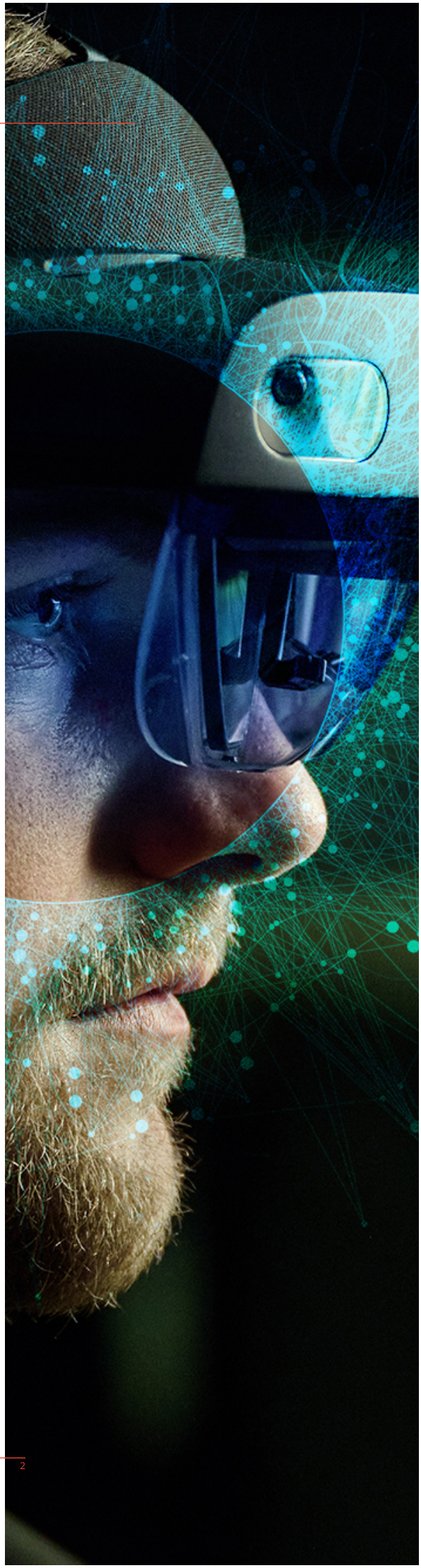
STRATEGISCHE INITIATIVE

NEUE DIGITALISIERUNGSPLATTFORM (NDP)

KOMMANDO CYBER

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee



INHALT

1. DIE WICHTIGSTEN VORTEILE DER NDP AUF EINEN BLICK

Mit der Entwicklung der Neuen Digitalisierungsplattform (NDP) stellt die Schweizer Armee zentrale Weichen für ihre Ausrichtung und Fähigkeiten in der Zukunft.

Die technologischen Fortschritte der letzten Jahre haben dazu geführt, dass heute eine immer grössere Anzahl an Sensoren und Messmöglichkeiten auf ein immer umfassenderes digitales Vernetzungspotenzial treffen. In Kombination resultieren aus diesen beiden Entwicklungen exponentiell wachsende Datenmengen, die dank immer besseren Fähigkeiten in der Datenverarbeitung wiederum neue Innovationen ermöglichen und so den technologischen Fortschritt vorantreiben. Deshalb ist auch in Zukunft von einer kontinuierlichen Verkürzung der Innovationszyklen sowie immer mehr Daten und Informationen auszugehen, welche Entscheidungsträgern zur Verfügung stehen. Gleichzeitig steigen die Schutzbedürfnisse in Bezug auf die einsatzrelevante IKT-Infrastruktur (Informations- und Kommunikationstechnologie).

Diese Erkenntnisse sind nicht neu. Seit vielen Jahren versuchen sowohl zivile, als auch militärische Akteure das Potential der Digitalisierung zu ihrem Vorteil zu nutzen. In der Schweizer Armee ist die NDP ein wichtiges Element dieser Bemühungen. Die Neue Digitalisierungsplattform hat das Ziel, als digitale Wirbelsäule der Armee in Zukunft einen standardisierten und bedarfsgerechten Datenaustausch innerhalb der verschiedenen Teilstreitkräfte und mit externen Partnern des Sicherheitsverbunds Schweiz (SVS) zu ermöglichen. Gleichzeitig schaffen die so zur Verfügung stehenden Daten die Basis für die Erstellung eines umfassenden Lagebilds und damit für schnellere und bessere Entscheide der Armee und ihrer Partner. Zudem adressiert die NDP Schutzbedürfnisse indem sie eine hochsichere, resiliente und robuste IKT-infrastruktur bereitstellt. Der Aufbau der Neuen Digitalisierungsplattform ist integraler Bestandteil des künftigen Kommando Cyber und stützt sich auf die Vorgaben aus der Gesamtkonzeption Cyber (GK Cyber) und der Vision 2030 der Schweizer Armee. (Mehr Informationen zur GK Cyber finden Sie hier sowie zur Vision 2030 hier)

Im Moment befindet sich die NDP und mit ihr die zahlreichen zugehörigen Komponenten im Aufbau. Diese Entwicklung bringt massgebliche Veränderungen mit sich. Das Potential der NDP für die Entwicklung und Einsatzfähigkeit unserer Armee ist sehr weitreichend. Allerdings macht es dies teilweise auch schwierig die Konsequenzen für den einzelnen Soldat bzw. Entscheidungsträger greifbar zu machen. Aus diesem Grund wird die NDP in dieser Dokumentation vorgestellt. Von der Einordung und Bedeutung im strategischen Kontext, über die konkrete technische Ausgestaltung sowie die daraus resultierenden Möglichkeiten, bis hin zu Praxisbeispielen, wie die NDP die Armee in Zukunft bei der Bewältigung von Krisensituationen unterstützen könnte. Abgeschlossen werden die Ausführungen von einem konkreten Ausblick, der aufzeigt, ab wann welche Leistungen durch die NDP möglich werden.

Die Möglichkeiten der NDP in Kürze: Die NDP...

... schafft die Voraussetzungen für einen **Wissens- und Entscheidvorsprung;**

... ermöglicht eine umfassende **Vernetzung & Verarbeitung von Daten und Informationen;**

... ist **hochsicher & robust;**

... verbessert die interne und externe **Koordination & Kooperation;**

2. KONTEXT

"Die Welt wird zunehmend volatiler, unsicherer, komplexer und vieldeutiger. Grosse Veränderungen finden bereits statt. Es bleibt uns deshalb nicht viel Zeit zur Transformation: Wir müssen heute damit beginnen." (Vision 2030, Zitat CdA, S.3)

Das aktuelle geopolitische Umfeld ist geprägt durch die wieder erstarkte Bedeutung von Machtpolitik, weltweit steigende Rüstungsausgaben, einen Wettlauf um die Führungsrolle innerhalb des technologischen Fortschritts sowie vom Trend der Regionalisierung. Der Krieg in der Ukraine hat diese Trends zusätzlich beschleunigt (Aussenpolitischer Bericht 2022). Im Bereich IKT finden rasante technologische Entwicklungen statt, die für die Schweizer Armee von höchster Relevanz sind. Dazu gehören beispielsweise die Verdichtung der Rechenleistung, künstliche Intelligenz (KI), Big Data, die umfassende Vernetzung, die Entwicklung von autonomen Plattformen, aber auch die zunehmende Bedeutung grosser Technologiefirmen. Dieser veränderte Kontext betrifft auch die Schweiz und bedingt eine strategische Neuausrichtung der Armee. Unter Berücksichtigung der Vision 2030, arbeitet in der Schweizer Armee deshalb seit Mai 2021 ein Projektteam am Aufbau des Kommando Cyber. Das einsatzorientierte, militärische Kommando wird ab 2024 erste Leistungen für die militärischen Schlüsselfähigkeiten in den Bereichen Lagebild, Cyberabwehr, IKT-Leistungen, Kryptologie und elektronische Kriegführung erbringen. Gleichzeitig sollen die durch Digitalisierung und Automatisierung erzielten Effizienzsteigerungen dabei helfen, die personellen Ressourcen der Armee in Zukunft noch effizienter einsetzen zu können. Der Aufbau der NDP ist ein integraler Bestandteil des Projekts Kommando Cyber.

2.1 Gesamtkonzeption Cyber

Der Aufbau der NDP ist auch im Kontext der am 13. April 2022 vom Bundesrat genehmigten Gesamtkonzeption Cyber zu betrachten. Diese zeigt die Herausforderungen im Bereich Cyber und Elektromagnetischer Raum (CER) und IKT auf und beschreibt, welche Fähigkeiten die Schweizer Armee bis Mitte der 2030er-Jahre entwickeln muss, um auch künftigen Bedrohungen begegnen zu können. Im Zentrum steht das Grundprinzip des Wissens- und Entscheidvorsprungs (siehe Infobox). Die NDP dient in diesem Kontext, mithilfe der Nutzung des Potentials der Digitalisierung, der Fähigkeitsentwicklung der Schweizer Armee. Dabei geht es um die folgenden, in der GK Cyber definierten, Fähigkeiten:

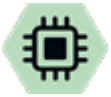
Lageverständnis im Verbund
Risiken und Bedrohungen identifizieren, den Kontext verstehen und Chancen erkennen – und bei Zusammenarbeit kohärent einschätzen.

CER-Eigenschutz
Die Truppenverbände, Systeme, Infrastrukturen, Informationen und Netze im CER vor Einwirkungen eines gegnerischen Akteurs schützen.

Datenverarbeitung robust und sicher
Die Verarbeitung und Verteilung von Daten auftragsbezogen und lagegerecht sicherstellen.

Aktionen im elektromagnetischen Raum
Aktionen im elektromagnetischen Raum führen.

Führung im Verbund organisatorisch und technisch
Die Führung lagegerecht über alle Stufen und Wirkungsräume sowie im Verbund mit Partnern organisatorisch und technisch sicherstellen.



Aktionen im Cyberraum
Aktionen im Cyberraum führen.

Die NDP ist gemäss GK Cyber ein essentieller Baustein für die Fähigkeitsentwicklung der Armee. Als Plattform ermöglicht sie die Nutzung all dieser Fähigkeiten im Verbund, dank verbessertem Eigenschutz, Nutzung des Potentials der Digitalisierung und der Führung eigener Aktionen im elektromagnetischen und Cyberraum. Truppen im Feld können in Zukunft direkt via militärische Endgeräte auf Anwendungen auf der NDP, wie zum Beispiel ein stufengerechtes Lagebild, zugreifen.

Wissens- und Entscheidvorsprung

«Für den Erfolg von Armeeeinsätzen ist entscheidend, wie schnell Informationen für die Führung nutzbar gemacht werden können. Wer schneller entscheidet als ein Gegner, beispielsweise wo Verbände oder Waffenwirkungen zum Einsatz gelangen, behält die Überhand. (...) Konkret geht es darum, gegenüber einem Gegner einen Wissens- und zeitlichen Entscheidvorsprung zu erreichen und zu halten, um mit begrenzten Mitteln die eigenen Ziele durchzusetzen. Ein Wissensvorsprung wird entweder mit dem eigenen Wissensvorsprung oder dem Wissensrückstand des Gegners erreicht. Ein eigener Wissensvorsprung entsteht, wenn Daten aktueller und besser verfügbar sind, wenn ihr Wahrheitsgehalt gewährleistet ist oder wenn sie rasch ausgewertet werden können. Ein gegnerischer Wissensrückstand lässt sich erzielen, indem beispielsweise eigene Mittel getarnt werden, indem der Gegner mit falschen Informationen getäuscht wird oder indem seine Führungssysteme mit Cyberangriffen beeinträchtigt werden. (...) Neben dem Wissensvorsprung streben Streitkräfte auch einen Entscheidvorsprung gegenüber dem Gegner an. Dabei geht es darum, entweder rascher zu handeln als ein Gegner oder den Gegner in seinem Handeln aktiv zu verlangsamen.»

Auszug aus der Gesamtkonzeption Cyber, S. 70–71.

2.2 Vision 2030

Die Vision 2030 beschreibt die Ambition der Schweizer Armee in Bezug auf ihren zukünftigen Zustand im Jahr 2030 und darüber hinaus. Im Kern zeichnet sich die Vision durch vier strategische Grundsätze aus:

- Denken und Handeln auf den Einsatz ausrichten
- Die Miliz befähigen
- Das Potenzial der Schweiz nutzen
- Innovation und Digitalisierung fördern und integrieren

Die Umsetzung der Vision 2030 erfolgt im Rahmen von 22 strategischen Initiativen, die sich allesamt an den vier strategischen Grundsätzen orientieren. Eine dieser Initiativen ist die strategische Initiative NDP (SI NDP), die im Rahmen dieser Dokumentation erläutert wird. Sie trägt direkt zur Realisierung der Vision 2030 bei. Insbesondere wird im Rahmen der SI NDP eine zentrale Herausforderung der Vision 2030 adressiert: Die Digitalisierung der Armee. Gemäss diesem Visionspunkt soll die Armee "digital schlagkräftig" werden. Streitkräfte, die das Potential der Digitalisierung nutzen, sind effektiver und anpassungsfähiger und können dementsprechend schneller auf die sich ständig verändernden Rahmenbedingungen und Herausforderungen künftiger Krisen und Konflikte reagieren. Ebenso begünstigt die Digitalisierung eine effiziente Nutzung der personellen Ressourcen der Armee.

Deshalb soll der gesamte Verbund von Sensoren, Nachrichtendienst, Führung bis Wirkung (SNFW) digitalisiert und integriert werden. Dies begünstigt die Generierung eines Wissens- und Entscheidvorsprungs und damit den schnellen und präzisen Einsatz von Effektoren. Ebenso muss aber die gesamte digitale Infrastruktur robust, resilient, degradationsfähig und vor Cyber-Angriffen geschützt sein.

2.3 Verbindungen (Abhängigkeiten) zu anderen Initiativen

Die 22 strategischen Initiativen der Vision 2030 sind eng miteinander verknüpft. Mit ihnen werden Lösungen gesucht, um die langfristige Sicherheit zu stützen, das Milizsystem zu stärken und die Führungspersönlichkeiten von morgen mit militärischer Führungsausbildung zu entwickeln. Es gibt diverse Berührungspunkte zwischen den einzelnen Initiativen, wobei sie sich gegenseitig ergänzen. Aus diesem Grund bestehen zwischen der SI NDP und anderen Initiativen ebenfalls Abhängigkeiten und Verbindungen, die in der Planung und im Aufbau der NDP berücksichtigt werden müssen. Wichtige Verbindungen und Abhängigkeiten bestehen insbesondere zu folgenden Strategischen Initiativen:

- **Cyber Fähigkeiten** (SI 14)

Neben der SI NDP wird diese Strategische Initiative ebenfalls vom Kommando Cyber geführt. Sie fokussiert sich direkt auf den Aufbau der in der GK Cyber definierten Fähigkeiten zu Führung von Aktionen im Cyber- und elektromagnetischen Raum. Sowohl die SI NDP als auch die SI Cyber Fähigkeiten sind zentrale Elemente zur zukünftigen Sicherstellung eines kontinuierlichen Wissens- und Entscheidvorsprungs. (Abbildung 1)

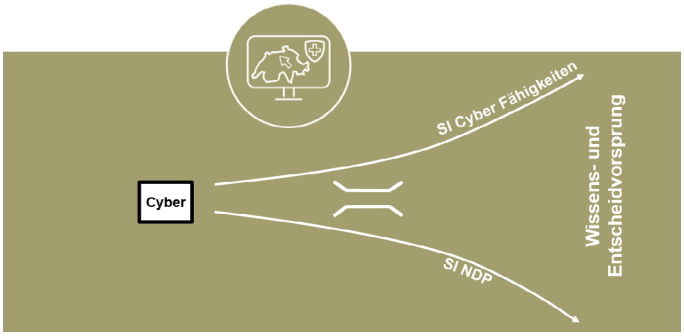


Abbildung 1: Der Wissens- und Entscheidvorsprung im Cyberraum, aber auch über alle anderen Wirkungsräume, basiert auf der erfolgreichen Umsetzung der Strategischen Initiativen NDP und Cyber Fähigkeiten.

- **Streitkräfte-Entwicklung** (SI 12)

Die Fähigkeiten und Kompetenzen der Armee müssen fortlaufend und in allen Wirkungsräumen weiterentwickelt werden, um mit dem technologischen Fortschritt mithalten zu können. Softwarebasierte Verteidigung ("software-defined defence", siehe Abbildung 6) und der Einsatz von künstlicher Intelligenz gelten beispielsweise als entscheidende Voraussetzungen für zukünftige militärische Operationen und müssen deshalb bereits heute im Kontext der Streitkräfte-Entwicklung berücksichtigt werden. In der Konsequenz werden die meisten zukünftigen Fähigkeiten und Systeme digitalisiert und vernetzt sein und sind damit auf eine gemeinsame digitale Plattform wie die NDP angewiesen. Von dieser Integration über alle Operationssphären hinweg profitieren auch andere aktuelle Rüstungsprojekte. Zum Beispiel können komplexe Systeme wie das F-35A Kampfflugzeug die zur Verfügung stehenden Sensoren und Wirkmittel nur im Verbund effektiv zum Einsatz bringen. Nebst der rein technischen Entwicklung der Streitkräfte bedingen die Veränderungen im Rahmen der NDP zudem eine Weiterentwicklung der Fähigkeiten in Bereichen wie Doktrin, der Führung von Operationen oder der Durchführung von Übungen.

- **Operative Kohärenz** (SI 13)

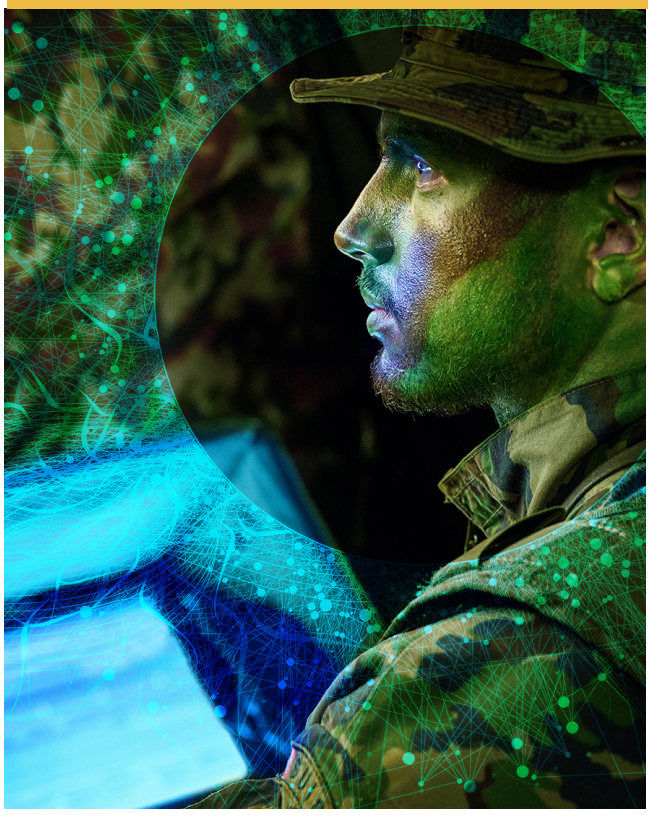
Die SI Operative Kohärenz hat das Ziel, das Zusammenspiel von militärischen Verbänden und Leistungen mit unterschiedlichen Waffen und Fähigkeiten im Verbund zu stärken und so ihre Wirkungen über alle Operationssphären (insbesondere Boden, Luft, Welt-, Cyber- und elektromagnetischen Raum) hinweg zu erhöhen. Dies erfordert multidimensionales bzw. operationssphärenübergreifendes Denken. Als digitale Wirbelsäule der Armee, schafft die NDP die technische Grundlage, um die operative Kohärenz in der Armee sicherzustellen.

- **Die Armee als Partnerin im SVS** (SI 8)

Die Armee und ihre Partner im Sicherheitsverbund Schweiz sollen in Krisensituationen in der Lage sein, Daten hochsicher und robust untereinander auszutauschen. Die NDP stellt dafür die notwendige Plattform zur Verfügung und dient als Bindeglied zwischen der Armee und ihren Partnern im SVS.

In Kürze: Der Aufbau der NDP...

- geschieht im Kontext der sich verstärkenden **geopolitischen Spannungen** und als Reaktion auf den **technologischen Fortschritt**;
- dient der Umsetzung der **Gesamtkonzeption Cyber** und ist damit ein zentraler Baustein der **Fähigkeitsentwicklung** der Schweizer Armee;
- ermöglicht den Aufbau einer **digital schlagkräftigen Armee** gemäss Vision 2030;
- erfolgt in **Koordination** mit weiteren **strategischen Initiativen**.



Exkurs: Die IKT-Infrastruktur der Ukraine im Krieg

Als in den frühen Morgenstunden des 24. Februars 2022 die ersten russischen Panzer über die russisch-ukrainische Grenze rollten, erwarteten viele Beobachter und Experten gleichzeitig den Beginn einer Serie von massiven Cyberangriffen auf die ukrainische IKT-Infrastruktur. Erwartet wurden parallel koordinierte Operationen im physischen und im digitalen Raum sowie grossangelegte Cyberkampagnen. Tatsächlich konnte in den ersten Wochen der Invasion eine Zunahme von Cyberattacken festgestellt werden. Bemerkenswert war insbesondere der Angriff auf das Satellitenkommunikationssystems des Unternehmens Viasat, welches nicht nur in der Ukraine, sondern auch in Westeuropa zu erheblichen Verbindungsstörungen führte. Auf den ersten Blick resultierten allerdings kaum strategische Effekte aus den Cyberattacken, ganz im Gegensatz zu den kinetischen Angriffen. Zusammenhängende sowie koordinierte Aktionen wurden in der Ukraine nur sehr vereinzelt und in einfachster Form beobachtet. Dementsprechend liegt der Schluss nahe, dass Cyberoperationen in traditionellen Konflikten weiterhin nur eine untergeordnete Rolle spielen. Bei genauerer Betrachtung lässt sich diese oberflächliche Feststellung jedoch nicht halten. Vielmehr spielten sichere Verbindungen und die kontinuierliche Verfügbarkeit von Daten eine Schlüsselrolle bei der Abwehr der ersten russischen Angriffswelle. Ebenso hatte die Tatsache, dass sich der ukrainische Präsident Wolodymyr Selensky in jeder Phase des Kriegs über die sozialen Medien direkt an die Bevölkerung und an die internationale Gemeinschaft wenden konnte, einen erheblichen Einfluss auf die ukrainische Verteidigungsmoral und die internationale Unterstützung der Ukraine. Gleichzeitig konnten wirkungsvolle militärische Verteidigungsaktionen und Gegenangriffe geplant und geführt werden.

Den Grundstein für diese erfolgreichen Verteidigungsmassnahmen legte das ukrainische Parlament erst wenige Tage vor der russischen Invasion. Am 17. Februar 2022 beschloss das Parlament, dass staatliche Daten und elektronische Dienstleistungen auf Server ausgelagert werden dürfen, die physisch ausserhalb der Ukraine liegen. In den darauffolgenden Wochen und Monaten wurden grosse Teile der staatlichen ukrainischen IKT-Infrastruktur, aber auch von privaten Unternehmen wie der grössten ukrainischen Privatbank, in die Cloud-Strukturen von internationalen IKT-Providern hochgeladen. Diese Massnahmen verringerten die ukrainische Verwundbarkeit gegenüber gezielten Cyber- und physischen Angriffen auf die IKT-Infrastruktur erheblich. Gleichzeitig verbesserten die sicheren und flexiblen Verbindungen über Starlink, ebenfalls ein privates Unternehmen, welches Internetverbindungen über Satelliten anbietet, die militärische und zivile Kommunikation in den Konfliktgebieten. Die vernetzten Verbindungen ermöglichten den ukrainischen Streitkräften, ihre militärischen Operationen präziser zu koordinieren und zeitverzugslos durchzuführen. Aktuell verfügt die Ukraine jedoch nicht vollständig autonom über eine eigene robuste und resiliente IKT-Infrastruktur. Mit dem Rückgriff auf externe Anbieter musste das Land potentielle Nachteile für die Daten- und Informationssicherheit hinnehmen. Konkret wurden zur Gewährleistung einer hohen Verfügbarkeit von Daten Abstriche im Bereich der Vertraulichkeit eingegangen, da die genutzten Plattformen nicht unter ukrainischer Kontrolle stehen (siehe Infobox zum C.I.A. Prinzip).

3. DIE NDP VERNETZT UND ERMÖGLICHT

"Damit die Armee ihre Aufgaben erfüllen kann, muss sie ganzheitlich über alle Wirkungsräume operieren können. Die Kernleistung der Armee im CER besteht darin, Informationen und Services auf der eigenen IKT ortsunabhängig zur Verfügung zu stellen und zu schützen. Dabei soll sie angebundene Partner nicht gefährden und damit ihre eigene Führungsfähigkeit und jene ihrer Partner in allen Lagen sicherstellen." (Gesamtkonzeption Cyber, S. 45)

3.1 Vernetzung – robust und sicher

Im Zentrum dieser Bestrebungen steht die NDP. Sie muss sicherstellen, dass die Schweizer Armee in Zukunft in der Lage ist, Operationen nahtlos und über alle Wirkungsräume hinweg autonom zu planen und durchzuführen. Damit wird die Plattform konsequent auf den Einsatz der Armee und ihrer Partner im SVS ausgerichtet. Ganz konkret handelt es sich bei der NDP um eine robuste, hochsichere und resiliente IKT-Plattform. Als zentraler Datenpool und Drehkreuz ermöglicht sie eine lückenlose Führungsfähigkeit sowie Verbesserungen in der Standardisierung und Automatisierung von Prozessen und bildet so die technische Basis für den eigenen Wissens- und Entscheidvorsprung. Die Automatisierung hat zudem positive Auswirkungen auf die Bedienungsfreundlichkeit von Systemen. Davon profitiert insbesondere die Miliz, die mit ihrem Einsatz die Durchhaltefähigkeit der NDP sicherstellt.

Eine zentrale Voraussetzung zur Schaffung eines Wissens- und Entscheidvorsprungs und damit für eine digital schlagkräftige Armee ist die umfassende Vernetzung von Sensoren und Effektoren. Dabei kann es sich beispielsweise um die Verbindung zwischen einem Aufklärungsradar und einem bodengestützten Luftabwehrsystem handeln. Oftmals sind die Zusammenhänge jedoch komplexer und eine Vielzahl von unterschiedlichen Sensoren und Effektoren sind miteinander vernetzt. So können zum Beispiel bodengesteuerte Mini-Drohnen gemeinsam mit lokalen Wetterstationen und Wettersatelliten eingesetzt werden. Die von den Sensoren gewonnenen Informationen in der Form von Luftaufnahmen sowie Geo- und Meteodaten werden fusioniert und anschliessend direkt und in Echtzeit an einen Effektor übermittelt. Im beschriebenen Szenario könnte es sich dabei beispielsweise um einen Rettungshubschrauber zur Durchführung eines Rettungseinsatzes in unzugänglichem Gelände handeln.

Die Herausforderungen beim Aufbau und Betrieb einer verbindenden Plattform, welche Vernetzungen über verschiedenste Wirkungsräume hinweg ermöglicht, sind vielfältig und komplex. Aufgrund der mit der Digitalisierung einhergehenden Vernetzung können umfassende Skaleneffekte erzielt werden, die wiederum zu immer kürzeren und schnelleren Innovationszyklen führen. Als Konsequenz sind beschaffte Systeme, die auf der Basis von spezifischen Hardware-Komponenten entwickelt wurden, teilweise bereits nach wenigen Jahren nicht mehr oder nur via komplexe Umwege mit neueren Systemen kompatibel. Die Folge sind isolierte Silosysteme, die nicht mit anderen Systemen verknüpft werden können. Diese fehlende Kompatibilität führt schlussendlich dazu, dass sehr umständlich oder unter Umständen keine integralen Lagebilder über alle Operationssphären hinweg erstellt und geteilt werden können. Genau dieser Zustand ist heute vielfach Realität.

Wie im Exkurs zum Ukraine-Krieg beschrieben, ist es der Ukraine gelungen, dank privater Ressourcen und Infrastrukturen ihre Daten zu schützen. Sie profitiert seitdem von der hohen Verfügbarkeit und Sicherheit der IKT-Systeme und erhöht so die Wirksamkeit ihrer Streitkräfte – ein zentraler Erfolgsfaktor in der Verteidigung des Landes. Aus Sicht der Schweizer Armee ist eine solche Lösung jedoch aus mehreren Gründen nicht praktikabel (vgl. Infobox zum C.I.A. Prinzip). Zum einen müsste zur Nutzung dieser Angebote auf zivile Infrastrukturen zurückgegriffen werden. Diese weist zwar in den meisten Fällen durchaus eine gewisse Redundanz und Robustheit auf, ist jedoch nicht primär auf den Betrieb in Krisensituationen ausgerichtet. So kann ein vorübergehender Strommangel oder Angriff auf die Strom-Infrastruktur zu kurzfristigen Ausfällen in der Verfügbarkeit (Availability) führen. Zum anderen wäre bei einem Rückgriff auf private Anbieter die insbesondere in Krisensituationen so zentrale Daten-Souveränität und Autonomie nicht mehr gewährleistet, da unbekannte Schwachstellen oder Abhängigkeiten bestehen können und die Integrität (Integrity) der Daten nicht garantiert werden kann. Im Fall der Ukraine ist die Vertraulichkeit der Daten (Confidentiality) zudem nicht mehr zwingend gewährleistet, da die entsprechende Infrastruktur unter externer Kontrolle steht. Die einsatzkritischen Daten und Dienstleistungen der NDP müssen dementsprechend direkt durch die Armee betrieben werden. Eine umfassende Abhängigkeit von privaten Anbietern für Netzwerk- und Datenplattformen ist deshalb nicht praktikabel. Der Aufbau der NDP bedingt aufgrund der zuvor beschriebenen immer kürzer werdenden Innovationszyklen einen grundsätzlichen kulturellen Paradigmenwechsel innerhalb der Schweizer Armee, der Innovation und Digitalisierung fördert und integriert. Dies äussert sich beispielsweise in der Anwendung von agilen Arbeitsmodellen oder einem neuen Umgang mit Wissen und Risiken.

C.I.A. Prinzip

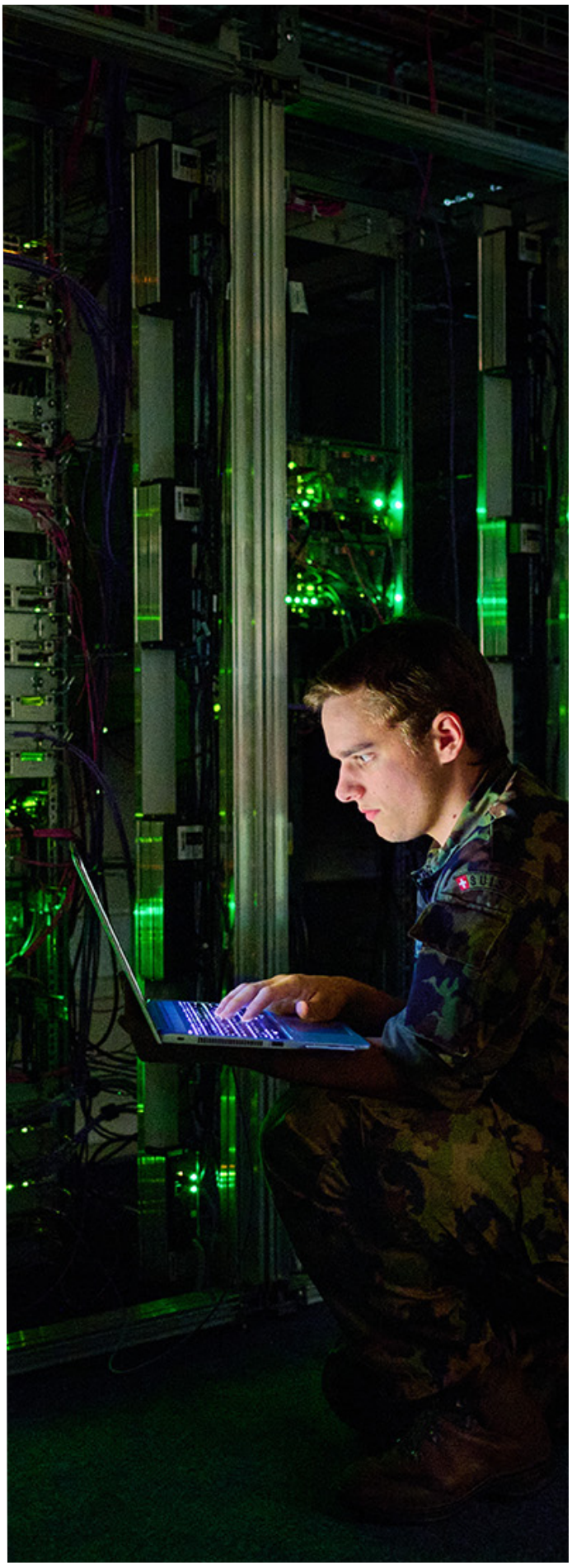
Im Bereich der Informationssicherheit bestehen drei wesentliche Schutzziele gemäss dem C.I.A. Prinzip. Dabei handelt es sich um den Schutz...

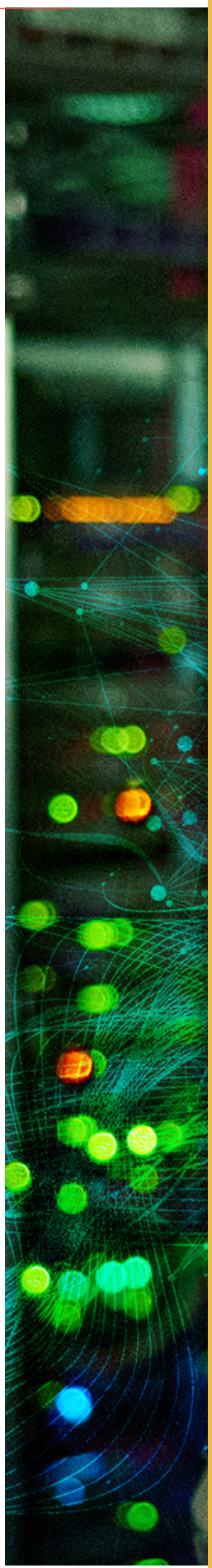
- der **Vertraulichkeit** von Daten (**C**onfidentiality) Daten dürfen lediglich von eindeutig identifizierten und autorisierten Benutzern eingesehen werden. Dies gilt sowohl für gespeicherte Daten als auch für die Sicherheit bei der Datenübertragung.
- der **Integrität** von Daten (**I**ntegrity) Änderungen an Daten müssen nachvollziehbar sein. Unbemerkte Änderungen an Daten müssen verhindert werden.
- der **Verfügbarkeit** von Daten (**A**vailability)Daten müssen dann verfügbar sein, wenn sie benötigt werden (in einem vereinbarten Zeitrahmen). Systemausfälle müssen verhindert werden.

Abbildung 2: Eigene Darstellung des C.I.A. Prinzips

Diese drei Bedingungen müssen erfüllt sein, um eine vollständige, informationstechnische Sicherheit (Datensicherheit) zu erlangen. Der Verlust einer oder mehrerer dieser Bedingungen stellt eine signifikante Bedrohung der informationstechnischen Sicherheit dar. Allerdings gilt es auch, Trade-offs zwischen den einzelnen Aspekten zu berücksichtigen. Sehr restriktive Sicherheitsanforderungen können beispielsweise zu Einbussen bei der Verfügbarkeit von Daten führen. Mit Blick auf die NDP bedeutet dies, dass die neue Plattform für einsatzkritische Leistungen die Schutzziele des C.I.A. Prinzips in allen drei Bereichen auf einem hohen Niveau erfüllen muss.

Auf diese Weise können die Entwicklungszyklen verkürzt und die Attraktivität der Armee als Arbeitgeberin für IKT-Fachkräfte gesteigert werden. Ebenso bedingt die Entwicklung der NDP eine Anpassung der Führungsprozesse innerhalb der Armee. Private Akteure sind dabei nicht vollständig vom Entwicklungsprozess ausgeschlossen. Da die Bausteine der NDP nach Möglichkeit auf gängigen Industriestandards basieren, werden wenn immer möglich direkt Produkte von privaten Akteuren verwendet. Für zentrale Leistungen geschieht dies im Rahmen von sogenannten strategischen Partnerschaften. Dies hat zur Folge, dass es sich bei den meisten NDP-Bausteinen um Standardprodukte von Drittherstellern handelt und nur in seltenen, begründeten Fällen um Eigenentwicklungen. Dieses Vorgehen fördert einerseits die Resilienz der Plattform und bringt andererseits Kosten- und Ressourcenvorteile in Form von Effizienzsteigerungen mit sich. Zudem vereinfacht diese Modularisierung die kontinuierliche Weiterentwicklung der Plattform, da direkt von den kurzen Innovationszyklen der Privatwirtschaft profitiert werden kann. Die Koordination von strategischen Partnerschaften stellt allerdings eine grosse Herausforderung dar, weshalb bereits im Rahmen der Initialisierung des Projekts spezifische Kontroll- und Steuermechanismen implementiert wurden.





NDP – Ein Blick in die Zukunft [Bewaffneter Konflikt]

Die Beziehungen der Schweiz zu einem bestimmten Staat haben sich derart verschlechtert, dass das autoritär geführte Land einen militärischen Angriff gegen die Schweiz startet. Die Attacken richten sich vor allem aus der Distanz gegen die kritische Infrastruktur und militärische Ziele im ganzen Land. Ebenso werden irreguläre bewaffnete Kräfte in die Schweiz eingeschleust. Der Gegner kämpft und koordiniert gleichzeitig in und aus verschiedenen Operationssphären. Insbesondere im Cyberraum ist er sehr aktiv. Es entsteht ein hybrides Konfliktumfeld.

In diesem Kontext bewährt sich die NDP in ihrer Funktion als digitale Wirbelsäule der Schweizer Armee. Trotz der heftigen Angriffe auf die militärische und zivile Infrastruktur ermöglicht die Plattform die Aufrechterhaltung von Kommunikations- und Führungsfähigkeit im Land, sowohl der Armee als auch von zivilen Partnern. Aufgrund gezielter kinetischer Angriffe kommt es zwar zu Unterbrüchen, der modulare Aufbau (Degradierbarkeit) der NDP erweist sich insgesamt aber als resilient. Die Auftragserfüllung zur Verteidigung unseres Landes, Bevölkerung und deren kritische Infrastruktur bleibt so stets gewährleistet. Dank der Nutzung von Lokal- und Regionalknoten können Systeme autonom weiterfunktionieren, auch wenn die Verbindung zum Gesamtsystem temporär nicht mehr möglich ist. So kann auch der Verlust eines Rechenzentrums (RZ) verkraftet werden, da die zwei weiteren RZ vollständig vor physischen Angriffen geschützt sind. Diese RZ stellen den Einsatz aller armeerelevanter Applikationen sicher und werden redundant betrieben. Dank ihrer modularen Architektur erweist sich die NDP als sehr resilient gegenüber Cyberangriffen des Gegners. Ausfälle bleiben auf wenige Systeme lokal beschränkt und haben keinen vollständigen Ausfall der NDP zur Folge.

Die NDP unterstützt aber auch direkt den Einsatz der eigenen Truppen gegen die feindlichen Kräfte. Zum einen steht der militärischen Führung über die NDP ein umfassendes Lagebild zur Verfügung, welches auf Daten und Informationen aus einer Vielzahl von Sensoren basiert, die sämtliche Wirkungsräume (Boden, Luft, Welt-, Cyber- und elektromagnetischer Raum) abdecken. Feindliche Drohnen und Abstandswaffen werden frühzeitig erkannt und abgefangen. Die Armee kann so den Wissens- und Entscheidvorsprung gegenüber den feindlichen Kräften sicherstellen. Zu diesem Vorsprung tragen auch ausländische Partner bei, welche mit der Schweiz im Rahmen dieses Konflikts kooperieren. Der politische Entscheid zur Kooperation ermöglicht ebenfalls eine Anbindung an die NDP; womit wertvolle – zum Teil Real Time - Daten und Informationen mit unserer Armee geteilt werden können, welche dann wiederum in das umfassende Lagebild, bzw. in den Sensor-, Nachrichten-, Führung und Wirkungsverbund einfliessen. Im Gegenzug gewinnen die ausländischen Partner Zugang zu wichtigen Informationen, die sie über die Plattform von der Schweiz erhalten. Insgesamt stellt die NDP auf diese Weise die Durchhaltefähigkeit der Schweizer Armee während eines bewaffneten Konflikts sicher, sodass die militärische Bedrohung abgewehrt werden kann.

Das fiktive Beispiel basiert auf einem Szenario, das im Rahmen der strategischen Initiative 8 "Armee als Partnerin im Sicherheitsverbund Schweiz" erarbeitet wurde.

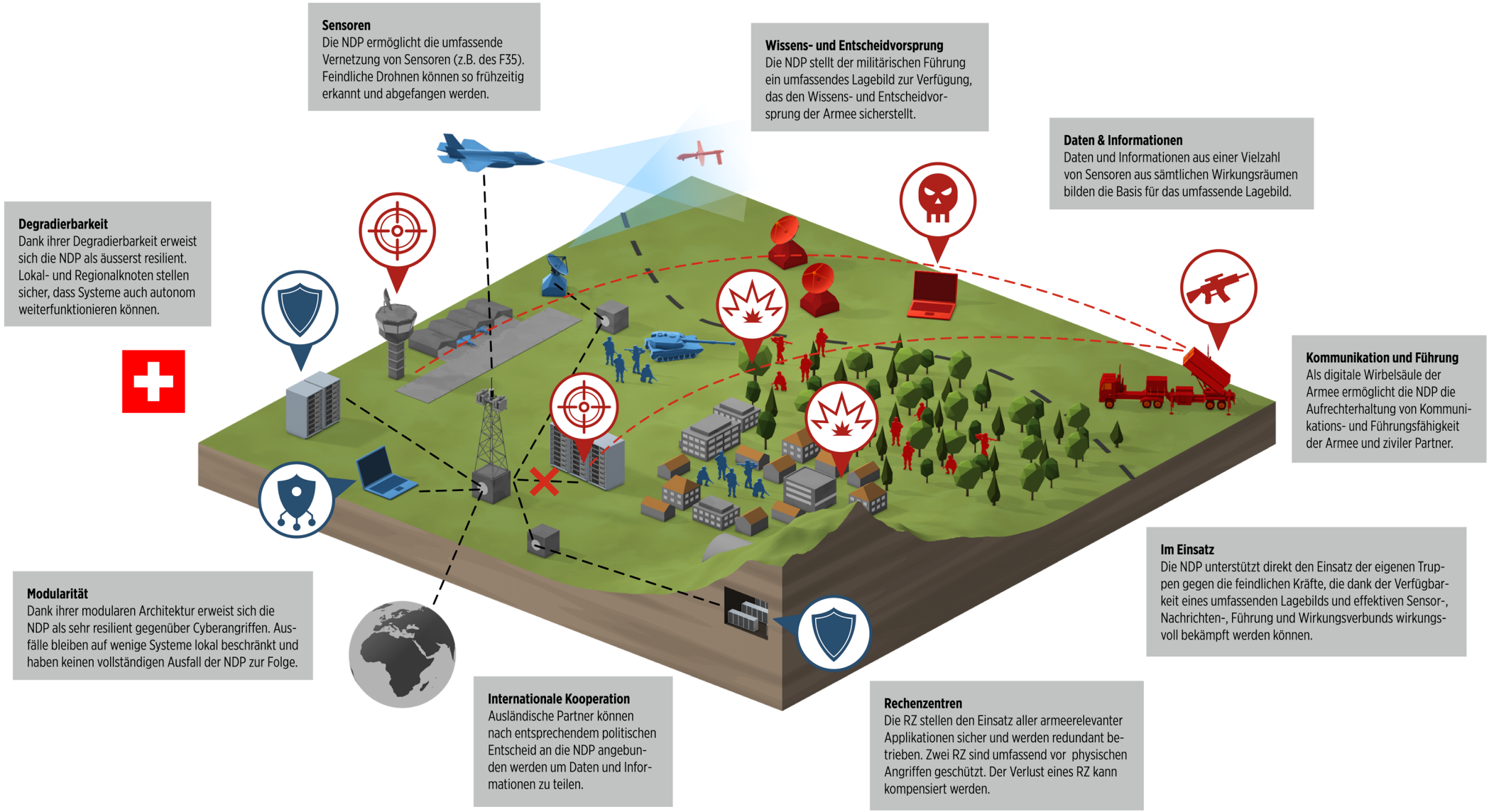
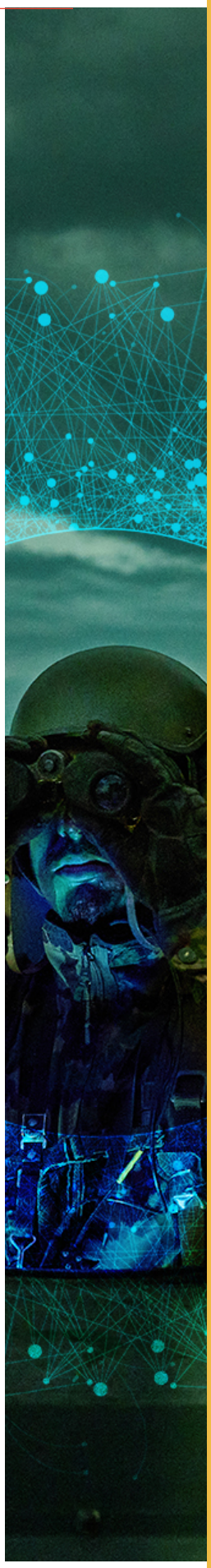


Abbildung 3: Mögliche Rollen und Szenarien der NDP während eines bewaffneten Einsatzes. Eigene Darstellung.



NDP – Ein Blick in die Zukunft [Erdbeben]

Ein starkes Erdbeben erschüttert die Nordwestschweiz und damit mehrere Kantone sowie die Nachbarländer Deutschland und Frankreich. Das Epizentrum liegt direkt unterhalb der stark besiedelten Metropolregion Basel. Besonders verheerend ist die Tatsache, dass vor dem Beben keine seismischen Auffälligkeiten registriert wurden und deshalb keine vorbereitenden Massnahmen getroffen werden konnten. Entsprechend gross sind die Schäden an Gebäuden und Infrastrukturen. Schnell werden hohe Opferzahlen registriert, die voraussichtlich noch deutlich ansteigen werden. Weiter verschärft wird die Krise durch zahlreiche Brände, Explosionen und Freisetzungen gefährlicher Stoffe in den betroffenen Gebieten. Diese erhöhen die akute Gefährdung für die Bevölkerung sowie für die im Einsatz stehenden Rettungskräfte zusätzlich. Mehrere Nachbeben und Plünderungen erschweren die Wiederherstellung von geordneten Verhältnissen. In vielen Gebieten sind keine zivilen Netzverbindungen mehr verfügbar.

Als Reaktion auf das Ereignis werden sofort nach dem Erdbeben die kantonalen Krisenstäbe gebildet, gefolgt von einem Krisenstab auf Stufe Bund. Zur aktuellen Lagebeurteilung können die Behörden auf ein umfassendes Lagebild zurückgreifen, welches der Armee und ihren Partnern im SVS zeitverzugslos über die NDP zur Verfügung steht. Dieses vereint die unterschiedlichsten Informationen von zivilen und militärischen Behörden, wie etwa die Verfügbarkeit von Krankenbetten, Einsatzmeldungen von Rettungsdiensten und militärischen Unterstützungseinheiten oder von Logistik-Daten. Aufgrund des modularen und robusten Aufbaus der NDP sind die lokalen Rettungskräfte via Lokalknoten direkt an die NDP angeschlossen und so ständig in der Lage, aktuelle Lageinformationen zu beziehen und zu übermitteln. Weiter ermöglicht das redundant aufgebaute und in die NDP integrierte Führungsnetz Schweiz, Daten sicher auszutauschen. Auch die Kooperation mit ausländischen Partnern, die ebenfalls vom Erdbeben betroffen sind bzw. ihre Unterstützung anbieten, wird von der Plattform deutlich vereinfacht, indem Daten und Informationen effizient ausgetauscht werden können.

Die grosse Menge an verfügbaren Daten auf der NDP macht es den Behörden einfacher, die verfügbaren Rettungs- und Sicherheitskräfte gezielt einzusetzen. Sie werden dabei durch verschiedene Anwendungen der künstlichen Intelligenz unterstützt. So können mithilfe von KI zum Beispiel die Auswirkungen von auslaufenden Chemikalien evaluiert und nach Schadenspotential kategorisiert werden. Darauf abgestimmt werden Logistik-Lösungen vorgeschlagen, um effektive flüssigkeitseindämmende Massnahmen zu installieren. Die Lieferungen der benötigten Maschinen und Materialien aus verschiedenen Logistikzentren werden dank einer implementierten KI-Anwendung weitgehend automatisch ausgelöst. Ebenso führen zu diesem Zeitpunkt zivile Behörden aufgrund der Beurteilung des Gefahrenpotentials bereits erste Evakuierungen durch. Die Zuteilung von Krankenbetten geschieht automatisiert. In der Nachbearbeitung der Krise zeigt sich, dass die umfassende Vernetzung der Rettungs- und Sicherheitskräfte über die NDP Planung und Koordination signifikant vereinfacht hatSchweiz erhalten. Insgesamt stellt die NDP auf diese Weise die Durchhaltefähigkeit der Schweizer Armee während eines bewaffneten Konflikts sicher, sodass die militärische Bedrohung abgewehrt werden kann.

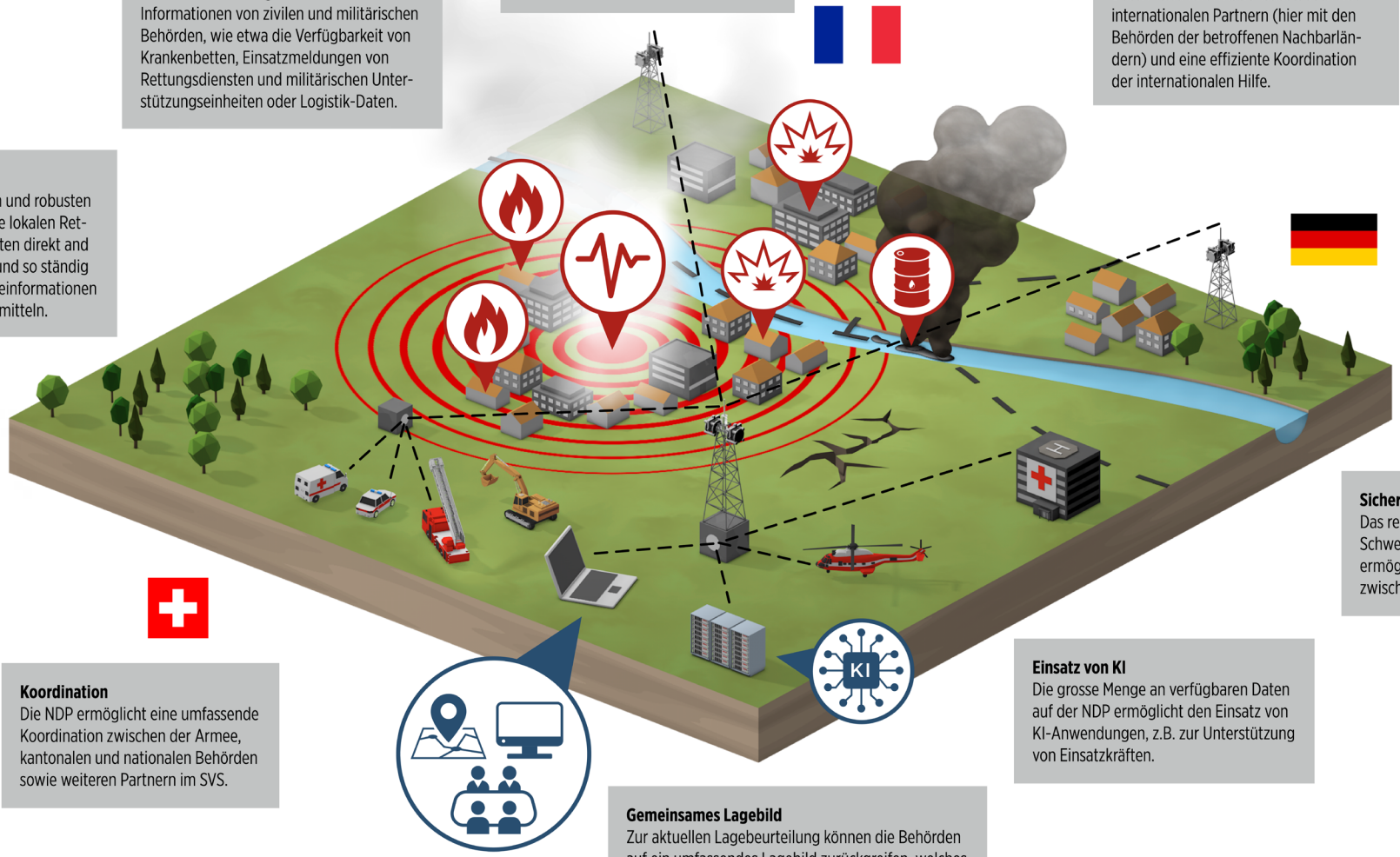
Das fiktive Beispiel basiert auf einem Szenario, das im Rahmen der strategischen Initiative 8 "Armee als Partnerin im Sicherheitsverbund Schweiz" erarbeitet wurde.

Im Einsatz
Durch die grosse Menge an verfügbaren Daten können die Behörden die verfügbaren Rettungs- und Sicherheitskräfte gezielt einsetzen.

Daten & Informationen
Das umfassende Lagebild vereint Daten und Informationen von zivilen und militärischen Behörden, wie etwa die Verfügbarkeit von Krankenbetten, Einsatzmeldungen von Rettungsdiensten und militärischen Unterstützungseinheiten oder Logistik-Daten.

Internationale Kooperation
Die NDP ermöglicht einen effizienten Daten- und Informationsaustausch mit internationalen Partnern (hier mit den Behörden der betroffenen Nachbarländern) und eine effiziente Koordination der internationalen Hilfe.

Lokalknoten
Aufgrund des modularen und robusten Aufbaus der NDP sind die lokalen Rettungskräfte via Lokalknoten direkt and die NDP angeschlossen und so ständig in der Lage, aktuelle Lageinformationen zu beziehen und zu übermitteln.



Sicherheit
Das redundant aufgebaute Führungsnetz Schweiz ist in der NDP integriert und ermöglicht den sicheren Datenaustausch zwischen Partnern.

Koordination
Die NDP ermöglicht eine umfassende Koordination zwischen der Armee, kantonalen und nationalen Behörden sowie weiteren Partnern im SVS.

Einsatz von KI
Die grosse Menge an verfügbaren Daten auf der NDP ermöglicht den Einsatz von KI-Anwendungen, z.B. zur Unterstützung von Einsatzkräften.

Gemeinsames Lagebild
Zur aktuellen Lagebeurteilung können die Behörden auf ein umfassendes Lagebild zurückgreifen, welches zeitverzugslos über die NDP zur Verfügung steht.

Abbildung 4: Mögliche Rollen und Szenarien der NDP während einer Naturkatastrophe. Eigene Darstellung.

3.2 Das Potential der Digitalisierung nutzen

Der erfolgreiche Aufbau sowie der anschliessende Betrieb der NDP ist mit erheblichen Verbesserungen der Resilienz und Fähigkeiten der Schweizer Armee und ihrer Partner im SVS verbunden. Die NDP ermöglicht in Zukunft einen barrierefreien, zeitverzugslosen Datenaustausch in einem geschützten Umfeld, sowohl innerhalb der verschiedenen Teile der Armee als auch mit externen Partnern des Sicherheitsverbunds Schweiz (Intraoperabilität) oder bei Bedarf mit ausländischen Streitkräften (Interoperabilität). Diese Durchgängigkeit zwischen der NDP und Partnern des SVS schafft die technischen Voraussetzungen für eine optimierte Zusammenarbeit. Die Optimierung der Zusammenarbeit ist jedoch nie lediglich eine technische Angelegenheit, sondern bedingt immer auch eine Anpassung der dazugehörigen Prozesse und Kultur. Diesem Umstand wird während des Aufbaus der NDP ebenfalls kontinuierlich Rechnung getragen. Im Zentrum der NDP steht die Schaffung der optimalen Rahmenbedingungen zur Erstellung eines aktuellen, integralen Lagebildes, auf dessen Basis zeitgerecht die richtigen Entscheidungen getroffen werden können. So können Effektoren zur richtigen Zeit, am richtigen Ort in der notwendigen Qualität ihre Wirkung entfalten. Weiter verbessert sich durch die spezielle Architektur der NDP die Resilienz, die Skalierbarkeit und die Unabhängigkeit der einzelnen IKT Systeme sowie des Systems Armee als Ganzes.

Konkret bedeutet dies zum Beispiel, dass Feuerleitstellen von Artillerie- oder Mörser-Einheiten direkt und zeitverzugslos auf die Positionsdaten von feindlichen Stellungen einer Aufklärungsdrohne zugreifen können. Dies verbessert nicht nur die Zielerfassung, sondern macht es auch möglich, anschliessend einen allfälligen Treffer direkt optisch zu verifizieren. Bearbeitet und übermittelt werden die Informationen dabei zum einen von Artillerie-spezifischen Systemen, welche direkt auf der NDP in einem hochsicheren und robusten Rechenzentrum betrieben werden, sowie von militärischen Endgeräten, die via Lokalknoten an die NDP angebunden sind.

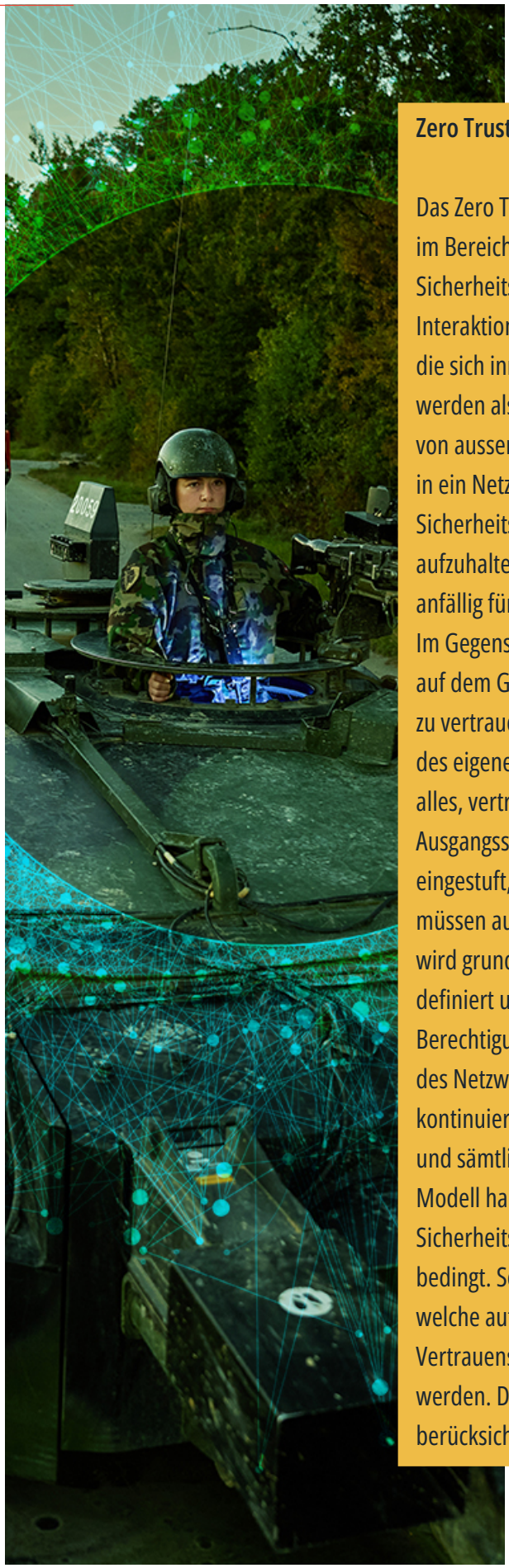
Gleichzeitig ist eine im gleichen Raum vorstossende Infanterie-Einheit nicht mehr darauf angewiesen, dass die Informationen zum Treffer der Artillerie so schnell wie möglich via mehrere Stationen an Übermittlungs- und Kommandostellen übertragen werden. Vielmehr kann die Einheit, da sie bereits über dieselben Informationen wie die Artillerie verfügt, sofort ihre Aktion im Sinne der Auftragstaktik fortführen und im Einklang mit dem umfassenden operativen Rahmen entscheidend wirken. Sie ist dazu ebenfalls mit militärischen Endgeräten ausgerüstet, die einen sicheren Datenaustausch ermöglichen. Zudem werden bei Bedarf auch Cyber Spezialisten eingesetzt. Sie kommen beispielsweise bei der Analyse und Auswertung von zurückgelassenem IKT-Material des Gegners zum Einsatz und überwachen die digitale und elektromagnetische Signatur der eigenen Einheit und damit einhergehende Gefahren

Die durchgängige Integration über alle Operationssphären hinweg ermöglicht sehr punktuelle, flexible Sperrungen des Luftraums. Bereits unmittelbar nach einem Artillerie-Beschuss und der damit einhergehenden Luftraumsperrung, können tieffliegende Lufteinheiten sowie Drohnen die vorstossenden Infanteriekräfte wieder im entsprechenden Raum unterstützen. Ebenfalls sind neue Sensor-Wirkungskombinationen innerhalb des SNFW-Verbunds möglich. So besteht zum Beispiel die Möglichkeit, die Sensoren des neuen Kampfflugzeugs F-35A zur verbesserten Zielerfassung mit bodengestützten Luft-Verteidigungssystemen wie den Patriot-Systemen zu verbinden. Da beide Systeme an die NDP angebunden sind, ist der Datenaustausch signifikant einfacher, als wenn jeweils eine spezifische Einzelverbindung aufgebaut werden müsste.

Als hochmoderner Sensor kombiniert und verdichtet der F-35A zudem verschiedene Daten direkt zu einem Lagebild. Dank der direkten Anbindung an die NDP und der umfassenden Integration sind auch übergeordnete Stufen umfassend über das aktuelle Geschehen im Einsatzgebiet informiert. Moderne Datenverarbeitungsmethoden wie Machine-Learning unterstützen die Entscheidungsträger in der Führung einer Aktion. Die grosse Flut an Informationen wird bedarfsgerecht automatisch priorisiert, stufengerecht dargestellt und auf mögliche Handlungsoptionen hin analysiert.

Einige Abgrenzungen zum spezifischen Aufbau der NDP sind in diesem Zusammenhang wichtig. Abbildung 4 stellt den Aufbau der NDP schematisch dar. Daraus wird ersichtlich, dass die NDP gegenüber klassischen Cloud-Plattformen Besonderheiten aufweist. Die modulare Architektur der NDP macht es einerseits möglich, dass auf der Plattform nebeneinander Daten unterschiedlichster Formate und Klassifizierungen bearbeitet und ausgetauscht werden können. Die Definition von klaren Integrationsrichtlinien ist hierfür zentral. Dabei handelt es sich um Vorgaben für die zukünftige An- und Einbindung von Anwendungen auf die NDP. Je nach den Bedürfnissen im Einsatz, Geheimhaltungsvorgaben oder benötigten Verbindungen werden Anwendungen unterschiedlich stark in die NDP integriert. So wird sichergestellt, dass einsatzrelevante Daten in Zukunft barrierefrei, in einem hochsicheren Umfeld, ausgetauscht werden können.

Andererseits stehen während des ganzen Aufbaus die Sicherheit und Resilienz der Plattform im Zentrum. Dazu gehört unter anderem die Zero Trust Architektur der NDP (siehe Infobox). Es muss zwingend verhindert werden, dass die NDP eine Schwachstelle aufweist, welche die ganze Plattform und alle darauf enthaltenen Informationen, Daten und Systeme kompromittieren oder zum Absturz bringen könnte. Zu diesem Zweck ist die NDP modular aufgebaut. Das heisst, dass die einzelnen Systeme und Anwendungen wohl über die NDP kommunizieren und Daten austauschen, aber im Falle eines Ausfalls eines bestimmten Systems oder einer Verbindung in der Lage sind, autonom zu arbeiten (siehe Abbildung 5). Zudem wird mit unterschiedlichen Integrationsstufen gearbeitet, so dass nicht alle Systeme gleich stark in die NDP integriert sind. Im Prinzip handelt es sich bei der NDP also um eine zentrale Struktur für unterschiedlichste, dezentrale Netzwerke und Anwendungen. Die NDP ermöglicht den Datenaustausch, wobei die Kompatibilität zwischen den Systemen und sichere und kontrollierbare Verbindungen zu externen Partnern gewährleistet wird. Dieser hochsichere und robuste Aufbau stellt sicher, dass die Schweizer Armee dank der Nutzung des Vernetzungspotentials der Digitalisierung in Zukunft über alle Wirkungssphären hinweg sowohl im Rahmen des SVS subsidiäre Unterstützung in Krisensituationen leisten kann, aber auch für potentielle militärische Konflikte gerüstet ist (siehe Fallbeispiele).



Zero Trust Architektur

Das Zero Trust Prinzip bedingt einen Paradigmenwechsel im Bereich der Cybersicherheit. Herkömmliche Sicherheitskonzepte vertrauen grundsätzlich Interaktionen aus dem eigenen Netzwerk. Benutzer, die sich innerhalb dieses Perimeters befinden, werden als vertrauenswürdiger eingestuft als solche von ausserhalb. Sobald aber jemand missbräuchlich in ein Netzwerk eindringt, sind kaum noch weitere Sicherheitsvorkehrungen vorhanden, um diesen Akteur aufzuhalten. Diese traditionelle Architektur ist deshalb anfällig für Cyberangriffe.

Im Gegensatz dazu basiert das Zero Trust Sicherheitsmodell auf dem Grundsatz, keinem Benutzer, Gerät oder Dienst zu vertrauen, sei es von innerhalb oder ausserhalb des eigenen Netzwerks. Es gilt das Motto "kontrolliere alles, vertraue niemandem". Jede Interaktion wird im Ausgangsstatus grundsätzlich als nicht vertrauenswürdig eingestuft, sämtliche Anwender und Anwendungen müssen authentifiziert werden und der Datenverkehr wird grundsätzlich verschlüsselt. Zugriffsrechte sind genau definiert und werden gemäss dem "Prinzip der geringsten Berechtigungen" erteilt. Ebenso bestehen innerhalb des Netzwerks Sicherheitssysteme, welche den Verkehr kontinuierlich analysieren, zulassen oder blockieren und sämtliche Aktionen aufzeichnen. Beim Zero Trust Modell handelt es sich also um einen datenzentrierten Sicherheitsansatz, der ein konstantes Monitoring bedingt. So können Lücken in der Sicherheitsarchitektur, welche auf einmaliger Authentifizierung oder impliziten Vertrauensmodellen basieren, wirkungsvoll geschlossen werden. Die NDP als standardisierte Plattform berücksichtigt die Prinzipien des Zero Trust Ansatzes.

3.3 Stand & Ausblick

Die NDP ist eng mit den Projekten "Telekommunikation der Armee" sowie "Führungsnetz Schweiz" verknüpft und wird in direkter Verbindung mit diesen Projekten aufgebaut. Seit 2021 arbeitet ein Team innerhalb des Projekts Kommando Cyber am Aufbau der Plattform.

In der ersten Phase des Projekts bis 2025 werden die zentralen Bausteine der Plattform entwickelt. Dazu gehören Arbeiten in Bezug auf den detaillierten Aufbau, die Anforderungen und die spezifische Architektur der Plattform. Zwingender Bestandteil dieser Phase ist auch die Ausarbeitung von Integrationsrichtlinien. Gleichzeitig werden bereits erste Demonstratoren und Testplattformen erstellt. Teilweise startet die Umsetzung der Konzepte parallel zur Konzeptionierung in der Form eines iterativen Prozesses. Zukünftige Leistungsbezüger werden kontinuierlich in diesen Prozess miteinbezogen.

Die Implementierung der NDP ist nicht nur ein technischer Prozess. Der Aufbau der NDP bedingt Anpassungen innerhalb der ganzen Armee – auch in der Arbeitskultur. Konzepte, Strategien und Prozesse müssen an die sich neu ergebenden Möglichkeiten und Herausforderungen angepasst werden. Aus kultureller Sicht gehören dazu zum Beispiel das gezielte Fördern vernetzter Denkweisen, agiler Arbeitsmodelle, eines neuen Umgangs mit Wissen und Risiken oder die konsequente Implementierung des Multi-Domain Gedankens. Viele dieser Aspekte werden über die zu Beginn beschriebenen strategischen Initiativen adressiert.

Im Juli 2026 wird durch die formale Betriebsaufnahme der NDP ab Landesknoten inklusive erster nutzbarer Referenzanwendungen ein wichtiger Meilenstein erreicht. Damit sind die Grundlagen für die Migration und den Neuaufbau der einsatzkritischen Anwendungen der Armee geschaffen. Zudem wird in dieser zweiten Projektphase zum ersten Mal ein zentrales IKT-Lagebild erstellt sowie erste Services autark und degradationsfähig für die Miliz zur Verfügung stehen.

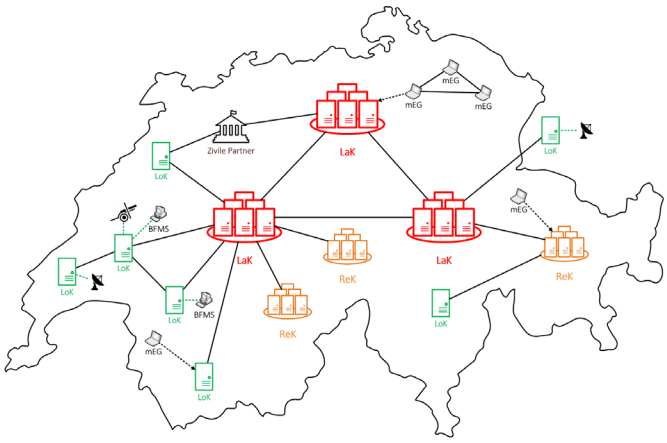


Abbildung 5: Schematische Darstellung der Plattform (Normalfall)

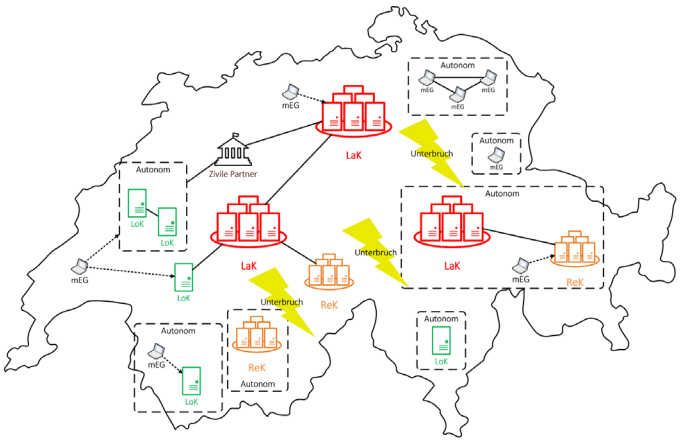


Abbildung 6: Schematische Darstellung der Plattform (Autonomiel)

Das volle Potential der NDP wird in einem etwas grösseren Zeitrahmen umgesetzt werden. Ab den 2030er Jahren werden die zuvor beschriebenen Skaleneffekte für die Armee nutzbar. Das bedeutet, dass die Systeme auf der NDP ab diesem Zeitpunkt kontinuierlich weiterentwickelt werden. Dies bedingt in dieser Phase die Anpassung auf ein agileres Beschaffungsmodell. So entsteht auch die angestrebte "Service-Orientierung" gegenüber externen militärischen Partnern sowie dem SVS. Ab dieser Phase soll es auch möglich sein, künstliche Intelligenz zur verbesserten Antizipation bei Lagebildern und Einsatzkonfigurationen hinzuzuziehen. Die KI profitiert dabei von den umfassenden Daten, welche auf der NDP interoperabel zur Verfügung stehen. Dazu soll auch eine neue Daten- und Informationsstrategie implementiert werden. Voraussetzung für die erfolgreiche Skalierung ist dabei die vollständige Inbetriebnahme des Rechenzenterverbunds RZ VBS/ Bund 2020 mit entsprechender Rechenleistung. sowie ein kontinuierlicher Wissensaufbau innerhalb der NDP wie auch im Gesamtsystem Armee. Mit diesen Voraussetzungen könnte die NDP zu einem späteren Zeitpunkt auch als technische Basis für den vermehrten Einbezug von Technologien aus dem Bereich der Robotik dienen. Damit ist die Entwicklung der NDP jedoch nicht abgeschlossen. Vielmehr handelt es sich bei der kontinuierlichen Weiterentwicklung der Plattform um einen etablierten Prozess, mit entsprechenden Strukturen und Ressourcen. Dieser Prozess ist ein wichtiger Bestandteil des "Software-basierten" Verteidigungsansatzes. Aufgrund der Tatsache, dass die Funktionen und Vernetzungen moderner Waffensysteme stark auf software-gesteuerten Prozessen basieren, sind lange, lineare Rüstungsprozesse, wie sie bei der Beschaffung von Waffensystemen oftmals heute noch üblich sind, nicht mehr praktikabel. Zu schnell entspricht auf diese Weise die Software, die wesentlich kürzere Entwicklungszyklen aufweist, nicht mehr den gängigen Standards. In der Konsequenz resultieren daraus reduzierte Kompatibilitäten und Fähigkeiten. Die Interoperabilität, ein zentraler Baustein der NDP, würde dadurch untergraben. Als Reaktion auf diese Entwicklungen wird deshalb der Beschaffungs- und Entwicklungsprozess auf die deutlich kürzeren Software-Entwicklungszyklen angepasst werden müssen. Abbildung 6 zeigt diesen Prozess schematisch auf. Der Entwicklungsprozess von militärischen Fähigkeiten soll in Zukunft verstärkt dem DevOps Zyklus aus dem Bereich der Software Entwicklung angelehnt sein. Nur auf diese Weise wird sich die NDP auch in Zukunft zusammen mit dem anhaltenden technologischen Fortschritt weiterentwickeln können.

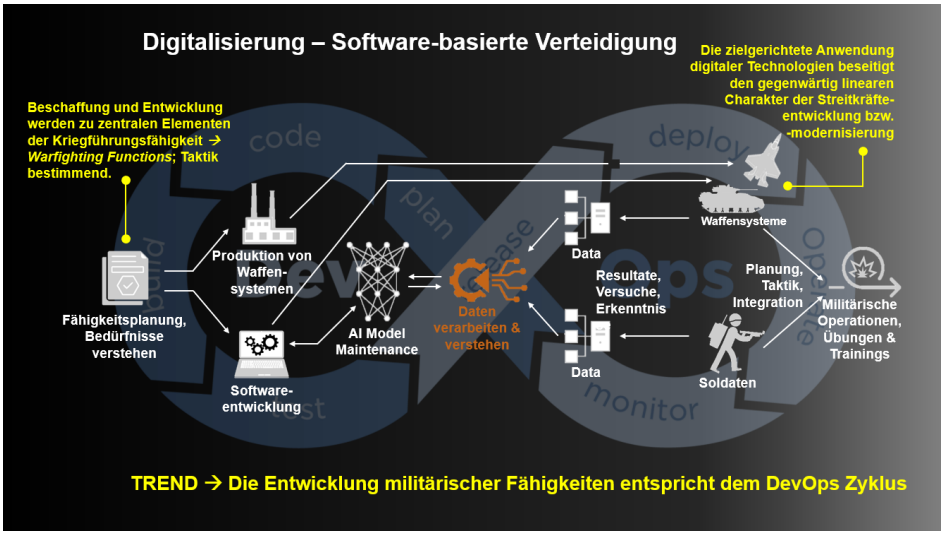


Abbildung 7: Schematische Darstellung des Software-basierten Verteidigungsansatzes. Eigene Darstellung basierend auf: Weiss, J. & Patt, D. (2022). Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era. Hudson Institute. S. 10.

3.4 Zentrale Voraussetzungen zum erfolgreichen Aufbau und Implementierung der NDP

- **Finanzielle & personelle Ressourcen:** Die Schweizer Armee ist während des Aufbaus sowie des anschliessenden Betriebs der NDP auf qualifizierte IKT-Fachkräfte angewiesen. Aufgrund des bestehenden Fachkräftemangels sind diverse Massnahmen geplant und teilweise bereits umgesetzt. Dazu gehören z.B. agilere Arbeitsmethoden, adäquate Einstiegslöhne für Berufseinsteigerinnen und Einsteiger sowie Initiativen zur Ausbildung von IKT-Fachkräften. Ebenso müssen finanzielle Ressourcen sichergestellt werden.
- **Strategische/ doktrinelle Anpassungen:** Die Implementierung der NDP ist nicht nur ein technischer Prozess. Der Aufbau der NDP bedingt Anpassungen innerhalb der ganzen Armee – auch in der Arbeitskultur. Konzepte, Strategien und Prozesse müssen an die sich neu ergebenden Möglichkeiten und Herausforderungen angepasst werden. Aus kultureller Sicht gehören dazu zum Beispiel das gezielte Fördern von vernetzten Denkweisen, innovative Arbeitsstrukturen oder die konsequente Implementierung des Multi-Domain Gedankens. Viele dieser Aspekte werden über die zu Beginn beschriebenen strategischen Initiativen aufgenommen.
- **Multidimensionales Denken:** Diese Voraussetzung wird durch die SI Operative Kohärenz aufgenommen. Diese strategische Initiative hat das Ziel, das Zusammenspiel von militärischen Verbänden und Leistungen mit unterschiedlichen Waffen und Fähigkeiten im Verbund zu stärken und so ihre Wirkungen über alle Operationssphären hinweg zu stärken. Dies erfordert multidimensionales bzw. operationssphärenübergreifendes Denken.
- **Erfolgreicher Aufbau des Kommando Cyber:** Der Aufbau der NDP ist eng mit dem Aufbau des Kommando Cyber verbunden. Zentrale Prozesse und Leistungen, die das Kommando Cyber erbringt, setzen die NDP voraus. Auf der anderen Seite ist die NDP auch direkt vom erfolgreichen Aufbau des Kommando Cyber abhängig. Das Kommando Cyber stellt die zentralen Ressourcen, Prozesse und Strukturen für den Aufbau und den Betrieb der NDP.
- **Entflechtung:** Damit die Sicherheit und Autonomie der einsatzkritischen militärischen IKT-Infrastruktur und damit auch der NDP gewährleistet werden kann, muss diese klar von der zivilen Infrastruktur abgegrenzt sein.
- **Rechenzenter/ Infrastruktur:** Die NDP ist auf eine resiliente und hochrobuste Infrastruktur, inkl. Rechenzentren, angewiesen.
- **Zusammenarbeit SVS und internationale Partner:** Die NDP ermöglicht in Zukunft einen standardisierten und bedarfsgerechten Datenaustausch innerhalb der verschiedenen Teilstreitkräfte der Armee und mit externen Partnern des Sicherheitsverbunds Schweiz oder bei Bedarf mit ausländischen Streitkräften (Inter- & Intraoperabilität). Damit dieser Austausch gewährleistet ist, müssen bereits während der Entwicklung der NDP die Bedürfnisse und Anforderungen von zivilen Partnern berücksichtigt werden.von zivilen Partnern berücksichtigt werden.

Das Wichtigste in Kürze
Die NDP...

- ist die zukünftige **robuste, hochsichere und resiliente IKT-Plattform** der Armee;
- bildet die technische Basis für ein **integrales Lagebild** und den eigenen **Wissens- und Entscheidvorsprung**;
- ermöglicht einen **standardisierten und bedarfsgerechten Datenaustausch** innerhalb der Armee und mit externen Partnern;
- ist **modular aufgebaut**, sodass Systeme auch **autonom** funktionieren können;
- wird unter **Kontrolle der Armee** aufgebaut und betrieben. **Ausgesuchte Instustriepartner** werden aber für die Entwicklung der einzelnen NDP-Bausteine einbezogen und können entlang der gesetzten Standards weiterführende Leistungen erbringen;
- verbessert dank der **Automatisierung von Prozessen** die **Bedienungsfreundlichkeit** von **Anwendungen und Systemen** und damit auch die **Miliztauglichkeit;**
- bezieht **Anwender** in die **Entwicklung** und den **Ausbau einsatzkritischer Services** mit ein;
- bedingt einen **Paradigmenwechsel** in der Schweizer Armee hin zur Förderung und Integration von Innovation und Digitalisierung;
- setzt sich, wenn immer möglich, aus **marktüblichen Komponenten** zusammen und profitiert so direkt von **Innovationen** der IT-Industrie;
- ermöglicht die **Nutzung des Potentials der Künstlichen Intelligenz;**
- wird durch die **Miliz** in ihrer **Durchhaltefähigkeit** unterstützt.

PROJEKT KOMMANDO CYBER

Schwarztorstrasse 53
3003 Bern

Website
www.vtg.admin.ch/de/organisation/fub/kdo-cyber