestuft sind, nutzen die Bundeswehrdienststellen für das MilNW „rote Netze“. Im Unterschied zum allgemeinen BWI-Netz, dem „schwarzen Netz“, funktionieren die nationalen sowie internationalen Netzwerke völlig autark und ohne Internetzugang. Die daran angeschlossenen „roten Rechner“ sehen aus wie normale Desktop-PCs. Sicherheitsvorkehrungen bei der Soft- und Hardware sorgen allerdings dafür, dass das MilNW nach außen größtmöglich geschützt ist. Wer einen Zugang

dazu hat, ist in der Regel Ü3 geprüft, die höchste Stufe der Sicherheitsüberprüfung in der Truppe. „Das alles dient dem Schutz des MilNW, unserer Quellen und Aufklärungsmethoden“, erklärt Oberstleutnant Kleinert.

Das Militärische Nachrichtenwesen ist nicht nur ein Netzwerk wichtiger Dienststellen, sondern auch ein großes Archiv. Eine Datenbank, die durch Bedarfsanfragen, Fachanalysen, Prognosen und ein weit verzweigtes Meldewesen in der Truppe täglich wächst. „Wir dokumentieren dadurch auch viele grundlegende Parameter eines Gegners, zum Beispiel die Ausbildung,

Ausrüstung und Einsatztaktiken seiner Truppen. Oft können wir Bedarfsanfragen bereits durch die Grundlagendaten im MilNW beantworten“, sagt Kleinert. Der Krieg in der Ukraine zeigt, dass sich das dortige Kampfgeschehen vor allem durch den umfassenden Einsatz von Drohnen erheblich gewandelt hat. „Wir müssen darauf vorbereitet sein, dass der Gegner seine Operationsführung ständig anpasst. Ziel ist es, dessen Optionen bereits im Vorfeld zu kennen“, so Kleinert. Das MilNW hat sich auf die neue Sicherheitslage der Bundeswehr eingestellt – von Deutschland bis nach Litauen. ●

Schon immer steht die Bundeswehr im Fadenkreuz feindlicher Kräfte. Um ihre Angehörigen für die Gefahren von Spionage, Sabotage und Co. zu sensibilisieren, hat die Truppe zahlreiche Plakate, Broschüren und Kampagnen herausgegeben. Y nimmt euch mit durch die Jahrzehnte.

TEXT Johannes Friedemann

Lieber Vetter!
Ihre Geburts- und Namenstags-
Karte haben Sie mündelhaft
in der Schublade, die Sie
mit der Tafel Schokolade
beschriftet haben. Bitte
sichergestellt und uns sehr
danke für die
Spende.

Geheimtinte

Doch Hans wusch über diesen Brief
eine Flüssigkeit mit leichtem Mief.
Wir trauen unsere Augen nicht:
Der Brief verändert sein Gesicht!

Denn zwischen der Verwandtenliebe
erkennt man Spionageriebe –
und zwar von vorne bis nach hinten.
Ein klarer Fall geheimer Tinten.

„Ich glaube, ich habe
vergessen, die Geheim-
karte abzuschließen!“

„Fehr schnell in die Kasse!“
Schnell bekommen wir die
gute Nacht Ruhe. Ich
kann das schon!“

Überfahrend
Schwarz, der Geheimkarte
nicht anständig in der Kasse.

Durch Nacht und Wind (ja nicht
ganz opferbringend) kreist
Boris auf dem Rad zur Kasse.

Der Fahrer wandert sich
über seine Geheimkarte,
ob „Nachtschlaf“ gelöst.

„Nebenbei war ich
in der Kasse.“

„Wenn alles nicht nötig
gewesen, ja, natürlich
würde man haben!“

Selbstverständlich ist die Geheimkarte
richtig verschlossen. Schwarz hat mit
seinem Rad ein Stück vom Haus.

Worte ist nicht nur die
Mutter der Perzelektion,
sondern vermittelt auch für
Geheimdienstarbeiten
Ruhe und Beuglichkeit.
Ständig muß die Sicherheits-
kugel eingeworfen sein
(„Habe ich auch abstrichlich
verschlossen!“) und automati-
sch auch im Geheimdienst
sein. Selbst wenn
etwas wegen Überwindung
oder Überforderung das Er-
innerungsvermögen oder
der klaren Verstand wahr-
scheinlich ausgeschaltet sind.

Wenn du weißt, wo diese Panzer-
einheit in Garnison ist, wieviel Kampf-
wagen sie zählt, wie die Einheitführer
heißen und welchen Dienstgrad sie be-
sitzen, so behalte diese Weisheit
für dich! Behandle alle Zahlen-, Orts-
und Namensangaben aus dem Bereich
der Bundeswehr als geheim, dann
kannst du keinen Schaden an-
richten! Der Wissende schweigt.

Nachschlagewerk
DIE SICHERHEITSFIBEL

Diese jungen Soldaten der deut-
schen Bundeswehr erwarten von dir,
daß du ihre Gesundheit und ihr Leben
nicht durch Geschwätz über militä-
rische Angelegenheiten gefährdest.
Sie vertrauen auch auf deine Ver-
schwiegenheit! Sicher willst du nicht
durch Verrat zu ihrem Mörder werden.



Spionage gibt es nicht erst,
seit Russland sich offen feind-
lich gegenüber den westlichen
Staaten positioniert oder China
seine Weltmachtstellung aus-
bauen will. Spione und Agen-
ten hat es immer gegeben. Als
Hochphase der Spionage gilt
der Kalte Krieg, die Konfronta-
tion zwischen den NATO-Staa-
ten und den Staaten des War-
schauer Pakts rund um die
Sowjetunion. Die Grenze dieses
Konflikts verlief durch Deutsch-

land – und die Bundeswehr war
dadurch mittendrin. Deswegen
wurde die Truppe schon damals
über die Gefahren aufgeklärt:
So gab das Amt für Sicherheit
der Bundeswehr (ASBw), wie
früher der Militärische Abschi-
rmdienst (MAD) hieß, in den 1960er-
Jahren die Sicherheitsfibel
heraus. Das kleine Buch machte
auf Spionage und den sorg-
samen Umgang mit Informati-
onen aufmerksam. Aufgeklärt
wurde über damals moderne
Abhörtechniken, aber auch
über Dinge, die heute wie aus
einem in die Jahre gekomme-
nen Agentenfilm anmuten – zum
Beispiel die Verwendung von
Geheimtinte und toten Brief-
kästen, also Verstecken für ge-
heime Botschaften. Die Autoren

setzten dabei weniger auf den
erhobenen Zeigefinger und
mehr auf originelle und humor-
volle Verse: „Ein heimlicher
Manövergast, der mit Bedacht
und ohne Hast der Truppe folgt
und interessiert, was man so
übt, ausspioniert (...)“. An an-
derer Stelle rufen die Autoren zur
sorgfältigen Vernichtung dienst-
licher Unterlagen auf: „Wenn
ein Papierwolf nicht zur Hand,
wird Überzähliges verbrannt, da
selbst die kleinsten Schrifttums-
fetzen Spione neu zusammen-
setzen.“ Wie erfolgreich wären
wohl heute Aufklärungskampa-
gnen in Versform?

S. 84–85: BAMAD (6)



1950er



1970er

Dienstvorschrift ZEHN GRUNDREGELN



OUTRO

Über Jahre hinweg war sie der Maßstab für Sicherheit in der Bundeswehr – die Zentrale Dienstvorschrift 2/30 aus dem Jahr 1971. Sie war die grundlegende Vorschrift für Militärische Sicherheit, Verschlussachen und die Sicherheitsüberprüfung im Geschäftsbereich des Vertei-

digungsministeriums. Sie existiert längst nicht mehr. Eigentlich schade, denn einige Inhalte würden heute durchaus für Erheiterung sorgen, zum Beispiel die „10 Grundregeln für die Militärische Sicherheit“. Auch wenn sie vom Inhalt her im Grunde immer noch aktuell sind, so wirkt

ihre Formulierung – freundlich ausgedrückt – ziemlich altbacken. Die zweite Grundregel lautet zum Beispiel: „Halte Maß! Denke daran, daß übermäßiger Alkoholgenuß den Menschen enthemmt. Bedenke, daß auch Frauen als Agenten eingesetzt werden. Sei Dir bewußt, daß der Gegner sich auch für Deine Schulden interessiert. Du mußt wissen, daß Fehlritte oft zur Nötigung ausgenutzt werden.“ Auch die fünfte Grundregel würde heute anders formuliert sein: „Sei hellhörig und kritisch! Rechne damit, daß der Gegner jede Möglichkeit zur Zersetzung ausnutzt. Hierzu bedient er sich aller publizistischen Mittel, des Briefes und des Gespräches. Traue nicht allem, was Du siehst, hörst oder liest. Die Verbreitung von Gerüchten hilft dem Gegner.“

S. 86–87: BAMAD (7)



1970er

1980er



1990er

Kampagnen MAD

Das Anliegen der Aufklärungskampagnen blieb über die Jahrzehnte unverändert: die Sensibilität der Truppe für Spionage, Sabotage und Zersetzung zu erhöhen. Was sich jedoch mit dem Zeitgeist änderte, waren die Darstellungsformen. An die Stelle bebildeter Verse traten Comics, später setzte der MAD bei der visuellen Gestaltung vermehrt auf Fotografien.

Plakat DER „SPI-SA-ZER“

Zur Sensibilisierung der Truppe wurden immer wieder Plakate verwendet. Eines der bekanntesten war seinerzeit das Plakat mit dem Spi-Sa-Zer-Motiv. Die Abkürzung steht für Spionage, Sabotage und Zersetzung. Das Plakat zeigt einen schwarz gekleideten und maskierten Mann mit Aktentasche. Eindeutig ein Spion! Auf die Frage „Kennst du schon den Spi-Sa-Zer?“ gibt das Plakat die Antwort in Gedichtform, wie rechts zu sehen ist. Im Übrigen handelt es sich um einen Paarreim. Der Verfasser hat sich dabei nicht (nur) von der Lust am Dichten leiten lassen, sondern ein bestimmtes Kalkül verfolgt. Paarreime sind wegen ihres gleichmäßigen Rhythmus leicht zu merken. Deshalb eignen sie sich nicht nur für Kinderverse, sondern auch für Merksprüche.



Schulungen CYBERSICHERHEIT UND PHISHING

Mit der Verbreitung der E-Mail und dem Siegeszug des Smartphones in den 2000er-Jahren haben sich Spioninnen und Spione ein neues Betätigungsfeld erschlossen: den digitalen Raum. Beim Phishing beispiels-

weise werden Nutzerinnen und Nutzer mit gefälschten E-Mails dazu verleitet, persönliche Daten preiszugeben. Das lässt sich am besten verhindern, wenn solche E-Mails gleich erkannt werden, was ein geschultes Auge voraussetzt. Für ihre Angehörigen hat sich die Bundeswehr daher vor einigen Jahren etwas einfallen lassen.

Um solche Attacken besser abwehren zu können, werden zur Sensibilisierung bewusst Phishing-E-Mails an die eigenen Leute verschickt. Die

Gefahren im Cyber- und Informationsraum werden so realistisch simuliert. Dienststellen können diesen Service für ihre Beschäftigten buchen. Zwischen Ende Juli und Ende September 2024 wurden rund 100.000 Phishing-Mails an zufällig ausgewählte Beschäftigte verschickt. Einige dieser Mails sahen aus, als kämen sie von DHL, Google oder der Deutschen Bahn. Etwa jede 23. der fingierten Mails wurde angeklickt. Fazit: Da ist noch Luft nach oben!

Kampagne SEI KEINE BEUTE!

Aus tiefen, dunkelbraunen Augen blickt er den Betrachter an: Der Bär wirkt bedrohlich. Kein Wunder, denn der Koloss wiegt bis zu 600 Kilogramm und kann bis zu drei Meter groß werden. Das Bild ist Teil der aktuellen Sicherheitskampagne „Sei keine Beute!“ des Verteidigungsministeriums. Anlass dafür ist die aktuelle sicherheitspolitische Lage: Krieg in der Ukraine,

Zeitenwende sowie hybride Bedrohungen und Angriffe. 30.000 Plakate, 75.000 Flyer und 225.000 Aufkleber sollen dafür sorgen, dass die Botschaft bei der Truppe ankommt: die Stärkung der Verteidigungsfähigkeit durch ein geschärftes Risikobewusstsein im Alltag. Die Angehörigen der Bundeswehr sind unter anderem dazu aufgefordert, Verschwiegenheit in dienstlichen Angelegenheiten zu wahren, sorgsam mit Smartphones und Laptops umzugehen – und ein gesundes Misstrauen an den Tag zu legen. Und zwar nicht nur bei finster dreinblickenden Bären.

OUTRO

VERHALTEN BEI IT-NOTFÄLLEN



Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten
--	-----------------------------	--

Wie angegeben (Bundesebene) für Sicherheit in der Informationsarbeit

Merkblatt und Notfallkarte INFORMATIONEN SCHÜTZEN

Bei der Informationssicherheit werden alle Angehörigen der Bundeswehr dezentral betreut. Zu diesem Zweck gibt es die Informationssicherheitsbeauftragten, kurz ISB. Probleme sollen nicht allein, sondern mit deren Hilfe gelöst werden. So steht es in den „Zehn Regeln zur Informationssicherheit am Arbeitsplatz“, einem Merkblatt, das im Dienstbetrieb immer griffbereit sein muss. Weitere Themen darin sind der Umgang mit Passwörtern und Verschlusssachen. Darüber hinaus gibt es noch die IT-Notfallkarte. Auch sie sollte in der Nähe des Schreibtischs aufbewahrt werden. Sie hilft Betroffenen, bei ungewöhnlichen Vorfällen mit der IT-Technik die richtigen Entscheidungen zu treffen.

Mehr Informationen
zu IT-Notfällen und Verhalten bei Cyberangriffen gibt es beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Einfach den QR-Code scannen!

Kampagne WER IST PIA?

Pia, Studentin an der Universität der Bundeswehr Hamburg, machte einst eine etwas unglückliche Figur. Für ein privates Video posierte sie so vor einem Auto, dass die gesamte Online-Welt den Parkausweis hinter der Windschutzscheibe erkennen konnte – mitsamt allen darauf befindlichen Informa-



tionen. Keine gute Idee! Später wurde dieser Vorfall zum Aufhänger für die Kampagne „Wer ist Pia?“ Pia war hier zugleich die Abkürzung für das Projekt „Partnerschaftliches Miteinander – IT- und Informationssicherheit – Awareness“. Das Projekt lief bis 2020. Die zentralen Anliegen waren die Vermittlung des richtigen Verhaltens am Arbeitsplatz und in sozialen Medien sowie des richtigen Umgangs mit mobilen Geräten und E-Mails. Hier hätte die Namensgeberin bestimmt auch einiges dazulernen können. ●

S. 88: Bundeswehr/Jane Harnemann (o.); Bundeswehr/PZ/CIR/Andreas Werner (u.)
S. 89: Bundesamt für Sicherheit in der Informationstechnik (o.); BAMAD (u.)

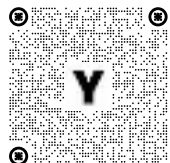
Dranbleiben

Mehr zum Thema

Ynside



Meldepflichten für sicherheitsüberprüftes Personal
Die meisten Angehörigen der Bundeswehr haben bereits eine Sicherheitsüberprüfung durchlaufen. Im Laufe der Zeit können sich jedoch Daten ändern. Was muss dem Sicherheitsbeauftragten der Dienststelle mitgeteilt werden? Hier erfährst du es.



Gemeinsam für mehr Sicherheit
Die Themen Datenschutz, militärische Sicherheit und Informationssicherheit sind in Zeiten von Spionage, Sabotage und Cyberkriminalität von zentraler Bedeutung. Jeder Einzelne muss sich in diesen Bereichen auskennen und aktiv mitwirken. Was das genau bedeutet, liest du hier.



Korruption: wachsam bleiben und vorbeugend handeln
Aufgepasst: Korruption beschränkt sich nicht auf das Zahlen und Annehmen von Geld. Aber was gehört noch dazu? Und wie kannst du dich davor schützen? Einen Überblick gibt dir dieser Artikel.



Ihre Frage – unsere Antwort: Militärischer Abschirmdienst
Um die Arbeit des Militärischen Abschirmdienstes (MAD) ranken sich so einige Mythen. Ynside beantwortet die wichtigsten Fragen und zeigt dir, wie der Nachrichtendienst der Bundeswehr wirklich arbeitet.

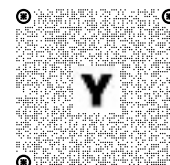


S. 90: Inago/Blickwinkel (E.S.); Bundeswehr/PIZ CIR/Andreas Wiener (Z.S.1-2); Bundeswehr/Forsten Kraatz (D.S.); Bundeswehr (V.S.o.); Bundeswehr/Forsten Kraatz (V.S.u.)
S. 91: Bundeswehr/Martina Pump (E.S.1-2); Bundeswehr (Z.S.1-2); picture alliance/Bea/Oliver Berg (D.S.o.); Bundeswehr/Maximilian Bosse (D.S.u.); Bundeswehr/Martina Pump (D.S.1-2)

Bundeswehr online



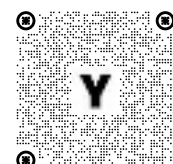
Zentrum für Cyber-Sicherheit der Bundeswehr
Die digitale Infrastruktur der Bundeswehr muss vor Angriffen geschützt werden. Dafür ist das Zentrum für Cyber-Sicherheit zuständig. Das Wichtigste in Kürze dazu findest du auf dieser Übersichtsseite.



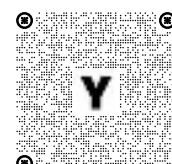
Militärischer Abschirmdienst
Der Militärische Abschirmdienst (MAD) kümmert sich um die innere Sicherheit der Bundeswehr. Neben dem Bundesamt für Verfassungsschutz und dem Bundesnachrichtendienst ist der MAD der dritte Nachrichtendienst auf Bundesebene. Weitere Informationen zu dieser Dienststelle findest du hier.



Wer schützt die Cyber-KRITIS?
Ein häufiges Ziel für Cyber-Angriffe sind kritische Infrastrukturen, wie etwa die Stromversorgung eines Landes, genannt KRITIS. Bei der NATO-Übung Cyber Coalition 2024 übten Militärangehörige aus 33 Nationen und diverse zivile Stellen die gemeinsame Abwehr eines Cyberangriffs. Mit dabei waren auch Angehörige des CIR sowie des Bundesamts für Sicherheit in der Informationstechnik. Mehr zur Übung gibt es hier.



Wie die Bundeswehr ihre IT-Systeme schützt
Computersysteme sind permanent der Gefahr von Cyberangriffen ausgesetzt. Besonders im Fokus stehen dabei staatliche Einrichtungen und damit auch die Bundeswehr. Wie die Truppe ihre IT-Systeme schützt, erfährst du in diesem Hintergrundartikel.



Museen



BND-Besucherzentrum

Von wegen Geheimniskrämerie: Mitten in Berlin und für jeden zugänglich informiert der Bundesnachrichtendienst über seine Arbeit. In einer interaktiven Ausstellung auf mehr als 1.000 Quadratmetern erfährst du, wie nachrichtendienstliche Informationen gewonnen werden und was es heißt, beim BND zu arbeiten.



Buch



Autor Markus Pöhlmann
Verlag De Gruyter Oldenbourg
Umfang 264 Seiten
Erscheinungsjahr 2024

„Geheimnis und Sicherheit“

Schon immer wollten Staaten das Militärpotenzial ihrer Nachbarn genau kennen. Doch erst im letzten Drittel des 19. Jahrhunderts schufen sie geheim operierende Organisationen, die diese Informationen dauerhaft beschaffen, auswerten und den Entscheidungsträgern zur Verfügung stellen. Die Studie des ZMSBw stellt die Entstehungsgeschichte militärischer Nachrichtendienste in Deutschland, Frankreich und Großbritannien zwischen 1871 und 1914 dar.



Impressum

Herausgeber Bundesministerium der Verteidigung, Stab Informationsarbeit, Stauffenbergstraße 18, 10785 Berlin

Verteilung innerhalb der Bundeswehr Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr, FA I RegMgmt BA, Referat 3 Bereitstellung, GM Freiherr-von-Gersdorff-Kaserne, Kommerner Straße 188, 53879 Euskirchen, 02251/953-3747, Bundeswehrkennzahl: 3461, mediendisposition@bundeswehr.org

Vertrieb Anteil Öffentlichkeitsarbeit Bundesamt für das Personalmanagement der Bundeswehr II 1.4 Vertrieb, Brühler Straße 309, 50968 Köln, bapersbw114vertrieb@bundeswehr.org

Redaktionsanschrift Zentrum Informationsarbeit Bundeswehr, Redaktion der Bundeswehr/Y-Redaktion, Reinhardtstraße 52, 10117 Berlin, Bundeswehrkennzahl: 8841, zivile Einwahl: 030/886228-Durchwahl

Redaktionssekretariat -2135, redaktionbweingang@bundeswehr.org

Leiter Redaktion der Bundeswehr Oberst Roman Grunwald, redaktionbweleiter@bundeswehr.org

Leitender Redakteur Y Dr. Florian Stöhr, -2481, leitung@y-magazin.de

Chefin vom Dienst Y Hauptmann Beate Schöne, -2482, cvd@y-magazin.de

Bildredaktion Andrea Bienert, -2660; Jörg Hüttenhölcher, -2665; bildredaktion@y-magazin.de

Schlussredaktion Frank Buchstein, schlussredaktion@y-magazin.de

Verlegerische Betreuung, Gestaltung und Produktion C3 Creative Code and Content GmbH, Heiligegeistkirchplatz 1, 10178 Berlin, info@c3.co
 Alleinige Gesellschafterin der C3 Creative Code and Content GmbH ist die Burda Gesellschaft mit beschränkter Haftung mit Sitz in Offenburg. Alleinige Gesellschafterin der Burda Gesellschaft mit beschränkter Haftung ist die Hubert Burda Media Holding Kommanditgesellschaft mit Sitz in Offenburg. Geschäftsführende, persönlich haftende Gesellschafter der Hubert Burda Media Holding Kommanditgesellschaft sind Prof. Dr. Hubert Burda und die Hubert Burda Media Holding Geschäftsführung SE.

Projektmanagement Tanja Klebsch, Account Director

Textredaktion Sebastian Blum, Lead Editorial; Michael Schulz, Senior Editor

Gestaltung Michael Pfirsich, Lead Design; Ben Kleinberg, Senior Information Designer (3D); Diana Brkovic, Senior Information Designer; Carsten Kalaschnikow, Bildredaktion

E-Paper Anica Schwarzer, Senior Art Director; Isabelle Emmerich, Senior Art Director

Mitwirkende Oberstleutnant Ralf Bonk, Simona Boyer, Franziska Hennecke, Fregattenkapitän Axel Herbst, Oberstabsfeldwebel Lars Hermann, Major Hannes Lembke, Hauptmann Norman Möller, Redaktion BAMAD, Oberstleutnant Torsten Stephan, Oberstleutnant Marc Trettenbach, Stabschef Michael Wils-Kudiabor

Aboverwaltung Im Auftrag von C3 Creative Code and Content GmbH: Fazit Communication GmbH, c/o CoverService GmbH & Co. KG, Postfach 1363, 82034 Deisenhofen, 089/85853-832, fazit-com@cover-services.de

Bezugspreis Jahresabonnement 22,20 € inkl. MwSt. und Versandkosten, Bundeswehrangehörige, Reservisten, Schüler, Auszubildende, Studierende und Ruhestandler erhalten mit Nachweis 15 Prozent Rabatt.

Erscheinungsweise Vier Ausgaben im Jahr
Druck Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel, www.ddm.de

Auflage 32.000

Hinweis Texte und Illustrationen sind urheberrechtlich geschützt. Nachdrucke, auch auszugsweise, fotomechanische Wiedergabe und Übersetzung sind nur nach schriftlicher Zustimmung seitens der Redaktion und mit Quellenangaben erlaubt.
 Sofern in den Bildcredits nicht anders angegeben, handelt es sich bei den urheberrechtlich geschützten Werken um Fotografien.

Redaktionsschluss Ausgabe Nr. 1/2025: 21. Januar 2025



Y im Abo!

Bundeswehr aus erster Hand gibt es nur im Y-Magazin. Viermal im Jahr spannende Reportagen, interessante Interviews und exklusive Informationen aus allen Bereichen der Bundeswehr – für 22,20 Euro jährlich. Jetzt per E-Mail abonnieren:

abo@y-magazin.de

Aboverwaltung durch Fazit Communication GmbH, c/o CoverService GmbH & Co. KG

MACH, WAS WIRKLICH ZÄHLT.



STOLZ AUF DAS, WAS SIE TUN? DANN ZEIGEN SIE ES ALLEN.

Zeigen Sie mit Herz und Leidenschaft, was in Ihnen und Ihrer Bundeswehr steckt. Repräsentieren Sie sich und Ihren Arbeitsplatz in neuen, deutschlandweiten Kampagnen. Bewerben Sie sich jetzt!

Ihr Talent, Ihre Fähigkeiten, Ihr Style. Zeigen Sie uns, was Sie drauf haben, und werden Sie Gesicht für unsere Kampagnen.

Sie brauchen sich nur unter ynside.extranet-bw.de anzumelden. Wir freuen uns auf Ihre aussagekräftigen Fotos und coole Kurzvideos. Kommen Sie in unser Team und inspirieren Sie andere.

Fragen? BMVgArbeitgebermarkeBw@bmvg.bund.de

WERDE GESICHT UND STIMME DER BUNDESWEHR.



JETZT ANMELDEN: [YNSIDE.EXTRANET-BW.DE](https://ynside.extranet-bw.de)



BUNDESWEHR