SWP

SWP-Studie

Alexandra Paulus

Eine Achillesferse moderner Streitkräfte

Risiken der Software-Lieferkette und Schutzmöglichkeiten

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

SWP-Studie 14
Oktober 2025, Berlin

- Moderne Streitkräfte sind enorm abhängig von Softwareprodukten. Diese sind das Ergebnis komplexer Geflechte aus Software-Anbietern, Dienstleistern, Softwarekomponenten und weiteren Unternehmen, die zusammen die Software-Lieferkette bilden.
- Bei »herkömmlichen« Cybersicherheitsvorfällen verschaffen sich Bedrohungsakteur:innen in der Regel direkt Zugang zu ihrem Ziel. Im Gegensatz dazu haben Risiken der Software-Lieferkette ihren Ursprung an einer vorgelagerten Stelle der Lieferkette und erzeugen dann an anderer Stelle einen Effekt — häufig bei den Endnutzer:innen.
- Streitkräfte sind besonders anfällig für diese Risiken. Vorfälle im militärischen Bereich, bei denen die Software-Lieferkette eine Rolle spielte, haben militärische Betriebsabläufe unterbrochen oder böswilligen Akteuren Wirtschaftsspionage, politische Spionage und Sabotage ermöglicht.
- Der Bundespolitik und der Bundeswehr stehen mehrere Maßnahmen zur Verfügung, um die Streitkräfte vor den Auswirkungen der Risiken der Software-Lieferkette zu schützen. Dabei müssen Entscheidungsträger:innen zunächst für unterschiedliche Einsatzbereiche von Software ein angemessenes Schutzniveau festlegen, um die Balance zu wahren zwischen dem Schutz vor den Risiken auf der einen und Funktionalität, Kosten und Einsatzgeschwindigkeit auf der anderen Seite.
- Die Bundesregierung und die Bundeswehr sollten einerseits Maßnahmen ergreifen, um einen bewussten Umgang der Streitkräfte mit den Risiken der Software-Lieferkette zu ermöglichen und sich selbst zu schützen; andererseits sollten sie Software-Anbieter dazu bringen, die Angreifbarkeit ihrer Produkte zu reduzieren. Durch die Kombination beider Ansätze kann diese mögliche Bedrohung in Schach gehalten werden.

SWP-Studie

Alexandra Paulus

Eine Achillesferse moderner Streitkräfte

Risiken der Software-Lieferkette und Schutzmöglichkeiten

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 14
Oktober 2025, Berlin

SWP-Studien unterliegen
einem Verfahren der Begut-
achtung durch Fachkolle-
ginnen und -kollegen und
durch die Institutsleitung *(peer
review)*, sie werden zudem
einem Lektorat unterzogen.
Weitere Informationen
zur Qualitätssicherung der
SWP finden Sie auf der SWP-
Website unter https://
www.swp-berlin.org/ueber-
uns/qualitaetssicherung/.
SWP-Studien geben die
Auffassung der Autoren und
Autorinnen wieder.

SWP
Stiftung Wissenschaft und
Politik
Deutsches Institut für
Internationale Politik und
Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6372
ISSN (Online) 2747-5115
DOI: 10.18449/2025S14

Inhalt

Dr. Alexandra Paulus ist Wissenschaftlerin in der Forschungsgruppe Sicherheitspolitik und Ko-Koordinierende Leiterin des Forschungsclusters Cybersicherheit und Digitalpolitik.

Eine Achillesferse moderner Streitkräfte. Risiken der Software-Lieferkette und Schutzmöglichkeiten

Moderne Streitkräfte sind enorm abhängig von Software — das gilt für Verwaltungsaufgaben und Logistik, aber auch für moderne Waffensysteme wie Panzer, Kriegsschiffe und Kampfflugzeuge. Die betreffenden Softwareprodukte sind das Ergebnis komplexer Geflechte aus Software-Anbietern, Dienstleistern, Softwarekomponenten und weiteren Unternehmen, die zusammen die Software-Lieferkette bilden.

Bei »herkömmlichen« Cybersicherheitsvorfällen verschaffen sich Bedrohungsakteur:innen häufig direkt Zugang zu ihrem Ziel. Im Gegensatz dazu haben Risiken der Software-Lieferkette ihren Ursprung an einer vorgelagerten Stelle der Lieferkette und treten dann an anderer Stelle in Form eines schädlichen Effekts zutage — häufig bei den Endnutzer:innen. Zum Beispiel drangen russische Spione zwischen 2019 und 2020 nicht direkt in die IT-Systeme der US-Behörde ein, die das US-Atomwaffenarsenal wartet. Stattdessen verschafften sie sich Zugang zum Softwarehersteller SolarWinds, um von dort aus ein Update mit Schadsoftware an die gut gesicherte Behörde zu senden und so an ihrem Ziel Daten abzugreifen.

Alle Glieder der Lieferkette sind dabei über Software verbunden — sei es durch das Softwareprodukt selbst, seine Komponenten oder über den Zugang zum Softwareprodukt, der beispielsweise einem Dienstleister gewährt wird. Entsprechend können alle Glieder in der Lieferkette von Softwareprodukten, die Streitkräfte nutzen, Einfallstore in militärische Systeme darstellen. Dabei sind gerade kleine und mittlere Unternehmen oder kleinere Open-Source-Software-Projekte (OSS-Projekte) oft schlecht geschützt und daher ein leichtes Ziel für Angreifer:innen. Dazu kommt, dass Streitkräfte üblicherweise keinen Überblick haben über alle Softwareprodukte, die sie nutzen — und erst recht nicht über alle Akteur:innen und Komponenten, die Teil der Lieferketten dieser Produkte sind. Und schließlich haben Streitkräfte keine oder nur sehr begrenzte Kontrolle über große Teile der Lieferkette. Daher sind Software-Lieferketten eine Achillesferse moderner Streitkräfte: Selbst das technologisch fortschrittlichste Militär kann zum

Opfer werden von Angriffen, die sich die komplexe Struktur von Software-Lieferketten zunutze machen.

Vorfälle, in denen die Software-Lieferkette eine Rolle spielt, können militärische Betriebsabläufe unterbrechen oder es böswilligen Akteur:innen erlauben, Wirtschaftsspionage, politische Spionage und Sabotage zu betreiben. So erlangten etwa zwischen 2013 und 2018 Personen aus dem Umfeld des chinesischen Nachrichtendienstes über Cloud-Anbieter Zugriff zu den Systemen der größten US-Marinewerft. Und 2022, am ersten Tag der russischen Invasion der Ukraine, kaperte der russische Militärgeheimdienst ein Software-Update eines Satellitenkommunikationsanbieters, um die Konnektivität des ukrainischen Militärs auf dem Gefechtsfeld zu unterbrechen. Auch unbeabsichtigte Fehler können großen Schaden bei Endnutzer:innen hervorrufen, wie der »CrowdStrike«-Vorfall aus dem Sommer 2024 zeigt, der weltweit etwa 8,5 Millionen Geräte vorübergehend unbrauchbar machte. Und schließlich kann auch fehlender Software-Support tiefgreifende Folgen haben — so drohten ukrainische Kampfflugzeuge im März 2025 ohne Software-Support durch die USA einsatzunfähig zu werden. Kurz: Entsprechende Vorfälle können die Kriegstüchtigkeit von Streitkräften gefährden.

Vor diesem Hintergrund beantwortet diese Studie die Frage, wie sich Streitkräfte vor Risiken der Software-Lieferkette schützen können. In den Hauptkapiteln der Studie werden (1) die Struktur von Software-Lieferketten und die daraus hervorgehenden Risiken beschrieben; (2) besondere Merkmale von Streitkräften, die ihre Anfälligkeit für diese Risiken verstärken, analysiert und die Auswirkungen wichtiger entsprechender Vorfälle im militärischen Bereich untersucht; und schließlich wird herausgearbeitet, (3) wie Streitkräfte sich selbst besser vor diesen Risiken schützen können und (4) wie Politik und Streitkräfte Software-Anbieter dazu bewegen können, die Risiken ihrer Produkte zu reduzieren.

Im Ergebnis wird empfohlen, dass die Politik und die Bundeswehr zunächst abwägen, wie das anzustrebende Schutzniveau von Softwareprodukten je nach Einsatzbereich aussehen sollte. Zudem sollte die Bundeswehr selbst Maßnahmen ergreifen, um sich vor den Risiken der Software-Lieferkette zu schützen:

- Um handlungsfähig zu werden, sollte einer Stelle die Verantwortung für den Umgang mit diesen Risiken übertragen werden. Aufgabe dieser zuständigen Person wäre es, Leitlinien für den Umgang mit Risiken in der Software-Lieferkette sowie für die militärische Nutzung von Open-Source-Software zu formulieren.
- Um entsprechende Maßnahmen auch in den operativen Betriebsabläufen der Bundeswehr zu verankern, sollten bundeswehrweit Prozesse zum Umgang mit Risiken der Software-Lieferkette etabliert werden — beispielsweise sollte das IT-Fachpersonal der Bundeswehr regelmäßig überprüfen, ob eingesetzte Softwareprodukte noch Sicherheitsupdates und funktionale Upgrades erhalten.
- Damit die hier aufgeführten Maßnahmen funktionieren, sollte die Bundeswehr mehr Fachexpertise zu diesem Thema aufbauen.
- Um Angriffsmöglichkeiten schon vorab zu identifizieren, sollte die Bundeswehr selbst nach Schwachstellen in eigenen Systemen und verwendeten Softwareprodukten suchen.
- Und um Angriffe von Innentäter:innen zu verhindern, sollte der Beschaffungsapparat Wege finden, die es ermöglichen, dass nicht vertrauenswürdige Anbieter von der Beschaffung ausgeschlossen werden.

Zudem sollten Politik und Bundeswehr Software-Anbieter dazu bringen, die Risiken ihrer Produkte zu reduzieren:

- Dafür sollten Politik und Bundeswehr zunächst Maßnahmen identifizieren, die die Anbieter umsetzen müssen. Die Studie macht dazu sechs Vorschläge, darunter die Bereitstellung von Informationen über Softwarekomponenten bzw. über die Ausnutzbarkeit von Schwachstellen in eigenen Produkten.
- Um die Anbieter zur Umsetzung dieser Schritte zu bewegen, sollte die Politik dem Beschaffungspersonal Musterverträge zur Verfügung stellen und die Beschaffungsanforderungen und das Produkthaftungsrecht anpassen.
- Zusammengenommen können es diese Maßnahmen der Bundeswehr ermöglichen, Risiken in der Software-Lieferkette auf ein akzeptables Maß zu reduzieren, ohne auf die Vorteile militärisch genutzter Software verzichten zu müssen.

Einleitung

Streitkräfte sind für die meisten ihrer Aktivitäten auf Software angewiesen, von administrativen Aufgaben und Logistik bis hin zur Kriegsführung: So sind etwa Lagebildplattformen unverzichtbar geworden und kaum ein Panzer, Kriegsschiff oder Kampfflugzeug funktioniert ohne Software. Diese Softwareprodukte sind das Ergebnis komplexer Lieferketten aus Lieferanten, Dienstleistern und Softwarekomponenten, die sich der Kontrolle der Streitkräfte entziehen. Folglich hängt die Sicherheit eines Militärs auch von der Sicherheit der zahlreichen Software-Anbieter, Dienstleister sowie Entwickler:innen und Maintainer:innen[1] von Softwarekomponenten ab.

Vorfälle im militärischen Bereich haben gezeigt, dass Software-Lieferketten-Risiken die Kriegstüchtigkeit von Streitkräften gefährden können.

Vorfälle im militärischen Bereich haben gezeigt, dass Software-Lieferketten-Risiken die Kriegstüchtigkeit von Streitkräften gefährden können, da sie die Truppe nicht nur zu Unterbrechungen im Betriebsablauf zwingen, sondern sie auch Spionage und Sabotage aussetzen können: So griff der chinesische Geheimdienst zwischen 2013 und 2018 auf die Systeme der größten US-Marinewerft zu, um geistiges Eigentum zu stehlen. Russland spionierte zwischen 2019 und 2020 die Behörde aus, die für die Verwaltung des US-Atomwaffenarsenals zuständig ist. Und 2022, am ersten Tag der russischen Invasion der Ukraine, schaltete der russische Militärgeheimdienst die Satellitenkommunikation aus, auf die die ukrainische Armee angewiesen war. In all diesen Fällen nahmen die Angreifer nicht direkt die gut gesicherten Streitkräfte und Rüstungsunternehmen ins Visier, sondern verschafften sich Zugang über die Software-Lieferkette.[2]

Kurzum, Software-Lieferketten-Risiken sind eine Achillesferse moderner Streitkräfte und stellen eine strategische Herausforderung dar. Dennoch haben weite Teile der Bundespolitik und der Bundeswehr die Bedeutung des Themas noch nicht erkannt. Im Jahr 2021 veröffentlichte eine Gruppe von Expert:innen aus der deutschen Sicherheits- und Verteidigungsindustrie und dem Bundesministerium der Verteidigung (BMVg) ein Papier mit Vorschlägen zur Verbesserung der Sicherheit von IT-Lieferketten,[3] doch diese wurden bisher nicht aufgegriffen. Welchen Risiken Streitkräfte in diesem Bereich ausgesetzt sind, hängt maßgeblich davon ab, welche Softwareprodukte sie beschaffen (und von welchen Anbietern) und wie sie diese nutzen und verwalten. Darüber entscheidet aktuell jedoch üblicherweise Beschaffungs- und IT-Fachpersonal ad hoc. Das muss sich ändern.

Stattdessen sollte die Bundeswehr zu einem strategischen Umgang mit Risiken der Software-Lieferkette kommen. Die Studie skizziert die vier dafür nötigen Schritte. Erstens müssen Entscheidungsträger:innen in Politik und Bundeswehr verstehen, wie Software-Lieferketten aussehen[4] und welche Risiken sie bergen.[5] Zweitens sollten sie sich bewusst werden, dass diese Risiken Streitkräfte besonders betreffen,[6] weil Software für militärisches Handeln unverzichtbar geworden ist — gerade in Zeiten, in denen unter dem

1 Maintainer:innen kümmern sich um Sicherheitsupdates und funktionale Upgrades von OSS-Komponenten und -Produkten.

2 Diese Vorfälle werden im Abschnitt »Die Auswirkungen vergangener Software-Lieferketten-Vorfälle auf Streitkräfte«, S. 16, erläutert.

3 BMVg u.a., *Ideenpapier »Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr«*, Berlin, 8.6.2021, <https://www.bmvg.de/resource/blob/5103740/9cc683ea3fac46f37290590cc41aa1a6/download-sichere-it-lieferketten-data.pdf>. Sofern nicht anders angegeben, wurden alle Websites zuletzt am 17.9.2025 aufgerufen.

4 Siehe Kapitel »Die Software-Lieferkette«, S. 9.

5 Siehe Kapitel »Risiken der Software-Lieferkette«, S. 11.

6 Siehe Kapitel »Die besondere Bedrohung von Streitkräften«, S. 14.

Stichwort »Software-defined Defense«[7] militärisches Gerät immer stärker vernetzt werden soll, was die Angriffsoberfläche dramatisch vergrößert. Dabei sollten Streitkräfte aus vergangenen Vorfällen im militärischen Bereich, in denen die Software-Lieferkette eine Rolle spielte, lernen.

Darüber hinaus zeigt die Studie — auf der Basis von Einschätzungen der Expert:innen[8] und praktischen Beispielen aus verschiedenen Ländern — auf, wie politische Verantwortliche und die Bundeswehr mit Software-Lieferketten-Risiken umgehen sollten. In einem dritten Schritt sollten sie zunächst selbst Maßnahmen ergreifen, um sich vor den Bedrohungen zu schützen.[9] Viertens sollten sie Software-Anbieter dazu bewegen, effektiver mit Software-Lieferketten-Risiken umzugehen.[10] Mit diesen vier Schritten können Entscheidungsträger:innen in der Politik und in der Bundeswehr diese Achillesferse schützen und die Kriegstüchtigkeit der deutschen Streitkräfte sicherstellen.

7 Simona Soare u.a., *Software-defined Defence: Algorithms at War*, London: The International Institute for Strategic Studies, Februar 2023, <https://www.iiss.org/research-paper/2023/02/software-defined-defence/>; Nand Mulchandani / John N. Shanahan, *Software-Defined Warfare: Architecting the DOD's Transition to the Digital Age*, Washington, D.C.: Center for Strategic & International Studies, September 2022, <https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age>.

8 Die in der Studie formulierten Politikempfehlungen basieren unter anderem auf mehr als 65 Interviews und einem Workshop mit internationalen Expert:innen.

9 Siehe Kapitel »Wie sich Streitkräfte selbst vor Risiken der Software-Lieferkette schützen können«, S. 19.

10 Siehe Kapitel »Wie Politik und Streitkräfte Software-Anbieter zum Risikomanagement bewegen können«, S. 27.

Die Software-Lieferkette

Softwareprodukte haben komplexe Lieferketten. Diese umfassen alle Artefakte (wie Programmcode), Prozesse, Technologien und nicht zuletzt Menschen, die an der Herstellung eines bestimmten Softwareprodukts beteiligt sind (siehe Grafik 1, S. 10).[11] Die Lieferkette eines jeden Softwareprodukts beginnt mit seinen »Rohstoffen«, das heißt den Softwarekomponenten. Dabei handelt es sich um unabhängige Einheiten von Quellcode wie etwa sogenannte Bibliotheken.[12] Solche Komponenten machen den Großteil des Codes vieler Softwareprogramme aus, da die Entwickler:innen häufig bereits geschriebene Codebausteine wiederverwenden.[13] Dabei spielen besonders die Open-Source-Software(OSS)-Community und kommerziell erhältliche Bibliotheken eine Schlüsselrolle.

Eine Person oder Organisation, die Software entwickelt[14] (etwa ein Hersteller), kann benötigte Softwarekomponenten auf drei Wegen beziehen: Erstens kann der Hersteller OSS-Komponenten aus einem Code-Repository wie GitHub verwenden. Dabei geht er keine vertragliche Bindung mit den Entwickler:innen der Komponente ein (und kennt sie in der Regel auch nicht).[15] Zweitens kann er eine Komponente von einem anderen Unternehmen kaufen. Und drittens kann er die Komponente selbst entwickeln.

OSS ist der Gegenentwurf zu proprietärer Software, bei der der Quellcode geheim gehalten wird, da er als geistiges Eigentum gilt. Im OSS-Ökosystem hingegen entwickeln und pflegen Einzelpersonen oder Gruppen Softwareprodukte und -komponenten und stellen sie der Allgemeinheit[16] zur Verfügung, die den Quellcode einsehen, bearbeiten und die Software nutzen kann. OSS ist das Fundament des modernen Software-Ökosystems: Fast alle Softwareprodukte enthalten OSS-Komponenten[17] und für bestimmte Anwendungsfälle sind OSS-Produkte führend.[18] Im Gegensatz dazu können kommerziell erhältliche Bibliotheken, die von Software-Anbietern unterstützt werden, oft nicht geprüft werden und sind darauf angewiesen, dass der Anbieter Schwachstellen ausbessert.

Jede Softwarekomponente hat ihre eigene Lieferkette, da sie sich wiederum auf Bausteine oder zumindest auf Hilfsmittel wie etwa Compiler stützt, die für Menschen lesbaren Quellcode in maschinenlesbaren Binärcode übersetzen. Da Softwareprodukte die Sicherheitsprobleme aller ihrer Bestandteile erben können, ist es zur Bewertung der (Un-)Sicherheit eines bestimmten Softwareprodukts erforderlich, all seine Komponenten und deren Teilkomponenten zu betrachten.

11 SAFECode, *Software Integrity Controls. An Assurance-Based Approach to Minimizing Risks in the Software Supply Chains*, Arlington, 14.6.2010, S. 3, <https://safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf>.

12 Charles W. Krueger, »Software Reuse«, in: *ACM Computing Surveys*, 24 (1992) 2, S. 131–183 (141); Fang Hou / Slinger Jansen, »A Systematic Literature Review on Trust in the Software Ecosystem«, in: *Empirical Software Engineering*, 28 (2023) 1, doi: <10.1007/s10664-022-10238-y>.

13 Krueger, »Software Reuse« [wie Fn. 12].

14 Dazu zählen auch Einzelpersonen oder gemeinnützige Organisationen wie OSS-Stiftungen; der Anschaulichkeit halber ist hier schlicht von Herstellern die Rede.

15 SAFECode, *Software Integrity Controls* [wie Fn. 11], S. 8.

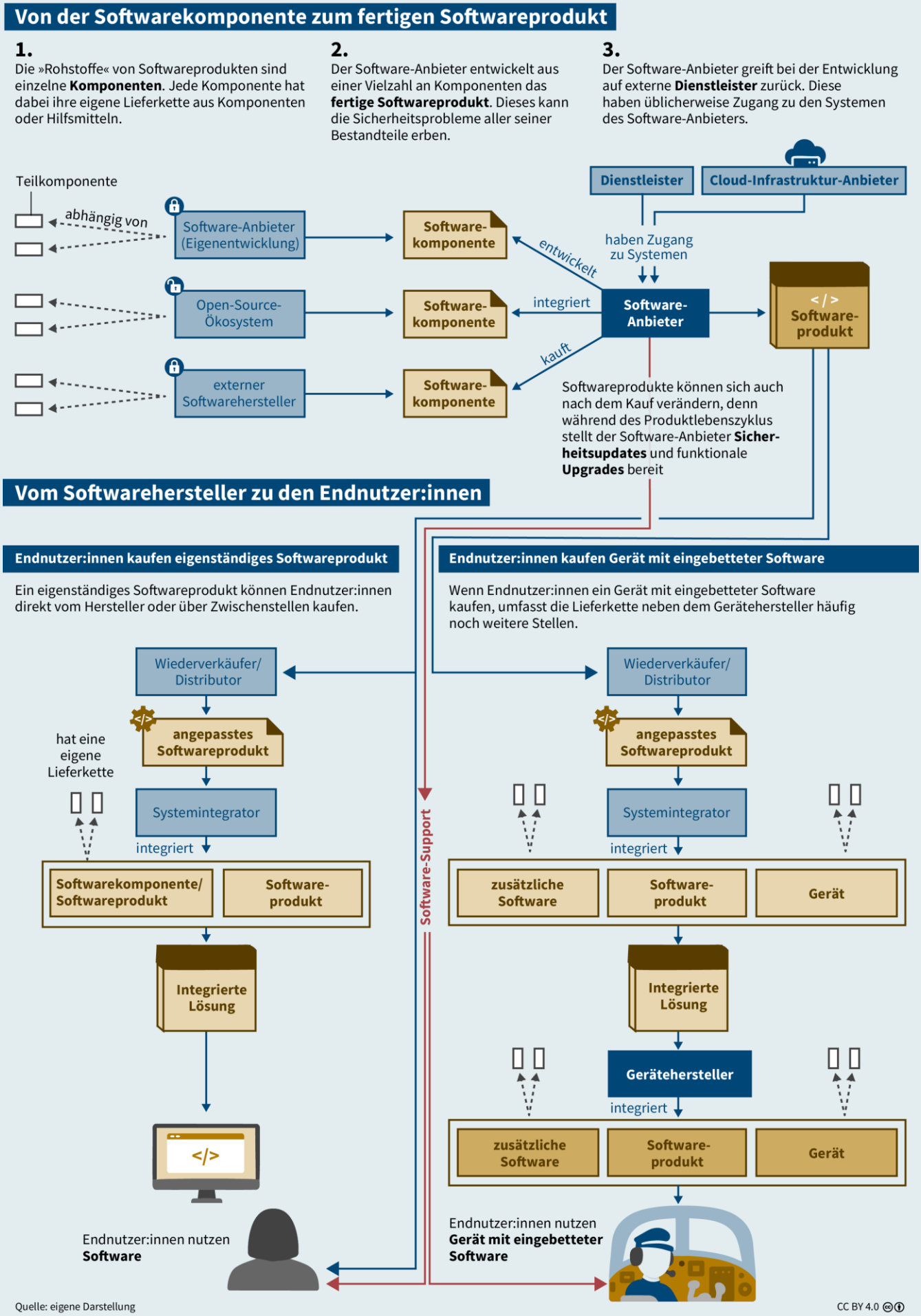
16 Es ist umstritten, ob OSS per Definition für alle frei nutzbar ist (Open Source Initiative, »The Open Source Definition«, 16.2.2024, <https://opensource.org/osd>) oder ob OSS-Lizenzen bestimmte Anwendungsfälle wie eine militärische Nutzung ausschließen können (Steve Dierker / Volker Roth, »Can Software Licenses Contribute to Cyberarms Control?«, in: Marco Carvalho u.a. (Hg.), *Proceedings of the New Security Paradigms Workshop*, New York: ACM, 28.8.2018, S. 41–51, doi: 10.1145/3285002.3285009).

17 Black Duck, *Open Source Security & Risk Analysis Report*, Burlington 2025, <https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html>; Julius Musseau u.a., »Is Open Source Eating the World's Software?«, in: David Lo (Hg.), *Proceedings of the 19th International Conference on Mining Software Repositories*, New York: Association for Computing Machinery, 2022, S. 561–565, doi: 10.1145/3524842.3528473.

18 Klint Finley, »Linux Took Over the Web. Now, It's Taking Over the World«, *Wired*, 25.8.2016, <www.wired.com/2016/08/linux-took-web-now-taking-world/>.

Grafik 1

Die Software-Lieferkette



Quelle: eigene Darstellung

Während des Entwicklungsprozesses greifen Softwarehersteller häufig auf externe Dienstleister zurück. So brauchen etwa Software-as-a-Service-Anbieter (SaaS-Anbieter) Dienstleister, die Cloud-Infrastruktur bereitstellen. Solche Dienstleister haben oft Zugang zu den Systemen ihrer Kund:innen, um ihre Dienste erbringen zu können.

Sobald das Softwareprodukt fertiggestellt ist, muss es seinen Weg zu den Endnutzer:innen finden — beispielsweise zur Bundeswehr. Welchen Weg es nimmt, hängt zunächst davon ab, ob die Nutzer:innen ein reines Softwareprodukt oder ein Gerät mit eingebetteter Software suchen. Die meisten Geräte mit Informations- und Kommunikationsfunktionen enthalten eingebettete Software und haben daher auch immer eine Software-Lieferkette.

Zu einem reinen Softwareprodukt können Endnutzer:innen auf drei Arten Zugang erlangen: Sie können das Produkt kaufen, eine Lizenz zur Nutzung des Produkts erwerben, oder Zugang zu einer in der Cloud gehosteten Version (SaaS) erwerben. Außerdem unterscheiden sich die Lieferketten darin, ob das Produkt (oder das Nutzungsrecht) direkt vom Softwarehersteller bezogen wird oder über Zwischenstellen. Ersteres ist häufig der Fall bei sogenannten Commercial-off-the-Shelf-Softwareprodukten (COTS), also handelsüblichen Lösungen, die nicht speziell an die Bedürfnisse der Endnutzer:innen angepasst werden und häufig direkt von der Website des Anbieters heruntergeladen werden können. Alternativ können auch weitere Unternehmen Teil der Lieferkette sein, wie Wiederverkäufer oder Distributoren, die das Produkt den Endkund:innen zur Verfügung stellen und oft zusätzliche Dienstleistungen wie etwa Anpassungen anbieten, oder Systemintegratoren, die Produkte verschiedener Anbieter kombinieren und an die Bedürfnisse der Kund:innen anpassen.

Kaufen Endnutzer:innen hingegen ein Gerät mit eingebetteter Software, so kaufen sie das Produkt vom entsprechenden Hersteller oder von den jeweiligen Wiederverkäufern, Distributoren oder Systemintegratoren. Der Gerätehersteller wiederum entwickelt die eingebettete Software entweder selbst oder kauft sie von einem oder mehreren Software-Herstellern ein. Im militärischen Kontext kann es sich bei solchen Geräten mit eingebetteter Software sowohl um einfache COTS-Geräte wie Klimaanlagen für Rechenzentren als auch um komplexe Waffensysteme wie Kampfflugzeuge handeln.

Schließlich endet die Software-Lieferkette nicht zum Zeitpunkt des Kaufs (oder Abschluss des Nutzungsvertrags). Vielmehr bieten Software-Hersteller üblicherweise Support für ihre Produkte an, das heißt Sicherheitsupdates und — in einigen Fällen — Upgrades, die Funktionalitäten ändern, hinzufügen oder entfernen. Sicherheitsupdates sind unerlässlich, da die meisten Softwareprodukte Schwachstellen enthalten,[19] also »Schwäche[n] in einem IT-System, die von Angreifer:innen für einen erfolgreichen Angriff ausgenutzt werden können«.[20] Sobald ein Hersteller von einer Schwachstelle erfährt, kann er eine Abhilfemaßnahme bereitstellen, etwa ein Sicherheitsupdate oder Empfehlungen für Konfigurationseinstellungen.

Dieses komplexe Geflecht aus Software-Anbietern, ihren Zulieferern, Dienstleistern und Softwarekomponenten bildet die Lieferkette eines jeden Softwareprodukts.

19 National Cyber Security Centre, *A Method to Assess »Forgivable« vs »Unforgivable« Vulnerabilities*, London, 28.1.2025, <https://www.ncsc.gov.uk/report/a-method-to-assess-forgivable-vs-unforgivable-vulnerabilities>; Black Duck, *Open Source Security & Risk Analysis Report* [wie Fn. 17].

20 National Cyber Security Centre, *Vulnerability Management. Advice, Guidance and Other Resources for Managing Vulnerabilities*, London, 12.2.2024, <https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities>. Bei wörtlichen Zitaten englischsprachiger Quellen handelt es sich um Übersetzungen der Autorin.

Risiken der Software-Lieferkette

Software-Lieferketten bergen eine Reihe von Risiken. Diese unterscheiden sich von anderen Cybersicherheitsrisiken in einem wesentlichen Punkt: Bei »herkömmlichen« Cybersicherheitsvorfällen verschaffen sich Bedrohungsakteur:innen üblicherweise direkt Zugang zu ihrem Ziel und erzielen dort einen Effekt (siehe Grafik 2). So versenden Angreifer:innen beispielsweise eine Phishing-E-Mail, um in das IT-System eines Unternehmens einzudringen und dort Ransomware zu installieren. Im Gegensatz dazu haben Software-Lieferketten-Risiken ihren Ursprung bei einer in der Lieferkette vorgelagerten Stelle. So nutzen Angreifer:innen etwa eine Schwachstelle in den IT-Systemen eines Softwareherstellers aus, um dessen Update-Server unter ihre Kontrolle zu bringen. Daraufhin »kapern« sie den Update-Prozess und fügen Ransomware in das Software-Update ein, das dann auf den Systemen aller Kund:innen des Herstellers installiert wird.[21]

Es gibt drei Übertragungsmechanismen, mit deren Hilfe Software-Lieferketten-Risiken zu nachgelagerten Stellen in der Lieferkette (oft zu den Endnutzer:innen) wandern (siehe Grafik 2):

1. Das Softwareprodukt selbst kann manipuliert werden, sei es zum Zeitpunkt der Installation oder durch Updates.
2. Einzelne Komponenten des Produkts können verändert werden. Im Gegensatz zu 1.) ist hierbei kein Zugriff auf die Systeme des Software-Anbieters nötig, so dass die Übertragung hier noch schwieriger festzustellen ist.
3. Der Zugriff auf das Produkt, der etwa Dienstleistern gewährt wurde, kann missbraucht werden.

Letzteres sehen nicht alle Expert:innen als Problem der *Software*-Lieferkette an, da das betreffende Softwareprodukt oder seine Komponenten in solchen Fällen nicht unbedingt verändert werden; stattdessen stufen sie solche Vorfälle oft als Drittanbieter-Risiko ein. Doch trotz dieses technischen Unterschieds gibt es viele Parallelen zwischen Sicherheitsvorfällen, die sich aus Zugriffsrechten von Dritten ergeben, und solchen, in denen Dritte das Softwareprodukt oder seine Komponenten manipulieren, und vielfach können dieselben Maßnahmen beide Arten von Risiko begrenzen. Daher werden hier auch missbrauchte Zugriffsrechte als Software-Lieferketten-Risiko eingestuft.

Aus Sicht der Endnutzer:innen bringen Software-Lieferketten-Risiken vier spezielle Probleme mit sich: Erstens wirken sich entsprechende Ereignisse häufig auf sehr viele Organisationen gleichzeitig aus — zum Beispiel, wenn alle Kund:innen eines bestimmten Software-Anbieters betroffen sind.[22] Zweitens gibt es in beinahe allen Software-Lieferketten Stellen mit lückenhaften Cybersicherheitsvorkehrungen, wie etwa kleine und mittlere Unternehmen (KMU) oder kleinere OSS-Projekte, die von wenigen oder nur einer Person als Hobby[23] gepflegt werden. Das bedeutet, dass auch Software-Nutzer:innen mit strengen Cybersicherheitsmaßnahmen — wie Streitkräfte — mit hoher Wahrscheinlichkeit über die Lieferketten der von ihnen verwendeten Softwareprodukte angreifbar sind. Drittens haben Endnutzer:innen üblicherweise nur einen begrenzten Einblick in die Lieferkette und wissen daher möglicherweise nicht einmal, dass sie einer Cyberbedrohung ausgesetzt sind. Und viertens

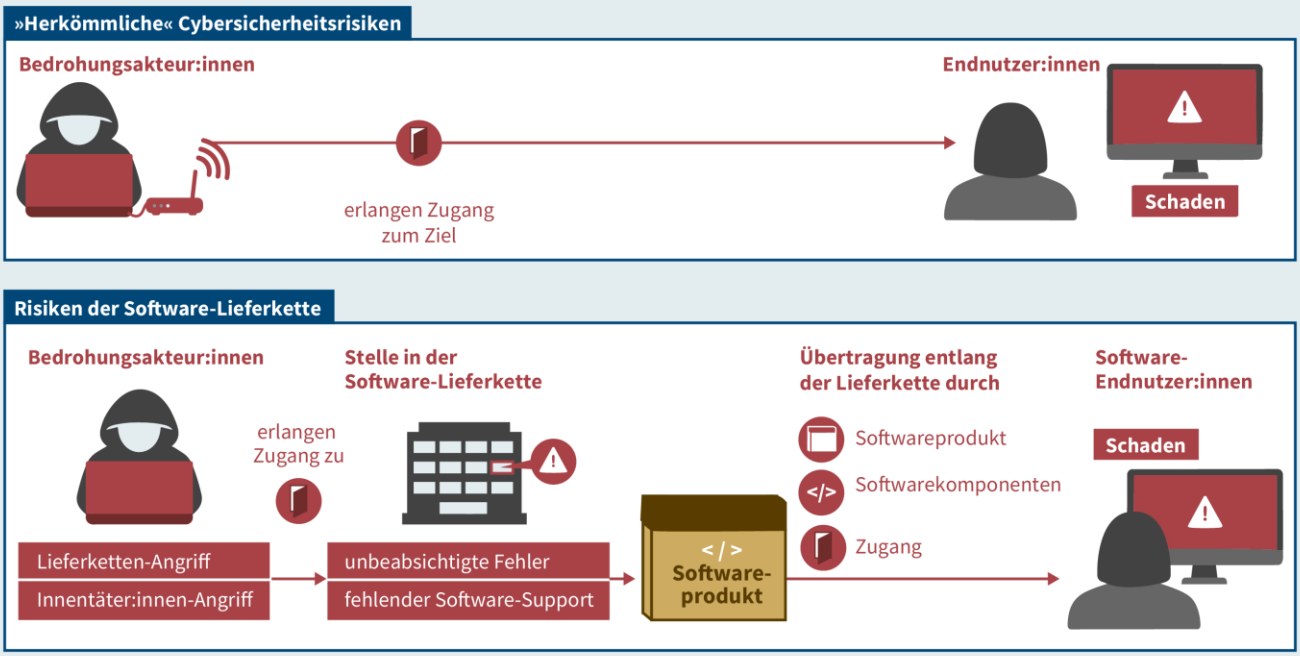
21 Andy Greenberg, »The Untold Story of NotPetya, the Most Devastating Cyberattack in History«, *Wired*, 21.8.2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

22 Trey Herr u.a., *Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain*, Washington, D.C.: Atlantic Council, 26.7.2020, <https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/>.

23 Tidelift, *The 2024 Tidelift State of The Open Source Maintainer Report*, Boston, 2024, S. 4, <https://4008838.fs1.hubspotusercontent-na1.net/hubfs/4008838/2024-tidelift-state-of-the-open-source-maintainer-report.pdf>.

Grafik 2

Risiken der Software-Lieferkette



Quelle: eigene Darstellung

können häufig weder Endnutzer:innen noch ihre unmittelbaren Zulieferer die Ursachen von Software-Lieferketten-Risiken beheben, da das Problem bei weit vorgelagerten Stellen in der Lieferkette (bei kleineren Software-Anbietern, Dienstleistern oder dem OSS-Ökosystem) liegt und nur diese Behebungsmaßnahmen durchführen können.

Diese Probleme machen den Umgang mit Software-Lieferketten-Risiken zu einem dringenden Anliegen für alle Software-Nutzer:innen, insbesondere aber für solche, die — wie Streitkräfte — Wert auf ein hohes Maß an Sicherheit legen. Dabei lassen sich Software-Lieferketten-Risiken in vier Kategorien einteilen: Lieferketten-Angriffe, Angriffe von Innentäter:innen, unbeabsichtigte Fehler und fehlender Software-Support (siehe Grafik 2).

Lieferketten-Angriffe von Dritten

Bei Angriffen von Dritten auf die Lieferkette verschaffen sich Angreifer:innen, die selbst nicht Teil der Lieferkette eines Softwareprodukts sind, Zugang zu einer Stelle in der Lieferkette, um einen Effekt bei einer nachgelagerten Stelle in der Lieferkette zu erzielen.[24]

Angriffe von Innentäter:innen

Angriffe von Innentäter:innen gehen von Akteur:innen aus, die selbst Teil der Lieferkette eines Softwareprodukts sind. In klassischen Szenarien wenden sich Angestellte gegen ihren Arbeitgeber, sei es aus eigenem Antrieb oder unter dem Einfluss von Dritten

24 Alexandra Paulus / Christina Rupp, *Government's Role in Increasing Software Supply Chain Security: A Toolbox for Policy Makers*, Berlin: Interface, März 2023, S. 18, <www.interface-eu.org/publications/governments-role-increasing-software-supply-chain-security-toolbox-policy-makers>. Im Abschnitt »Die Auswirkungen vergangener Software-Lieferketten-Vorfälle auf Streitkräfte« in der vorliegenden Studie, S. 16, werden mit der »Cloud Hopper«-Kampagne, der »Sunburst«-Kampagne und dem Viasat-Vorfall Beispiele für solche Angriffe skizziert.

wie ausländischen Nachrichtendiensten.[25] Auch Veränderungen in der Eigentumsstruktur von Unternehmen können Gelegenheiten für Innentäter:innen bieten, zum Beispiel wenn eine staatliche Stelle die Kontrolle über ein Unternehmen erlangt, das Teil einer bestimmten Lieferkette ist. In international arbeitsteiligen Unternehmen können zudem — über Subunternehmer — Bürger:innen aus gegnerischen Staaten Teil der Software-Lieferkette werden, die nationalen Auskunftspflichten unterliegen oder instrumentalisiert werden können.[26]

Weitere Szenarien ergeben sich aus der besonderen Struktur des OSS-Ökosystems: Da Softwarehersteller, die OSS-Komponenten verwenden, in der Regel deren Entwickler:innen und Maintainer:innen nicht kennen, haben sie einen blinden Fleck in ihrer Lieferkette, der ein Einfallstor für böswillige Innentäter:innen sein kann. Im Fall der »XZ-Hintertür«[27] beispielsweise wurden zwischen 2022 und 2024 eine oder mehrere Unbekannte für die Maintenance der OSS-Komponente »XZ Utils« verantwortlich und fügten eine Hintertür ein.[28] Die beliebte Bibliothek wird unter anderem für den Fernzugriff auf Linux-Server verwendet. Durch diese Hintertür hätten die Verantwortlichen die Kontrolle über die betroffenen Geräte übernehmen können — darunter die meisten Server weltweit.[29] Glücklicherweise wurde der Schadcode dank mehrerer Zufälle zeitnah entdeckt und entfernt, bevor er seine Wirkung entfalten konnte.[30] Doch bösartige OSS-Komponenten sind insgesamt ein weitverbreitetes Problem.[31] Solche Komponenten stehen häufig ganz am Anfang vieler Software-Lieferketten, so dass ein Sicherheitsvorfall enorm weitreichende Auswirkungen haben kann.

Unbeabsichtigte Fehler

Software-Lieferketten-Risiken können auch ohne vorsätzliche Handlungen von Dritten entstehen, etwa durch unbeabsichtigte Fehler von Stellen in der Lieferkette. OSS-Entwickler:innen und -Maintainer:innen machen ebenso Fehler wie die Hersteller proprietärer Software. Diese Fehler können zu Schwachstellen im Softwareprodukt führen, die später von böswilligen Akteur:innen ausgenutzt werden können.[32]

Fehlender Software-Support

Das vierte Risiko, das Software-Lieferketten mit sich bringen, liegt in fehlendem Software-Support durch den Hersteller. Ohne funktionale Upgrades sind manche Produkte mit der Zeit nicht mehr oder nur eingeschränkt nutzbar. Ohne Sicherheitsupdates sammeln sich in Softwareprodukten bekannte, aber nicht behobene Schwachstellen an. Insgesamt wird Software ohne Support also mit der Zeit ein leichtes Angriffsziel. Und wenn SaaS-Anbieter ihre Dienste für alle oder bestimmte Nutzer:innen einstellen, haben diese sogar unmittelbar keinen Zugriff mehr auf die Software.

Der Support für Softwareprodukte kann aus verschiedenen Gründen enden oder fehlen: Weil die Nutzer:innen nicht (mehr) für die Produktwartung

25 Siehe etwa Codi Starks u.a., »Staying a Step Ahead: Mitigating the DPRK IT Worker Threat«, *Google Cloud Blog*, 23.9.2024, <https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat>.

26 Camilla Turner, »Britain's Nuclear Submarine Software Built by Belarusian Engineers«, in: *The Telegraph*, 2.8.2024, <https://www.telegraph.co.uk/news/2024/08/02/britains-nuclear-submarine-software-designed-russia-belarus/>; Renee Dudley, »A Little-Known Microsoft Program Could Expose the Defense Department to Chinese Hackers«, *ProPublica*, 15.7.2025, <https://www.propublica.org/article/microsoft-digital-escorts-pentagon-defense-department-china-hackers>.

27 Dieser Vorfall wird im Abschnitt »Die Auswirkungen vergangener Software-Lieferketten-Vorfälle auf Streitkräfte«, S. 16, genauer skizziert.

28 Evan Boehs, »Everything I Know About the XZ Backdoor«, *Evan Boehs* (online), 29.3.2024, <https://boehs.org/node/everything-i-know-about-the-xz-backdoor>.

29 Thomas Roccia, »The XZ Backdoor Story«, *Speaker Deck* (online), 8.9.2024, <https://speakerdeck.com/fr0gger/the-xz-backdoor-story>; Sarah Fluchs, »Almost a Master Key to the Internet: The XZ Utils Backdoor«, *Industrial Cyber* (online), 28.5.2024, <https://industrialcyber.co/news/almost-a-master-key-to-the-internet-the-xz-utils-backdoor/>; Bruce Schneier, »Backdoor in XZ Utils that Almost Happened«, in: *Lawfare*, 9.4.2024, <https://www.lawfaremedia.org/article/backdoor-in-xz-utils-that-almost-happened>.

30 Kevin Roose, »Did One Guy Just Stop a Huge Cyberattack?«, in: *The New York Times*, 3.4.2024, <https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html>.

31 Sonatype, *2024 State of the Software Supply Chain*, Fulton 2024, S. 31ff, <https://www.sonatype.com/state-of-the-software-supply-chain/introduction>.

32 Mit dem Crowdstrike-Vorfall von 2024 wird im Abschnitt »Die Auswirkungen vergangener Software-Lieferketten-Vorfälle auf Streitkräfte«, S. 16, ein Beispiel für einen solchen Vorfall dargestellt.

zahlen; weil der Hersteller den Support einstellt;[33] weil der Hersteller in Konkurs geht oder die (oft einzige[34]) Person, die ein OSS-Projekt pflegt, die Arbeit daran aufgibt; oder weil der Hersteller den Support für bestimmte Endnutzer:innen abbricht, zum Beispiel als Folge von Sanktionen. Und selbst wenn ein Anbieter ein Produkt noch unterstützt, kann es sein, dass eine eingebettete OSS-Komponente nicht mehr gewartet wird — der Anbieter weiß das aber möglicherweise nicht.

33 Anbieter machen manchmal Ausnahmen im Rahmen von bezahlten Servicevereinbarungen oder nach der Entdeckung extrem kritischer Schwachstellen.

34 Tidelift, *The 2024 Tidelift State of The Open Source Maintainer Report* [wie Fn. 23], S. 6.

Die besondere Bedrohung von Streitkräften

Die vier Arten von Software-Lieferketten-Risiken können alle Organisationen betreffen, doch Streitkräfte sind besonders verwundbar.

Bedeutung von Software für Streitkräfte

Streitkräfte nutzen ein breites Portfolio verschiedener Softwareprodukte (siehe Grafik 3). Dabei verwenden sie einerseits, wie zivile Organisationen, Software zur Prozessunterstützung und zur Verarbeitung von Informationen. Zu diesen unterstützenden Anwendungen gehören beispielsweise Office-Programme oder Warenwirtschaftssysteme. Andererseits brauchen Streitkräfte Gefechtsfeldanwendungen wie Lagebildplattformen oder Führungssysteme. Darüber hinaus arbeiten Streitkräfte mit Verschlusssachen und die Systeme, die solche Daten verarbeiten, müssen besondere Sicherheitsanforderungen erfüllen. Schließlich sind all diese Anwendungen auf eine ganze Reihe anderer Softwaretypen angewiesen, wie etwa Betriebssysteme und Datenbanken.

Kurz gesagt: Software ist für die meisten militärischen Aktivitäten unverzichtbar. Auch der Großteil militärischen Geräts ist auf Software angewiesen. So ermöglicht Software häufig Funktionserweiterungen, etwa von Waffensystemen wie Kriegsschiffen, deren Lebensdauer dadurch verlängert werden kann. Folglich tangieren Software-Lieferketten-Risiken das gesamte Spektrum militärischer Aktivitäten. Die Auswirkungen entsprechender Vorfälle hängen dabei von der Art der betroffenen Software ab. Selbst die Kompromittierung eines COTS-Produkts kann Nachrichtendiensten wertvolle Informationen liefern, aber Sabotageoperationen sind viel gefährlicher, wenn sie auf Gefechtsfeldanwendungen wie Waffensysteme abzielen.

Die Abhängigkeit wird weiter zunehmen

Software spielt auch heute schon eine wichtige Rolle in Waffensystemen. Allerdings sind diese Großgeräte bisher nur begrenzt vernetzt — miteinander, mit Sensoren und mit Netzwerken wie dem Internet.[35] Zu einem gewissen Grad mindert diese mangelnde Vernetzung bestehende Software-Lieferketten-Risiken.[36]

Streitkräfte, die ohne Software ihren Auftrag nicht erfüllen können, werden den Risiken der Software-Lieferkette noch stärker ausgesetzt sein.

Doch viele Streitkräfte, darunter die Bundeswehr, streben danach, ihre Prozesse noch stärker zu digitalisieren, immer mehr Geräte noch intensiver zu vernetzen und Software ins Zentrum des Gefechtsfelds zu stellen. Das Konzept »Software-defined Defense« (SDD)[37] beschreibt eine Zukunft, in der militärisches Großgerät über eine zentrale Softwareplattform gesteuert werden kann und die Funktionalität militä-

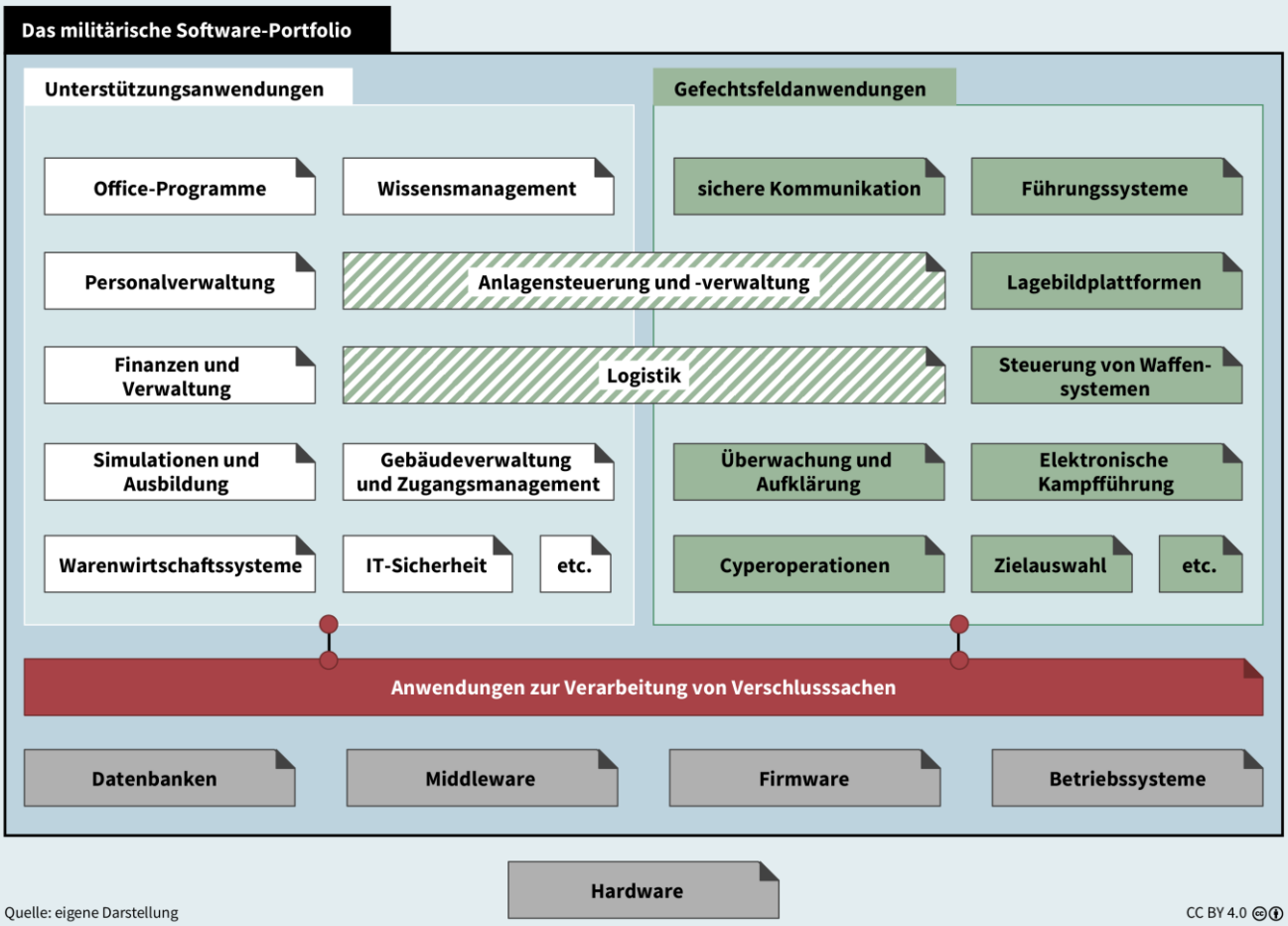
35 Christian Brose, *The Kill Chain. Defending America in the Future of High-Tech Warfare*, New York: Hachette Books, 2020.

36 Der »Stuxnet«-Vorfall hat jedoch gezeigt, dass auch »Air-gapped«-Systeme anfällig für Angriffe sein können, siehe Kim Zetter, *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon*, New York: Crown Publishers, 2014.

37 Mulchandani / Shanahan, *Software-Defined Warfare* [wie Fn. 7]; Soare u.a., *Software-defined Defence* [wie Fn. 7]; *Software Defined Defence. Positionspapier des BDSV, BDLI, Bitkom und BMVg*, Berlin, 31.10.2023, <https://www.bmvg.de/resource/blob/5711942/6fb70a45412601fdf03f63aeebf72451/cyber-defined-defence-papier-data.pdf>. Zuvor wurden ähnliche Ideen unter dem Begriff der netzwerkzentrierten Kriegsführung diskutiert, siehe z. B. Arthur K. Cebrowski / John J. Garstka, »Network-Centric Warfare: Its Origin and Future«, in: *Proceedings of the Naval Institute*, 124 (1998), S. 28—35.

Grafik 3

Das militärische Software-Portfolio



Quelle: eigene Darstellung

rischer Ausrüstung durch Software-Updates anstelle von Hardware-Modifikationen verändert wird.

Noch sind die meisten Streitkräfte weit davon entfernt, dieses Konzept umzusetzen,[38] doch einige haben bereits erste Schritte in diese Richtung unternommen.[39] Das Konzept erlaubt daher Rückschlüsse auf die Bedeutung von Software für die Streitkräfte von morgen. Streitkräfte, die ohne Software als Rückgrat ihren Auftrag nicht erfüllen können, werden den Risiken der Software-Lieferkette noch stärker ausgesetzt sein.

38 Soare u.a., *Software-defined Defence* [wie Fn. 7], S. 3f.

39 Emelia Probasco, *Building the Tech Coalition. How Project Maven and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense*, Washington, D.C.: Center for Security and Emerging Technology (CSET), August 2024, <https://cset.georgetown.edu/publication/building-the-tech-coalition/>.

Verschärfte Bedrohung durch militärische Besonderheiten

Darüber hinaus erhöhen vier militärische Besonderheiten die Software-Lieferketten-Risiken für Streitkräfte. Erstens ist deren oberste Aufgabe die Kriegsverhütung, basierend auf der Fähigkeit zur wirksamen Kriegsführung. Dementsprechend können Lieferketten-Angriffe Menschen, Infrastruktur und Ressourcen in Gefahr bringen. Diese Gefährdung kann unmittelbar sein, etwa durch einen Angriff auf Software, die Waffensysteme steuert, aber auch indirekt, indem beispielsweise gegnerische Nachrichtendienste Informationen über Stützpunkte sammeln. Da militärische Betriebsabläufe auch unter außergewöhnlichen Umständen funktionieren müssen, können auch unbeabsichtigte Fehler — die beispielsweise die Logistiksysteme stören — oder fehlender Software-Support dramatische Folgen haben.

Zweitens sind Streitkräfte häufig von IT-Systemen abhängig, die anderen gehören und von diesen betrieben werden.[40] Bei der Landesverteidigung ist die militärische Logistik oft auf zivile kritische Infrastrukturen angewiesen und steht mit diesen in enger Wechselwirkung,[41] und bei der Bündnisverteidigung gilt Ähnliches für die Systeme der Verbündeten. Dementsprechend stehen Streitkräfte vor dem Problem, dass sie Teile ihrer Software-Lieferkette weder kennen noch in diesem Bereich selbst Risikomanagement betreiben können.

Drittens kauft das Militär nicht nur militärisches Gerät, sondern auch Software häufig bei spezialisierten Herstellern ein und ist dann von diesen Anbietern und ihren proprietären Technologien abhängig (»vendor lock-in«).[42] Diese Abhängigkeit bringt die Streitkräfte in eine schwache Verhandlungsposition gegenüber ihren Anbietern, wenn es beispielsweise darum geht, striktere Maßnahmen für den Umgang mit Risiken der Software-Lieferkette durchzusetzen. Außerdem haben Streitkräfte oft keine Alternative, wenn kein Software-Support (mehr) bereitgestellt wird.

Viertens müssen Streitkräfte bei der Beschaffung von Software Beschaffungsregeln befolgen (auch auf EU-Ebene).[43] Diese Beschaffungsprozesse sind nicht nur langsam und involvieren viele Stellen, sondern sie wurden auch für Hardware — nämlich Waffensysteme — entwickelt und lassen daher oft die Geschwindigkeit und Flexibilität vermissen, die für die Beschaffung von Software entscheidend sind.

Zusammenfassend lässt sich sagen, dass Software-Lieferketten-Risiken zwar alle Organisationen betreffen, ihre potentiellen Auswirkungen für das Militär jedoch besonders gravierend sind.

Die Auswirkungen vergangener Software-Lieferketten-Vorfälle auf Streitkräfte

Die Streitkräfte verschiedener Staaten haben bereits die verheerende Wirkung von Software-Lieferketten-Vorfällen zu spüren bekommen (siehe Grafik 4). Dabei kam es sowohl zu Beeinträchtigungen von Betriebsabläufen als auch zu Angriffen, die der Spionage und Sabotage dienten.

Beeinträchtigung von Betriebsabläufen

Selbst unbeabsichtigte Fehler von Softwareherstellern können die Betriebsabläufe von Organisationen weltweit zum Erliegen bringen: Im Jahr 2024 veröffentlichte das US-amerikanische Software-Unternehmen CrowdStrike, das sich auf Cybersicherheitsanwendungen spezialisiert, ein fehlerhaftes automatisches Update für alle Kunden weltweit, die seine Software »Falcon« verwenden.[44] Geräte, die das Update erhalten hatten, starteten automatisch neu und erlitten während des Starts einen Systemabsturz, so dass sie vorübergehend nicht mehr funktionsfähig waren. Die schätzungsweise 8,5 Millionen betroffenen Geräte weltweit mussten manuell zurückgesetzt werden, was bei Geräten mit Festplattenverschlüsselung sogar physischen Zugang zu jedem einzelnen Gerät erforderte.[45] Das US-Verteidigungsministerium und

40 Bundeswehr, *Operationsplan Deutschland. Eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe*, Berlin 2025, <https://www.bundeswehr.de/resource/blob/5920008/5eb62255741addec3f38d49a443d0282/booklet-operationsplan-deutschland-data.pdf>.

41 Defense Management Institute, *Department of Defense Dependencies on Critical Infrastructure*, Alexandria, 27.9.2024, <https://www.dmi-ida.org/knowledge-base-detail/Department-of-Defense-Dependencies-on-Critical-Infrastructure-Executive-Summary>; Annie Fixler u.a., *Military Mobility Depends on Secure Critical Infrastructure*, Washington, D.C.: Cyberspace Solarium Commission 2.0, 27.3.2025, <https://cybersolarium.org/csc-2-0-reports/military-mobility-depends-on-secure-critical-infrastructure/>.

42 Lai Xu / Sjaak Brinkkemper, »Concepts of Product Software«, in: *European Journal of Information Systems*, 16 (2007) 5, S. 531—541.

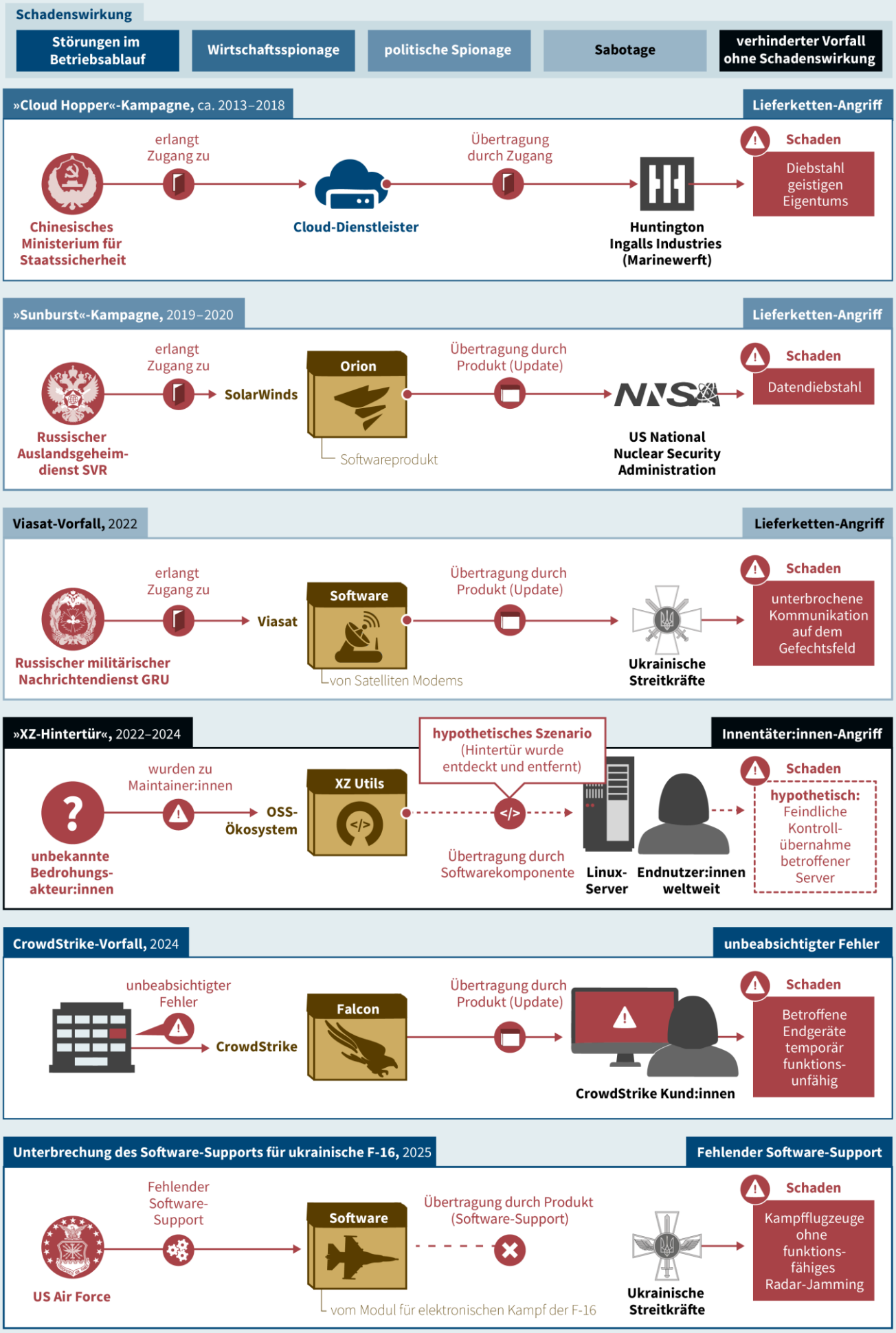
43 Dazu zählen BMVg, *Projektbezogene Bedarfsdeckung und Nutzung. A-1500/3*, Berlin, 23.5.2024, <www.bundeswehr.de/resource/blob/133334/d5cdf4ad42eaa94618f429ad06a684e3/pbn-data.pdf>; Europäisches Parlament und Rat, *Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit und zur Änderung der Richtlinien 2004/17/EG und 2004/18/EG*, Brüssel, 25.6.2025, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32009L0081>.

44 »Remediation and Guidance Hub: Channel File 291 Incident«, *CrowdStrike*, 6.8.2024, <https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/>.

45 James Coker, »CrowdStrike Fault Causes Global IT Outages«, *Infosecurity Magazine*, 19.7.2024, <www.infosecurity-magazine.com/news/crowdstrike-fault-it-outages/>; David Weston, »Helping Our Customers through the CrowdStrike Outage«, *Official Microsoft Blog*, 20.7.2024, <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>.

Grafik 4

Wichtige Software-Lieferketten-Vorfälle im militärischen Bereich



Quelle: eigene Darstellung

mehrere Verteidigungsunternehmen nutzten »Falcon«,[46] aber es gab »keine Auswirkungen auf den Betrieb des US-Verteidigungsministeriums«.[47] Dennoch zeigte der Vorfall, welche Folgen selbst ein versehentlicher Fehler eines Unternehmens in der Software-Lieferkette haben kann.

Darüber hinaus wird gewisses militärisches Gerät ohne regelmäßige Software-Upgrades unbrauchbar: Das ukrainische Militär verfügt über F-16-Kampfflugzeuge, deren Modul für elektronischen Kampf Radar-Jamming während des Flugs ermöglicht.[48] Diese Fähigkeit verhindert, dass gegnerische Bodenstationen ein Flugzeug ins Visier nehmen, um es mit Raketen abzuschießen. Für eine wirksame Störung des Radars muss die entsprechende Software regelmäßig auf die — mit der Zeit wechselnden — Radarfrequenzbereiche angepasst werden, die von den gegnerischen Bodenstationen verwendet werden. Ohne diese Upgrades würden die Flugzeuge ihre Abwehrfähigkeit verlieren und müssten mutmaßlich am Boden bleiben.[49] Für die ukrainischen F-16 ist bisher nur die US-Luftwaffe in der Lage, diese Software-Updates bereitzustellen.[50] Im März 2025 stellte die Trump-Regierung ihre Militärhilfe für die Ukraine vorübergehend ein, wozu auch der Software-Support für die F-16 gehörte.[51] Obwohl die Trump-Administration ihren Kurs zügig wieder änderte,[52] zeigt diese Episode, welche Folgen mangelnder Software-Support für die Einsatzbereitschaft großer Waffensysteme hat.

Wirtschaftsspionage, politische Spionage und Sabotage

Neben diesen Fällen, in denen ganz ohne Angreifer:innen große Schäden entstehen können, bietet die Software-Lieferkette auch Einfallstore für böswillige Akteure, die es auf Streitkräfte oder die Rüstungsindustrie abgesehen haben (siehe Grafik 4). Erstens betreiben staatliche Akteur:innen oder private Unternehmen Wirtschaftsspionage. Sie stehlen also geistiges Eigentum. Zwischen mindestens 2013 und 2018 stahlen Personen, die mit dem chinesischen Ministerium für Staatssicherheit in Verbindung stehen, im Rahmen der »Cloud Hopper«-Kampagne geistiges Eigentum von westlichen Unternehmen. Dabei infiltrierten sie Cloud-Anbieter und nutzten deren Zugang zu den Systemen ihrer Kunden aus.[53] Zu den Zielen der Kampagne gehörte Huntington Ingalls Industries, die größte Marinewerft der USA, die unter anderem nuklear angetriebene U-Boote für die US Navy baut.[54]

Zweitens führen Geheimdienste politische Spionage durch. Zwischen 2019 und 2020 schleuste der russische Auslandsgeheimdienst SVR im Rahmen der »Sunburst«-Kampagne Schadsoftware in Updates des

46 »CrowdStrike Achieves IL5 Authorization to Secure U.S. Department of Defense«, Pressemitteilung, *CrowdStrike*, 31.5.2023, <https://www.crowdstrike.com/en-us/press-releases/crowdstrike-achieves-il5-authorization-to-secure-us-dod/>.

47 Carley Welch, »Joint Chiefs Chairman Says DoD Operations not Affected by Widespread CrowdStrike ›Glitch‹«, *Breaking Defense*, 19.7.2024, <http://breakingdefense.com/2024/07/joint-chiefs-chairman-says-dod-operations-not-affected-by-widespread-crowdstrike-glitch/>.

48 »F-16 Fighting Falcon«, *United States Air Force*, September 2021, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104505/f-16-fighting-falcon/>.

49 David Axe, »France to the Rescue! French-Made Mirage 2000 Jets Could Become Ukraine's Most Important Aerial Radar Jammers«, in: *Forbes*, 7.3.2025, <www.forbes.com/sites/davidaxe/2025/03/07/france-to-the-rescue-french-made-mirage-2000-jets-could-become-ukraines-most-important-aerial-radar-jammers/>; Justin Bronk, *Airborne Electromagnetic Warfare in NATO: A Critical European Capability Gap*, London: Royal United Services Institute (RUSI), 19.3.2025, <https://www.rusi.org/explore-our-research/publications/occasional-papers/airborne-electromagnetic-warfare-nato-critical-european-capability-gap>.

50 Benjamin Aronson, »Dominate the Spectrum: 350th SWW Enables EW Capabilities for Ukrainian F-16s«, *Air Combat Command*, 26.8.2024, <https://bit.ly/3IBP4bi>; US Defense Security Cooperation Agency, *Ukraine – F-16 Sustainment Services*, 10.12.2024, <https://www.dsca.mil/Press-Media/Major-Arms-Sales/Article-Display/Article/4009609/ukraine-f-16-sustainment-services>.

51 Axe, »France to the Rescue!« [wie Fn. 49].

52 »After Trump's Freeze, US Military Aid to Ukraine Resumes — Poland Confirms«, *Kyiv Post*, 12.3.2025, <https://www.kyivpost.com/post/48761>.

53 U.S. Department of Justice, *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, Washington, D.C., 20.12.2018, <https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>; PwC UK/BAE, *Operation Cloud Hopper*, London, April 2017, <https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf>.

54 Jack Stubbs u.a., »Stealing Clouds«, *Reuters*, 26.6.2019, <https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/>.

Unternehmens SolarWinds ein.[55] Dessen Software »Orion« dient zur Überwachung und Verwaltung von Infrastrukturen. Über den bösartigen Code, der per Update an die »Orion«-Nutzer:innen verteilt wurde, verschaffte sich der SVR unter anderem Zugang zum US-Verteidigungsministerium und zur National Nuclear Security Administration, die das US-Atomwaffenarsenal verwaltet.[56]

Drittens nutzen Nachrichtendienste oder Streitkräfte Schwachstellen in Software-Lieferketten zu Sabotagezwecken aus, um Netzwerke, Systeme oder Dienste vorübergehend zu stören oder dauerhaft zu zerstören. So kaperte etwa der russische Militärgeheimdienst GRU den Update-Mechanismus des Satellitenkommunikationsanbieters Viasat.[57] Am 24. Februar 2022 — dem ersten Tag der russischen Vollinvasion der Ukraine — verschickte der GRU per automatischem Update Schadsoftware an die Modems von Viasat-Kund:innen.[58] Diese überschrieb wichtige Daten im Speicher der Modems und machte die Geräte dadurch funktionsunfähig.[59] Mutmaßliches Ziel dieser Operation waren die ukrainischen Streitkräfte, die Viasats Dienste für ihre Konnektivität auf dem Gefechtsfeld nutzten. Die genauen Auswirkungen des Angriffs sind unklar, unter anderem, weil die ukrainischen Streitkräfte auch Zugang zu den Satellitenkommunikationsdiensten des Unternehmens Starlink hatte.[60]

Zudem ist denkbar, dass Cyberkriminelle militärische Ziele anvisieren, um einen finanziellen Vorteil zu erzielen. Bisher wurden allerdings keine finanziell motivierten Software-Lieferketten-Angriffe auf militärische Ziele öffentlich bekannt. Das mag daran liegen, dass diese in der Regel besser gesichert sind als andere Sektoren und Regierungsstellen oft nicht mit Kriminellen verhandeln (etwa über Ransomware-Zahlungen). Außerdem werden solche Angriffe auf militärische Ziele häufig nicht publik gemacht. Daher ist davon auszugehen, dass viele Vorfälle schlicht nicht veröffentlicht sind — und möglicherweise auch bekannte Vorfälle eine nicht öffentlich bekannte militärische Dimension hatten.

Schließlich ist der Weg über die Software-Lieferkette für Angriffe auf militärische Ziele nicht immer das Mittel der Wahl. Für Spionage- oder Sabotageoperationen kann es einfacher sein, Innentäter:innen schlicht durch Bezahlung oder Erpressung zu gewinnen. Und um militärische Ziele in einem bewaffneten Konflikt zu erreichen, ist es oft günstiger und schneller, gegnerische Stellungen mit kinetischen Mitteln auszuschalten als durch Cyberoperationen.[61]

55 Trey Herr u.a., *Broken Trust: Lessons from Sunburst*, Washington, D.C.: Atlantic Council, 29.3.2021, <https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst>.

56 Adam Janofsky, »Cyber Command: ›No Evidence‹ that SolarWinds Attackers Compromised DoD Networks«, *The Record*, 17.11.2022, <https://therecord.media/cyber-command-no-evidence-that-solarwinds-attackers-compromised-dod-networks>; Natasha Bertrand / Eric Wolff, »Nuclear Weapons Agency Breached Amid Massive Cyber Onslaught«, in: *Politico*, 17.12.2020, <https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855>; Herr u.a., *Broken Trust* [wie Fn. 55].

57 »Russia Behind Cyber-Attack with Europe-Wide Impact an Hour Before Ukraine Invasion«, *Foreign, Commonwealth & Development Office*, London, 10.5.2022, <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion>; Nick Saunders u.a., »Space Cybersecurity Incident Response Framework: A Viasat Case Study«, in: *2025 IEEE Aerospace Conference*, S. 1—15, doi: <https://doi.org/10.1109/AERO63441.2025.11068784>.

58 Saunders u.a., »Space Cybersecurity Incident Response Framework« [wie Fn. 57]; Katrina Manson, »The Satellite Hack Everyone Is Finally Talking About«, *Bloomberg*, 1.3.2023, <https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/>.

59 Juan Andres Guerrero-Saade / Max van Amerongen, »AcidRain: A Modem Wiper Rains Down on Europe«, *SentinelOne*, 31.3.2022, <https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/>.

60 Dustin Volz, »Russian Hackers Tracked Ukrainian Artillery Units Using Android Implant: Report«, *Reuters*, 22.12.2016, <https://www.reuters.com/article/technology/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU/>; Jon Bateman, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Washington, D.C.: Carnegie Endowment for International Peace, 16.12.2022, <https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en>.

61 Lennart Maschmeyer, *Subversion. From Covert Operations to Cyber Conflict*, New York: Oxford University Press, 2024, doi: 10.1093/oso/9780197745854.001.0001; Matthias Schulze / Mika Kerttunen, *Cyber Operations in Russia's War Against Ukraine. Uses, Limitations, and Lessons Learned so Far*, Berlin: Stiftung Wissenschaft und Politik, April 2023 (SWP Comment 23/2023), doi: 10.18449/2023C23; Frederik A. Pedersen / Jeppe T. Jacobsen, »Narrow Windows of Opportunity: The Limited Utility of Cyber Operations in War«, in: *Journal of Cybersecurity*, 10 (2024) 1, doi: 10.1093/cybsec/tyae014.

Wie sich Streitkräfte selbst vor Risiken der Software-Lieferkette schützen können

Vergangene Vorfälle zeigen, dass Risiken der Software-Lieferkette die Kriegstüchtigkeit der Bundeswehr beeinträchtigen können. Angesichts dessen sollte die Bundeswehr die Risiken erkennen und Handlungsmöglichkeiten identifizieren und bewerten.

Die in diesem und dem folgenden Kapitel dargestellten Maßnahmen sind das Ergebnis einer Analyse, die in drei Schritten erfolgt. Zunächst wird auf Basis der zuvor herausgearbeiteten Risiken und unter Berücksichtigung der besonderen Bedrohung von Streitkräften festgestellt, welche Sicherheitsprobleme bestehen. Anschließend wird, sofern möglich, durch einen internationalen Vergleich geprüft, mit welchen Maßnahmen andere Streitkräfte bereits Erfahrungen gesammelt haben. Zumeist liegen solche Erfahrungswerte nicht vor; in dem Fall wird zurückgegriffen auf die Empfehlungen internationaler Expert:innen, die in mehr als 65 Interviews und einem Workshop eingeholt wurden.[62] Und schließlich werden vor dem Hintergrund der internationalen Erfahrungen und der Meinungen von Expert:innen Empfehlungen ausgesprochen, welche Maßnahmen BMVg und Bundeswehr umsetzen sollten.

Die Maßnahmen setzen dabei an zwei Stellen an. Erstens können Streitkräfte bei ihren eigenen Aktivitäten beginnen und selbst Maßnahmen ergreifen, um sich zu schützen. Die dazu notwendigen Schritte (siehe Grafik 5) werden in diesem Kapitel skizziert. Zweitens können Politik und Streitkräfte Vorgaben für Software-Anbieter entwickeln, wie diese ihre Produkte weniger anfällig für diese Risiken gestalten und außerdem Streitkräfte bei ihrem Risikomanagement unterstützen können. Wie entsprechende Vorgaben aussehen können und auf welchen Wegen Politik und Streitkräfte die Anbieter dazu bringen können, sie auch umzusetzen, wird im folgenden Kapitel erläutert. Für einen effektiven Umgang mit militärischen Software-Lieferketten-Risiken müssen beide Ansätze — die ohnehin komplementär sind — miteinander kombiniert werden.

Die im Folgenden vorgeschlagenen Maßnahmen würden für viele Streitkräfte tiefgreifende Veränderungen mit sich bringen und erhebliche Ressourcen erfordern. Dementsprechend ist es denkbar, dass in einigen Fällen Widerstand aufkommt. In solchen Fällen können die Maßnahmen zunächst im kleinen Maßstab in einer geeigneten militärischen Einheit getestet werden.[63]

Festlegung des angemessenen Schutzniveaus

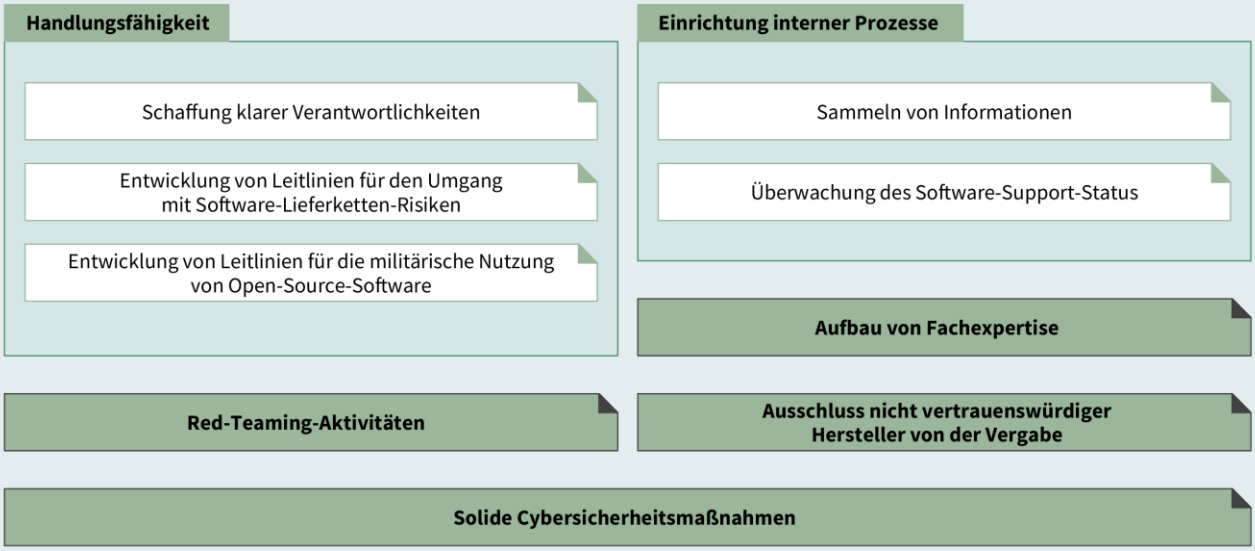
Auch wenn die Auswirkungen von Risiken der Software-Lieferkette verheerend sein können, kann die Antwort der Bundeswehr nicht lauten, gänzlich auf Software zu verzichten oder Abhängigkeiten von Dritten in der Software-Lieferkette vollständig zu vermeiden. Angesichts der Komplexität des Software-Ökosystems wäre ein solcher Ansatz kaum realisierbar und höchst ineffizient. Stattdessen sollte die Bundeswehr zu einem bewussten Umgang mit den Risiken gelangen.

62 Zu den Teilnehmenden des Workshops, denen die Autorin zu großem Dank verpflichtet ist, zählen Amy Ertan, Andrew Dwyer, Chris Wysopal, Christoph Lobmeyer, Clotilde Bômont, Colin Topping, Daniel Voelsen, James Shires, John Scott, John Speed Meyers, Jörg Eschweiler, Marc Lanouette, Philip Engelmartin, Sara Ann Bracket, Sebastian Lange und Simon Stanley.

63 Probasco, »Building the Tech Coalition« [wie Fn. 39], S. 9.

Grafik 5

Wie sich Streitkräfte selbst vor Risiken der Software-Lieferkette schützen können



Quelle: eigene Darstellung

Dabei müssen Politik und Bundeswehr eine grundlegende Güterabwägung vornehmen.[64] Einerseits sollte militärisch genutzte Software nur bekannte und akzeptable Sicherheitsrisiken aufweisen; andererseits sollte sie eine bestimmte Funktionalität bereitstellen, zu einem angemessenen Preis erhältlich sein und schnell eingesetzt und aktualisiert werden können. Hier gilt es, Entscheidungen zu treffen, da diese Ziele oft im Konflikt stehen: Viele Maßnahmen, die Software-Lieferketten-Risiken reduzieren, machen das Produkt teurer, beispielsweise wenn statt einer verfügbaren OSS-Komponente eine Funktionalität von Grund auf neu entwickelt wird. Zudem verlangsamen viele Risikomanagement-Maßnahmen den Beschaffungs- und Bereitstellungsprozess. Das ist beispielsweise der Fall, wenn Streitkräfte Sicherheitstests für Updates durchführen, bevor sie sie in der Fläche ausrollen, oder wenn sie (unter hohem Personalaufwand[65]) vor der Nutzung eines Produkts Schwachstellen in darin verwendeten OSS-Komponenten schließen.

In der Bundeswehr gibt es nicht die eine maßgebliche Instanz, die für die Beschaffung und das Management von Software verantwortlich ist.

Es geht also nicht darum, Software-Lieferketten-Risiken um jeden Preis zu senken. Ein Softwareprodukt mit sehr geringem Risiko ist nutzlos, wenn es nicht die benötigte Funktionalität bietet, zu teuer ist oder schlicht zu spät bereitgestellt oder aktualisiert wird. Stattdessen müssen BMVg und Bundeswehr gemeinsam festlegen, welches Schutzniveau angestrebt werden soll. Mit Blick auf das diverse militärische Software-Portfolio sollte das anvisierte Schutzniveau je nach Software-Typ differenziert werden. So erfordern etwa Produkte, die auf dem Gefechtsfeld genutzt werden oder die der Verarbeitung von Verschlusssachen dienen, mehr Schutzmaßnahmen. Entsprechend sollten die genannten Maßnahmen zielgerich-

64 Eine weitere Abwägung, nämlich ob Streitkräfte sich primär auf den Umgang mit den Risiken in den eigenen Software-Lieferketten oder auf die Ausnutzung von Schwachstellen in gegnerischen Software-Lieferketten konzentrieren sollten, kann hier nicht diskutiert werden; die Argumente ähneln aber der Debatte zum Umgang mit Software-Schwachstellen allgemein, siehe etwa Sven Herpig, *Schwachstellen-Management für mehr Sicherheit. Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte*, Berlin: Interface, August 2018, <https://www.interface-eu.org/storage/archive/files/vorschlag.schwachstellenmanagement.pdf>.

65 John S. Meyers, »How to Fix the Military's Software SNAFU«, *Defense One*, 4.4.2024, <https://www.defenseone.com/ideas/2024/04/how-fix-militarys-software-snafu/395489/>.

tet auf Softwareprodukte in bestimmten Einsatzbereichen angewandt werden.

Handlungsfähigkeit

Der erste Schritt hin zu einem wirkungsvollen Umgang mit Software-Lieferketten-Risiken ist, handlungsfähig zu werden: Verteidigungsministerium und Streitkräfte sollten speziellen Stellen und Personen klare Rollen und Verantwortlichkeiten für das Thema zuweisen und Leitlinien entwickeln, die entsprechende Prioritäten festlegen. Auch wenn sich eine Streitkraft wohl kaum nur mit Blick auf die Begrenzung der Risiken, die mit Software-Lieferketten verknüpft sind, umstrukturieren wird, sollte die Problematik doch oben auf der Agenda stehen, sobald eine Reorganisation ansteht. Die derzeitige Reorganisation des Bereichs Cyber- und Informationsraum (CIR) der Bundeswehr nach seiner Erhebung zur Teilstreitkraft bieten eine solche Gelegenheit.

Schaffung klarer Verantwortlichkeiten

Für viele der hier vorgeschlagenen Maßnahmen ist es wichtig, dass eine Person die Verantwortung für den Umgang mit Software-Lieferketten-Risiken trägt.[66] Eine solch klare Zuweisung von Verantwortlichkeit findet sich etwa im niederländischen Verteidigungsministerium, in dem eine Zentralstelle für die gesamte IT-Beschaffung und die Verwaltung von Software während des kompletten Lebenszyklus zuständig ist.[67] Diese Abteilung ist dadurch in der Lage, strategisch auf den Umgang mit Risiken der Software-Lieferkette zu blicken. Im Gegensatz dazu gibt es in der Bundeswehr nicht die eine maßgebliche Instanz, die für die Beschaffung und das Lebenszyklusmanagement von Software verantwortlich ist, sondern die Zuständigkeit ist auf viele unterschiedliche Stellen verteilt (siehe Infokasten).

Zuständigkeiten für den Umgang mit Software-Lieferketten-Risiken in der Bundeswehr

- Die Abteilung Innovation und Cyber (IC) im BMVg ist für die politische Steuerung zuständig.
- Die BWI GmbH, ein IT-Dienstleister im Besitz des BMVg, beschafft und betreibt vor allem administrative IT-Anwendungen.
- Für Softwareprodukte, die nicht von der BWI beschafft werden, definiert das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) die Fähigkeitsanforderungen. Für Geräte (einschließlich solcher mit eingebetteter Software) nimmt das Planungsamt der Bundeswehr diese Aufgabe wahr.
- Auf der Grundlage dieser Fähigkeitsanforderungen beschaffen die Projektmanager:innen im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) Produkte.
- Das für Baumaßnahmen zuständige Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (BAIUDBw) beschafft Soft- und Hardware für die Gebäudetechnik und IT-Infrastruktur.
- Die Wehrtechnische Dienststelle für Informationstechnologie und Elektronik (WTD 81) und eine Abteilung im ZDigBw testen und bewerten ausgewählte Softwareprodukte.
- Das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) ist für die Erkennung von Cybersicherheitsvorfällen und die Reaktion zuständig. Zu seinen Aufgaben gehört darüber hinaus das Sammeln und Auswerten von Informationen über Software-Schwachstellen und die Akkreditierung von IT-Produkten.
- In allen Dienststellen ist das IT-Fachpersonal für das Lebenszyklusmanagement der Softwareprodukte in ihrem Portfolio verantwortlich.

Auch die Bundeswehr sollte einem Dienstposten die Verantwortung für alle Facetten von Software-Lieferketten-Risiken übertragen. Die entsprechende Person sollte das Thema gegenüber der militärischen Führung ansprechen und die Umsetzung der hier vorgeschlagenen Maßnahmen überwachen. Um den Aufbau zusätzlicher Verwaltungsstrukturen zu vermeiden, sollte die Verantwortung der oder dem Chief Information Security Officer der Bundeswehr (CISOBw) übertragen werden. Diese Position ist bisher verantwortlich für die Informationssicherheit der Bundeswehr und in diesem Bereich weisungsbefugt gegenüber allen Stellen der Bundeswehr. Entscheidend ist, dass der verantwortlichen Person ausreichend

66 Bundesamt für Sicherheit in der Informationstechnik (BSI), *Grundlagen des Cyber-Supply Chain Risk Management (C-SCRM)*, Bonn, Oktober 2023, <www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_C-SCRM.html>.

67 »Materiel and IT Command«, *Ministry of Defence*, Den Haag, <https://english.defensie.nl/organisation/materiel-and-it-command>.

Personal zur Verfügung gestellt wird und sie sich gegen andere Leitungspersonen durchsetzen kann, etwa wenn es um die Verteilung von Geldern geht.

Darüber hinaus sollten die für die Softwarebeschaffung zuständigen Stellen (BAAINBw, BAIUDBw und BWI) Beauftragte einsetzen, deren Hauptaufgabe der Umgang mit Software-Lieferketten-Risiken ist und die das Beschaffungspersonal in die Lage versetzen, die hier formulierten Maßnahmen in die Praxis umzusetzen. Zudem sollte auch eine Person im BMVg explizit zuständig für das Thema sein.

Entwicklung von Leitlinien für den Umgang mit Software-Lieferketten-Risiken

Zusätzlich zeigt aus Sicht internationaler Expert:innen der Vergleich mit Themenfeldern wie IT-Sicherheit allgemein, dass Streitkräfte Leitlinien für den Umgang mit Software-Lieferketten-Risiken brauchen. Allerdings hat bisher kein Militär entsprechende umfassende Leitlinien veröffentlicht.

Deshalb sollten BMVg und Bundeswehr solche Leitlinien entwickeln. Zusätzlich zu spezifischen Punkten, die in den folgenden Abschnitten skizziert werden, sollten diese Leitlinien Orientierung bieten für das angestrebte Schutzniveau; für die Bewertung der Kritikalität eines Softwareprodukts, um den Grad des akzeptierten Risikos und der zu investierenden Ressourcen zu bestimmen; und für die Identifizierung von und den Umgang mit Abhängigkeiten von einzelnen Komponenten, Lieferanten[68] oder Staaten[69]. Darüber hinaus sollten Streitkräfte möglichst viele der in diesem und dem folgenden Kapitel besprochenen Prozesse und Regeln in Dienstvorschriften verankern. Der oder die CISOBw sollte die Leitlinien umsetzen und ihre Wirksamkeit regelmäßig bewerten. Statt eines eigenen Dokuments können diese Leitlinien auch in bestehende Leitlinien zur IT-Sicherheit integriert werden.

68 PwC, *Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern*, Berlin, August 2019, <www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/marktanalyse-reduzierung-abhaengigkeit-software-anbieter.pdf>.

69 Siehe dazu auch den Abschnitt »Ausschluss nicht vertrauenswürdiger Hersteller von der Vergabe«, S. 26.

Entwicklung von Leitlinien für die militärische Nutzung von Open-Source-Software

Angesichts der entscheidenden Rolle, die OSS bei nahezu allen Softwareprodukten spielt, muss für einen bewussten Umgang mit den Risiken der Software-Lieferkette auch das OSS-Ökosystem berücksichtigt werden — als Quelle von Bedrohungen wie von Lösungen. Da das OSS-Ökosystem anders funktioniert als das von proprietärer Software, sind eigene Leitlinien für den militärischen Einsatz von OSS nötig.[70] Das US-Verteidigungsministerium hat bereits umfangreiche entsprechende Dokumente erarbeitet.[71]

Auch BMVg und Bundeswehr sollten Leitlinien für die militärische Nutzung von OSS entwickeln. Ein solches Dokument sollte Ziele und Maßnahmen definieren, die richtungsweisend sind für die Koordination und — sofern gewünscht — Förderung des Einsatzes von OSS-Produkten durch die Bundeswehr. Am Anfang sollten eine Bestandsaufnahme der verwendeten OSS-Produkte und -Komponenten und eine Bewertung ihrer Kritikalität und Sicherheit stehen. Begleitet werden sollte dieser Prozess von einem Dialog mit Herstellern, die in ihren Produkten OSS-Komponenten verwenden. Zudem sollte dem Fachpersonal die Beschaffung und Nutzung von OSS-Produkten erleichtert werden, indem OSS-spezifische Beschaffungsanforderungen angepasst und Musterverträge, Nutzungsstrategien und Sicherheitsbewertungen bereitgestellt werden. Darüber hinaus sollte das Dokument spezifizieren, wie die Bundeswehr zur Absicherung kritischer OSS-Komponenten beitragen

70 Sven Herpig, *Fostering Open Source Software Security. Blueprint for a Government Cybersecurity Open Source Program Office*, Berlin: Interface, 31.5.2023, S. 16, <https://www.interface-eu.org/index.php/publications/fostering-open-source-software-security>. Die militärische Nutzung von OSS hat Auswirkungen weit über den Umgang mit Software-Lieferketten-Risiken hinaus, die hier nicht diskutiert werden.

71 Department of Defense (DoD), Chief Information Officer (CIO), *Memorandum: Software Development and Open Source Software*, Washington, D.C., 24.1.2022, <https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf>; dass., »Open Source Software FAQ«, Washington, D.C., 28.10.2021, <https://dodcio.defense.gov/Open-Source-Software-FAQ/>; dass., *Open Technology Development (OTD). Lessons Learned and Best Practices for Military Software*, Washington, D.C., 16.5.2011, <https://dodcio.defense.gov/portals/0/documents/foss/otd-lessons-learned-military-signed.pdf>.

kann, indem sie entweder andere Organisationen für eine entsprechende Tätigkeit bezahlt[72] oder eigenes IT-Fachpersonal selbst an OSS-Projekten mitwirkt.[73] Schließlich sollten die Leitlinien im Einklang mit allgemeinen Regierungsgrundsätzen zum Einsatz von OSS stehen.[74]

Einrichtung eines militärischen Open Source Program Office

Eine neue Struktur kann helfen, die in den Leitlinien gesteckten Ziele zu erreichen — etwa in Form eines Open Source Program Office (OSPO), wie es von vielen Unternehmen und einigen Regierungen[75] eingerichtet wurde. Ein OSPO ist eine zentrale Anlaufstelle für Fragen zu OSS-Prozessen und zur OSS-Nutzung innerhalb einer Organisation.[76] In vielen Streitkräften nimmt ausgewähltes Personal schon einzelne OSPO-Funktionen wahr, aber bisher hat noch keine Streitkraft ein eigenes OSPO etabliert.

Wenn sich die Bundeswehr dazu entschließt, ein OSPO einzurichten, sollte sie auf eine schlanke Struktur achten, in der das OSPO als zentrale Anlaufstelle für OSS-bezogene Fragen dient — beispielsweise für Beschaffungs- und IT-Fachpersonal —, aber die Verantwortung für operative Aufgaben wie die Überwachung kritischer OSS-Komponenten bei den Dienststellen verbleibt. Ein Bundeswehr-OSPO sollte im engen Austausch stehen mit dem sich in Gründung befindlichen OSPO im Bundesamt für Sicherheit in der Informationstechnik (BSI)[77] und dem Zentrum für Digitale Souveränität der öffentlichen Verwaltung (ZenDiS),[78] das vom Bundesministerium des Innern aufgebaut wurde, um OSS in die Verwaltung zu tragen.[79] So kann das Fachwissen dieser Stellen für die Bundeswehr nutzbar gemacht werden. Zudem können »OSPO-Botschafter:innen«[80] in den verschiedenen Dienststellen Bedarfe für OSS-Lösungen und Beratung ermitteln und die Arbeit des OSPO in der gesamten Bundeswehr verankern.

Einrichtung interner Prozesse

Neben dem Aufbau dieser Strukturen müssen Organisationen, die sich vor den Risiken der Software-Lieferkette schützen möchten, interne Prozesse aufbauen, die die Ideen in die Tat umsetzen.[81] Für Streitkräfte sind zwei Prozesse vorrangig: Das Sammeln verschiedener Informationen über die genutzten Softwareprodukte und die Überwachung des Support-Status der verwendeten Softwareprodukte. In beiden Bereichen hat die Bundeswehr bisher keine ausreichenden Prozesse etabliert.

Dabei ist jedoch zu beachten, dass die im Folgenden beschriebenen Prozesse nicht starr in der gesam-

72 So finanziert etwa das Bundesministerium für Wirtschaft und Energie die Sovereign Tech Agency, die wiederum Einzelpersonen und Organisationen unterstützt, die sich der Absicherung von OSS widmen, siehe »Sovereign Tech Agency. Investing in the Infrastructure of the 21st Century«, *Sovereign Tech Agency* (online), Berlin, 25.4.2025, <www.sovereign.tech/>.

73 Herpig, *Fostering Open Source Software Security* [wie Fn. 70], S. 17; Sara A. Bracket u.a., *O$$ Security: Does More Money for Open Source Software Mean Better Security? A Proof of Concept*, Washington, D.C.: Atlantic Council, 18.4.2024, <https://www.atlanticcouncil.org/content-series/cybersecurity-policy-and-strategy/o-security-does-more-money-for-open-source-software-mean-better-security-a-proof-of-concept/>.

74 IT-Planungsrat, *Föderale IT-Architekturrichtlinie*. *Version 1.9.0*, 2025, S. 21—26, <www.it-planungsrat.de/beschluss/beschluss-2025-17>.

75 Herpig, *Fostering Open Source Software Security* [wie Fn. 70], S. 20—21.

76 TODO Group, »Open Source Program Office (OSPO) Definition and Guide«, *GitHub*, 9.7.2024, <https://github.com/todogroup/ospodefinition.org>; OpenForum Europe / OSPO Alliance, *The OSPO. A New Tool for Digital Government*, Brüssel, Juni 2022, S. 9ff, <https://openforumeurope.org/wp-content/uploads/2022/06/The-OSPO-A-New-Tool-for-Digital-Government-2.pdf>; Herpig, *Fostering Open Source Software Security* [wie Fn. 70].

77 BSI, »Vortrag des BSI beim Fachkongress Public-IT-Security im Juni 2025«, *FragDenStaat*, 3.6.2025, <https://fragdenstaat.de/anfrage/vortrag-des-bsi-beim-fachkongress-public-it-security-im-juni-2025/>.

78 Siehe die Website von ZenDiS, <https://www.zendis.de/>.

79 Dies sollte über die bestehende Zusammenarbeit zwischen der BWI GmbH und ZenDiS hinausgehen (»BWI und ZenDiS schließen Rahmenvertrag über souveräne Kommunikations- und Kollaborationslösungen«, *ZenDiS*, Bochum, 4.4.2025, <https://www.zendis.de/newsroom/presse/bwi-und-zendis-schliessen-rahmenvertrag-ueber-souveraene-kommunikations-und-kollaborationsloesungen>).

80 Shilla Saebi / Aison Yu, »Growing Sustainable Contributions through Ambassador Networks«, in: *FOSDEM '20*, Brüssel, Februar 2020, <https://archive.fosdem.org/2020/schedule/event/ambassadornetworks/>; Michael Picht, »How SAP Manages Open Source Software with an Open Source Program Office«, *SAP*, 28.10.2021, <https://community.sap.com/t5/open-source-blogs/how-sap-manages-open-source-software-with-an-open-source-program-office/ba-p/13512864>.

81 BSI, *Grundlagen des Cyber-Supply Chain Risk Management* [wie Fn. 66].

ten Bundeswehr ausgerollt werden sollten — schließlich ist die Bundeswehr, wie die meisten Streitkräfte, dezentral organisiert und die Bedürfnisse der verschiedenen Dienststellen unterscheiden sich voneinander. Vielmehr sollte der oder die CISOBw zusammen mit dem ZCSBw Musterprozesse entwickeln, Anleitungen und Vorlagen bereitstellen, die Umsetzung der Prozesse kontrollieren und ihre Wirksamkeit regelmäßig bewerten. Auf dieser Grundlage können dann die verschiedenen Dienststellen selbst Prozesse einrichten, die an ihre Bedürfnisse angepasst sind.

Neben diesen Prozessen, die speziell auf Software-Lieferketten-Risiken ausgerichtet sind, braucht die Bundeswehr solide Prozesse im Bereich Cybersicherheit, wie etwa die Vorfallsbearbeitung und die Verarbeitung von Informationen über Software-Schwachstellen.[82] Beides fällt in die Zuständigkeit des ZCSBw, dessen Ausstattung daher entscheidend ist für die Cybersicherheit der Bundeswehr insgesamt — nicht nur, aber auch mit Blick auf Software-Lieferketten-Risiken.

Sammeln von Informationen

Viele Angriffe auf die Software-Lieferkette werden dadurch ermöglicht, dass Softwareprodukte Schwachstellen haben. Die Ausnutzung von Schwachstellen, die dem Software-Anbieter noch unbekannt sind (sogenannte Zero-Days), lässt sich nur mit großem Aufwand verhindern. Doch Angriffe, die bereits bekannte Schwachstellen ausnutzen, kann die Bundeswehr in vielen Fällen unterbinden — wenn die richtigen Informationen vorliegen. Dazu zählen vor allem:

1. Ein Inventar aller von der Bundeswehr verwendeten Softwareprodukte,
2. Informationen über Schwachstellen in Softwarekomponenten,
3. Sogenannte *software composition information*, die Aufschluss darüber gibt, aus welchen Komponenten die verwendeten Softwareprodukte bestehen, und
4. Informationen über die Ausnutzbarkeit von Schwachstellen *(vulnerability exploitability information)*, die anzeigen, ob eine bestimmte Schwachstelle in einem bestimmten Softwareprodukt tatsächlich ein Sicherheitsrisiko darstellt.[83]

Das IT-Fachpersonal muss nur dann Maßnahmen ergreifen, um eine Schwachstelle zu schließen, wenn es feststellt, dass die Bundeswehr ein Produkt verwendet, das auf einer Komponente beruht, in der eine bestimmte Schwachstelle vorhanden und auch ausnutzbar ist.

Bisher hat die Bundeswehr nur für die hier an zweiter Stelle genannte Art von Informationen einen zuverlässigen Prozess etabliert, nämlich um Informationen über Schwachstellen zu erhalten und mit anderen zu teilen. Zu diesem Zweck ist sie Teil entsprechender Formate im Rahmen der Nato und nationaler Cybersicherheitsbehörden wie dem BSI und bilateraler oder multilateraler Arrangements mit militärischen oder zivilen Stellen aus anderen Staaten.

Im Gegensatz dazu müssen für das Sammeln der anderen drei Arten von Informationen erst noch Prozesse aufgebaut und automatisiert werden. Was ein Software-Inventar betrifft, so hat die Bundeswehr — wie viele andere Streitkräfte — keinen vollständigen Überblick über alle Softwareprodukte, die sie verwendet, da sie diese (teilweise) dezentral beschafft. Mit Blick auf mögliche Angriffe sollte auch kein zentrales Register geführt werden. Vielmehr sollte jede Dienststelle ihr Inventar in einem standardisierten Datenformat führen, so dass Daten leicht abgefragt und verglichen werden können.

Ebenso fehlen den meisten Streitkräften — wie auch der Bundeswehr — Informationen über die Zusammensetzung der verwendeten Softwareprodukte. Das liegt daran, dass Software in der Regel ohne vollständige Informationen über ihre Komponenten bereitgestellt wird.[84] Solche Informationen können

82 BSI, *Informationssicherheit mit System. Der IT-Grundschutz des BSI*, Bonn, 22.10.2024, <www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html>.

83 Selbst wenn ein Softwareprodukt eine Komponente mit einer bekannten Schwachstelle enthält, stellt dies kein Sicherheitsrisiko dar, wenn die Schwachstelle nicht ausgenutzt werden kann — etwa weil es an anderer Stelle im Code Schutzmaßnahmen gibt oder die Art und Weise der Einbindung der Komponente keine Ausnutzung erlaubt, siehe National Telecommunications and Information Administration (NTIA), *Vulnerability-Exploitability eXchange (VEX) – An Overview*, Washington, D.C., 27.9.2021, S. 1, <https://www.ntia.gov/sites/default/files/publications/vex_one-page_summary_0.pdf>.

84 Boming Xia u.a., »An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead«, in: *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, New York: IEEE, 2023, S. 2630—2642, doi: 10.1109/ICSE48619.2023.00219.

Anbieter und OSS-Projekte in Form einer sogenannten *Software Bill of Materials* (SBOM) teilen, also »einer maschinenlesbaren Datei, die Lieferkettenbeziehungen und Details der in einem Softwareprodukt verwendeten Komponenten enthält«.[85] Militärs können SBOM-Daten entweder von ihren Lieferanten oder OSS-Projekten erhalten oder kostenpflichtige Tools von Drittanbietern verwenden, um selbst SBOMs zu erstellen.[86] Da bisher viele SBOMs keine gute Datenqualität aufweisen,[87] sollte der oder die CISOBw Mindestanforderungen für SBOMs festlegen, an denen sich Software-Anbieter orientieren müssen. Diese Anforderungen sollten sich an einem Rahmendokument[88] des BSI orientieren. Der oder die CISOBw sollte zudem sicherstellen, dass alle Dienststellen Prozesse etabliert haben, um Informationen über die Zusammensetzung von Softwareprodukten auswerten zu können, und sich die verschiedenen Dienststellen untereinander austauschen, um erhaltene Informationen zusammenzuführen.

Was schließlich die Informationen zur Ausnutzbarkeit von Schwachstellen betrifft, so trägt das IT-Fachpersonal der Bundeswehr — wie in vielen anderen Streitkräften auch — diese Informationen derzeit manuell zusammen, da Software-Anbieter diese Daten nicht in einem maschinenlesbaren Format bereitstellen. Streitkräfte sollten also Anbieter dazu veranlassen, diese Informationen zur Verfügung zu stellen (wie im folgenden Kapitel dargestellt). Solange die Bundeswehr diese Informationen nicht von den Anbietern bekommt, sollte der oder die CISOBw Hilfsmittel anbieten und Musterprozesse entwickeln, um das Datensammeln und -verarbeiten zu erleichtern. Sobald einige Anbieter die Daten bereitstellen, sollten ein Musterprozess und konkrete Anleitungen verfügbar gemacht werden, damit Dienststellen entsprechende Prozesse aufsetzen können.

Überwachung des Software-Support-Status

Darüber hinaus sollten Organisationen, die sich vor Risiken der Software-Lieferkette schützen möchten, beobachten, ob die Anbieter der von ihnen verwendeten Softwareprodukte noch Support leisten. Derzeit stellen Anbieter diese Daten nicht in einem standardisierten, maschinenlesbaren Format zur Verfügung.[89] Stattdessen durchsucht das IT-Fachpersonal der Bundeswehr die Websites der Anbieter manuell nach Hinweisen zum Ende des Supports, sofern es ihre Zeit erlaubt.

Damit die Bundeswehr den Support-Status genutzter Softwareprodukte überwachen kann, sollte der oder die CISOBw zunächst definieren, was »aktiver Support« oder, im Fall von OSS, »aktive Maintenance« bedeutet.[90] Diese Definition sollte (etwa durch eine Differenzierung nach Stufen) berücksichtigen, dass Software mit unterschiedlichen Sicherheitsanforderungen auch unterschiedlich engmaschigen Software-Support erfordert. Zudem sollte der oder die CISOBw Anleitungen zur Erleichterung der manuellen Informationssuche und einen Musterprozess für die Verarbeitung dieser Daten bereitstellen. Außerdem sollte die Bundeswehr — wie im folgenden Kapitel skizziert — Anbieter dazu bringen, ihnen entsprechende Daten zur Verfügung zu stellen, damit der Prozess automatisiert werden kann.

Die Bundeswehr sollte dringend die Expertise des Beschaffungs- und IT-Fachpersonals im Umgang mit Risiken der Software-Lieferkette ausbauen.

Vor allem aber muss der oder die CISOBw festlegen, was passiert, wenn ein Produkt keinen aktiven Support mehr erhält. In diesem Fall gibt es zwei Möglichkeiten: Das IT-Fachpersonal kann entweder ein prak-

85 BSI, *Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products. Part 2: Software Bill of Materials (SBOM)*, Bonn, 20.8.2025, S. 7, <http://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2-2_0_0.pdf?__blob=publicationFile&v=3>.

86 Cybersecurity and Infrastructure Security Agency (CISA), *Types of Software Bill of Material (SBOM) Documents*, Washington, D.C., 2023, <https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf>.

87 Santiago Torres-Arias u.a., »A Viewpoint on Knowing Software: Bill of Materials Quality When You See It«, in: *IEEE Security & Privacy*, 21 (2023) 6, S. 50—54.

88 BSI, *Technical Guideline TR-03183* [wie Fn. 85].

89 Omar Santos u.a., *OpenEoX. A Standardized Framework for Managing End of Life and other Product Lifecycle Information*, 24.4.2025, <https://docs.oasis-open.org/openeox/standardization-framework/openeox-standardization-framework-technical-report.pdf>.

90 Eine solche Definition kann auf Reifegradmetriken basieren wie etwa Linux Foundation, »OpenSSF Scorecard«, <https://securityscorecards.dev/>; OpenCode, »Badge Programm«, Bochum, 9.5.2025, <https://badges.opencode.de/de/introduction/>. Die Einhaltung kann vertraglich vereinbart werden, J. C. Herz, »Crumbling Bridges: The Failed Economics of Software Maintenance«, in: *Cyber Security: A Peer-Reviewed Journal*, 8 (2024) 2, S. 150—159 (157).

tikables Alternativprodukt identifizieren und einführen oder den Support selbst in die Hand nehmen — mit eigenen Ressourcen oder durch die Beauftragung Dritter. Gerade für Streitkräfte ist es häufig schwierig, ein Alternativprodukt einzuführen, weil komplexe militärische Prozesse auf bestimmte Produkte ausgerichtet sind und das Personal entsprechend geschult ist. Die Leitlinien für den Umgang mit Software-Lieferketten-Risiken sollten daher Anhaltspunkte dafür liefern, unter welchen Umständen die Bundeswehr ein Produkt ohne aktiven Support ersetzen sollte.

Aufbau von Fachexpertise

Das Beschaffungs- und IT-Fachpersonal der Bundeswehr ist in der Regel nicht im Umgang mit Risiken der Software-Lieferkette geschult. Die Bundeswehr sollte daher dringend die Fachexpertise der Verantwortlichen weiter aufbauen.

Angesichts des IT-Fachkräftemangels[91] und der Schwierigkeiten des öffentlichen Sektors, IT-Talente anzuwerben und zu halten, sollte die Bundeswehr Kenntnisse zum Umgang mit den Risiken der Software-Lieferkette in ihren Akademien für die zivile und militärische Aus- und Weiterbildung vermitteln. Im Ergebnis sollte das Fachpersonal drei »Sprachen«[92] beherrschen: Militär-, IT- und Beschaffungsterminologie. Darüber hinaus sollten die Streitkräfte die in dieser Studie genannten Stellen mit angemessenen Ressourcen ausstatten, um gut ausgebildetes Personal einstellen zu können.

Red-Teaming-Aktivitäten

Zudem haben Unternehmen wie Regierungsstellen gute Erfahrungen mit sogenannten *Red-Teaming*-Aktivitäten gemacht. Dabei schlüpft eigenes IT-Fachpersonal in die Rolle von Angreifer:innen, um Schwachstellen in den eigenen Systemen und den verwendeten Softwareprodukten zu finden. Üblicherweise stehen bei diesen Überprüfungen kritische OSS-Produkte und -Komponenten und proprietäre Software im Fokus. Wenn die Hersteller proprietärer Software solchen *Red Teams* Zugang zum Quellcode gewähren, können diese die Produkte gezielter auf bekannte Schwachstellen überprüfen, den Reifegrad integrierter OSS-Komponenten beurteilen und feststellen, ob gute Praktiken sicherer Software-Entwicklung[93] eingehalten wurden. Doch auch ohne Zugang zum Quellcode können solche Aktivitäten etwa Schwächen in der Konfiguration von Software aufdecken.

Einige Streitkräfte, darunter die Bundeswehr mit dem ZCSBw, haben bereits Teams, die den Programmcode ausgewählter Produkte untersuchen.[94] Das ZCSBw sollte jedoch seine Aktivitäten ausweiten: Erstens sollten die entsprechenden Fachleute auch kritische OSS-Produkte und -Komponenten unter die Lupe nehmen.[95] Zweitens sollten sie zusätzlich auf Maßnahmen setzen, die auch ohne Zugriff auf den Quellcode Erkenntnisse liefern können. Um diese Aufgaben erfüllen zu können, sollte das zuständige Team im ZCSBw vergrößert werden. Die Leitlinien für den Umgang mit Software-Lieferketten-Risiken sollten zudem vorgeben, auf welche Softwareprodukte sich entsprechende Bemühungen konzentrieren sollten.

Ausschluss nicht vertrauenswürdiger Hersteller von der Vergabe

Öffentliche Beschaffungsprozesse beruhen in der Regel auf *funktionalen Anforderungen* an das Produkt und *Sicherheitsanforderungen* an das Produkt und/oder den Anbieter. Doch es gibt Fälle, in denen ein Produkt, das alle Bedingungen erfüllt, trotzdem von der Vergabe ausgeschlossen werden sollte: Wenn der Hersteller als nicht vertrauenswürdig gilt, etwa wegen der Eigentumsverhältnisse und der Kontrolle und

91 Ralf Wintergerst, *IT-Fachkräfte 2040: Wo steht die deutsche Wirtschaft?*, Berlin: Bitkom, 11.4.2024, <www.bitkom.org/sites/main/files/2024-04/240411Bitkom-Charts-IT-Fachkraftemangel-2040final.pdf>.

92 Probasco, »Building the Tech Coalition« [wie Fn. 39], S. 8.

93 Diese werden im folgenden Kapitel dargestellt.

94 Emily Dreyfuss, »Pentagon Weapons Systems Are Easy Cyberattack Targets, New Report Finds«, *Wired*, 10.10.2018, <https://www.wired.com/story/us-weapons-systems-easy-cyberattack-targets>; Bundeswehr, »CIR 2.0. Von der Idee zur Dimension«, in: *cpm Forum für Rüstung, Streitkräfte und Sicherheit*, September 2022, S. 83, <www.bundeswehr.de/resource/blob/5519316/29945909e7ed8cc36f2c9ff4ecd53186/download-sonderheft-cir-2-0-data.pdf>.

95 John S. Meyers u.a., »The US Military Should Red-Team Open Source Code«, *Defense One*, 10.8.2022, <www.defenseone.com/ideas/2022/08/military-should-red-team-open-source-code/375635/>.

Einflussnahme durch gegnerische Regierungen.[96] Letztere können Hersteller etwa dazu bringen, schädliche versteckte Funktionen in ein Produkt einzubauen, sei es von Anfang an oder — etwa durch Updates — zu einem späteren Zeitpunkt.[97]

Es gibt Fälle, in denen ein Software-Produkt, das alle Bedingungen erfüllt, trotzdem von der Vergabe ausgeschlossen werden sollte.

Viele militärische Beschaffungsprozesse, wie auch der der Bundeswehr, sehen keine Möglichkeit vor, Produkte von der Vergabe auszuschließen, die formal alle Voraussetzungen erfüllen. Erschwerend kommt hinzu, dass die Informationen, die einer Einstufung als nicht vertrauenswürdiger Hersteller zugrunde liegen, oft nicht öffentlich sind. Vor diesem Hintergrund hat häufig das Beschaffungspersonal die Aufgabe, die funktionalen Anforderungen so anzupassen, dass nicht vertrauenswürdige Anbieter diese nicht erfüllen — eine äußerst ineffiziente Strategie, die sich in einer rechtlichen Grauzone bewegt.

Der Gesetzgeber sollte daher das Vergaberecht und das BMVg entsprechende Verwaltungsvorschriften anpassen, um den Ausschluss nicht vertrauenswürdiger Hersteller zu erleichtern.

96 Wie im Fall der 5G-Telekommunikationstechnologie (siehe CSIS Working Group on Trust and Security in 5G Networks, *Criteria for Security and Trust in Telecommunications Networks and Services*, Washington, D.C.: Center for Strategic & International Studies, 13.5.2020, <https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services>) ist die Kategorie »(un)vertrauenswürdiger Anbieter« politisch geprägt.

97 Kim Zetter, »Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors«, *Wired*, 19.12.2015, <https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/>.

Wie Politik und Streitkräfte Software-Anbieter zum Risikomanagement bewegen können

Doch Streitkräfte sind nicht allein in der Lage, sich vor den Risiken der Software-Lieferkette schützen. Vielmehr sind sie darauf angewiesen, dass auch die Software-Anbieter[98] aktiv werden — indem sie die Risiken ihrer Produkte reduzieren und ihre Kund:innen bei deren Risikomanagement unterstützen. Entscheidungsträger:innen in Politik und Bundeswehr stehen mehrere Instrumente zur Verfügung, um die Anbieter zu entsprechenden Schritten zu bewegen (siehe Grafik 6, S. 32).

Anforderungen an Software-Anbieter

Bevor Entscheidungsträger:innen geeignete Politikinstrumente auswählen, müssen sie definieren, welche Maßnahmen sie von Software-Anbietern erwarten. Die Bundeswehr hat zwar ein »Software Engineering Framework«[99] entwickelt, doch da es als Verschlusssache eingestuft wurde, ist unklar, welche Anforderungen es enthält. Basierend auf Einschätzungen von Expert:innen können besonders die folgenden sechs Maßnahmen die Lieferketten-Risiken von Softwareprodukten bedeutend reduzieren:

1. Software-Anbieter sollten gute Praktiken sicherer Software-Entwicklung einhalten.[100] Konkret sollten sie ausnutzbare bekannte Schwachstellen in den Komponenten ihrer Produkte beheben,[101] Software in speichersicheren Programmiersprachen (neu) schreiben,[102] auf einen sicheren Build-Prozess — der für Menschen verständlichen Programmcode in maschinenlesbaren Binärcode umwandelt — bei den von ihnen verwendeten Komponenten[103] und

98 Der Begriff »Anbieter« bezieht sich hier nicht nur auf Software-Hersteller, sondern auf jede Einheit in der Software-Lieferkette, die die Software anpasst, wie Wiederverkäufer/Distributoren (wenn sie das Produkt anpassen), Systemintegratoren oder Hardware-Anbieter, siehe CISA, *Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)*, 3. Aufl., Washington, D.C., 3.9.2024, S. 26, <https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf>.

99 Rolf Hager, »Software Defined Defence. Schnellere Softwareentwicklung für die Bundeswehr mit der ›Platform42‹«, in: *Europäische Sicherheit & Technik*, 19.3.2024, <https://esut.de/2024/03/fachbeitraege/47794/it-news-software-defined-defence-schnellere-softwareentwicklung-fuer-die-bundeswehr-mit-der-platform42/>.

100 Siehe z. B. Murugiah Souppaya u.a., *Secure Software Development Framework (SSDF) Version 1.1. Recommendations for Mitigating the Risk of Software Vulnerabilities*, Gaithersburg: National Institute of Standards and Technology (NIST), Februar 2022; »Fundamental Practices for Secure Software Development. Essential Elements of a Secure Development Lifecycle Program«, *SAFECode*, März 2018, <https://safecode.org/uncategorized/fundamental-practices-secure-software-development/>; BSI, *Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products. Part 1: General Requirements*, Bonn, 20.9.2024, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-1-0_9_0.pdf?__blob=publicationFile&v=4>.

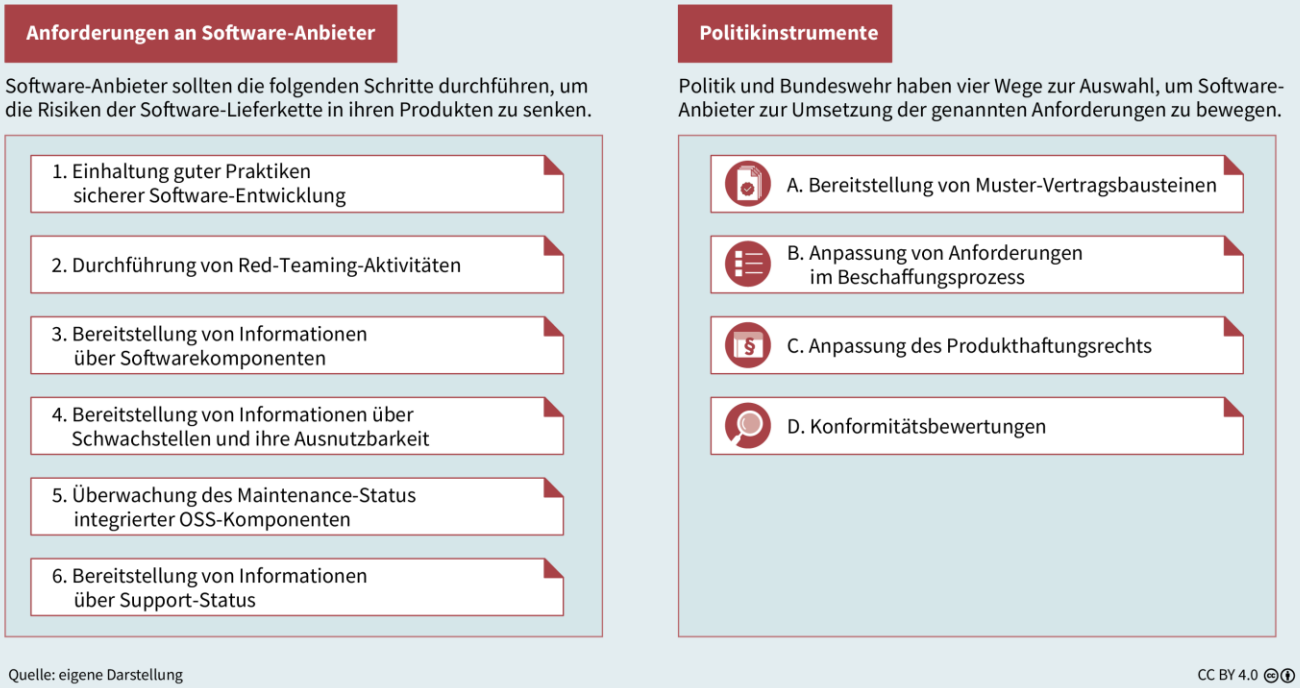
101 »Reduce Supply Chain Risk. Continuous SBOM Analysis Platform«, *Dependency Track*, <https://dependencytrack.org/>.

102 Alex Gaynor, »Introduction to Memory Unsafety for VPs of Engineering«, *alexgaynor.net*, 12.8.2019, <https://alexgaynor.net/2019/aug/12/introduction-to-memory-unsafety-for-vps-of-engineering/#what-is-memory-unsafety>.

103 »Requirements«, *SLSA*, <https://slsa.dev/spec/v0.1/requirements>; Mikaël Barbero, »Understanding Software Provenance«, *Opera Omnia*, 26.12.2023, <https://mikael.barbero.tech/blog/post/2023-12-26-understanding-software-provenance>.

Grafik 6

Wie Politik und Streitkräfte Software-Anbieter zum Risikomanagement bewegen können



Quelle: eigene Darstellung

eigenen Produkten[104] achten und ihren Programmcode signieren.

2. Zusätzlich zum oben genannten Red-Teaming der Endprodukte durch die Bundeswehr sollten auch Anbieter entsprechende Tests in ihren eigenen Systemen durchführen (lassen) und ebenso ihre Zulieferer und Dienstleister dazu verpflichten.
3. Anbieter sollten der Bundeswehr (und idealerweise auch ihren übrigen Kund:innen) Informationen über die Zusammensetzung ihrer Softwareprodukte zur Verfügung stellen, etwa als SBOMs. Diese Daten sollten dabei einem der etablierten Standards[105] entsprechen und langfristig alle Ebenen von Komponenten beinhalten,[106] da eine ausnutzbare Schwachstelle tief in der Software-Lieferkette verborgen sein kann.
4. Anbieter sollten für ihre Produkte Informationen über Schwachstellen und ihre Ausnutzbarkeit in einem standardisierten und maschinenlesbaren Datenformat[107] und über einen definierten Verteilungsmechanismus bereitstellen.
5. Anbieter sollten während der gesamten Lebensdauer ihrer Produkte den Maintenance-Status der OSS-Komponenten, die in ihren Produkten inte-

104 »Definitions«, *Reproducible Builds*, <https://reproducible-builds.org/docs/definition/>; Chris Lamb / Stefano Zacchiroli, »Reproducible Builds: Increasing the Integrity of Software Supply Chains«, in: *IEEE Software*, 39 (2022) 2, S. 62 – 70; openCode / ZenDiS / BSI: *Sichere Softwarelieferketten: openCode als Baustein einer souveränen digitalen Infrastruktur*, Bochum, März 2025, <www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ZenDiS/Strategiepapier-Softwarelieferketten.pdf?__blob=publicationFile&v=2>.

105 NTIA, *Survey of Existing SBOM Formats and Standards*, Washington, D.C., 2021, <www.ntia.gov/sites/default/files/publications/sbom_formats_survey-version-2021_0.pdf>.

106 CISA, *Framing Software Component Transparency* [wie Fn. 98], S. 10f. Eine solche Anforderung würde über die Anforderung des CRA hinausgehen, nur die erste Ebene von Komponenten darzustellen, siehe Europäisches Parlament und Rat, *Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)*, 23.10.2024, Anhang I, Teil I(1), <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2847>).

107 *Common Security Advisory Framework (CSAF)*, <www.csaf.io/>; NTIA, *Vulnerability-Exploitability eXchange* [wie Fn. 83].

griert sind, im Blick behalten. Zum Entwicklungszeitpunkt sollten sie nur solche Komponenten integrieren, die der Bundeswehr-Definition von »aktiver Maintenance« entsprechen. Sollte eine Komponente, die bereits in ein Produkt integriert wurde, diese Anforderungen irgendwann nicht mehr erfüllen, sollte der Anbieter die Komponente austauschen, das Produkt selbst maintainen oder Dritte damit beauftragen. Anbieter, deren Produkte unter den EU Cyber Resilience Act (CRA) fallen, sind bereits ab 2027 dazu verpflichtet.[108] Doch diese Vorschrift findet keine Anwendung auf Produkte, die ausschließlich für militärische Zwecke oder zur Verarbeitung von Verschlusssachen entwickelt wurden.[109]

6. Anbieter sollten Informationen zum Support-Status ihrer Produkte in einem standardisierten, maschinenlesbaren Format[110] bereitstellen.

Viele dieser Maßnahmen sind unter Software-Anbietern noch nicht weit verbreitet. Daher brauchen entsprechende Vorgaben großzügige Umsetzungszeiträume. Zudem sollten Software-Anbieter auch dazu verpflichtet werden, allgemeine Cybersicherheitsmaßnahmen umzusetzen, die nicht spezifisch auf Software-Lieferketten-Risiken ausgerichtet sind, aber dennoch Auswirkungen darauf haben. Dazu zählen etwa Netzwerksegmentierung und eine »Zero trust«-Architektur,[111] ein Schwachstellen-Management,[112] regelmäßiges Einspielen von Software-Updates[113] und die Detektion und Bearbeitung von Cybersicherheitsvorfällen.[114]

Wenn diese Anforderungen in Anreizsystemen oder Regulierung politisch verankert werden, muss beachtet werden, dass KMU und kleinere OSS-Projekte in der Regel weniger Möglichkeiten haben, anspruchsvolle Vorschriften umzusetzen. Voraussetzungsreiche Regulierung kann daher unbeabsichtigte Folgen haben: So ist es denkbar, dass KMU oder kleinere OSS-Projekte ihre Softwareprodukte aufgeben oder Anbieter die OSS-Komponenten, die sie in ihre Produkte integrieren, abschotten.[115] Daher sollten Entscheidungsträger:innen prüfen, ob Pflichten für KMU und OSS-Projekte reduziert werden und wie diese bei der Umsetzung unterstützt werden können.

Bereitstellung von Muster-Vertragsbausteinen

Wenn die Vorgaben für Anbieter definiert wurden, müssen Politik und Bundeswehr entscheiden, auf welche Weise sie die Adressaten dazu bewegen wollen, diese Maßnahmen umzusetzen. Eine niedrigschwellige Möglichkeit sind Beschaffungsverträge. Auch ohne zentrale Vorschriften können auf diesem Weg die genannten Vorgaben vereinbart werden. Ein Beispiel aus dem Privatsektor zeigt, dass Software-Anbieter etwa vertraglich dazu verpflichtet werden können, regelmäßig den Support-Status der OSS-Komponenten zu überprüfen, die sie in ihre Produkte integriert haben, und falls nötig Abhilfemaßnahmen zu ergreifen.[116] Die Bundeswehr, wie auch die Streitkräfte anderer Staaten, machen von dieser Möglichkeit allerdings erst wenig Gebrauch.

Der aktuelle Beschaffungsprozess der Bundeswehr berücksichtigt Software-Lieferketten-Risiken nicht.

Um dies zu ändern, sollten dem Beschaffungspersonal der Bundeswehr Muster-Vertragsbausteine zur Verfügung gestellt werden, zum Beispiel in Form von Service Level Agreements.[117]

108 Europäisches Parlament und Rat, *Cyberresilienz-Verordnung* [wie Fn. 106], Art. 13(5).

109 Ebd, Art. 2(7).

110 Santos u.a., *OpenEoX* [wie Fn. 89].

111 Scott Rose u.a., *Zero Trust Architecture*, Gaithersburg: NIST, August 2020, doi: 10.6028/NIST.SP.800-207.

112 Allen D. Householder u.a., *The CERT Guide to Coordinated Vulnerability Disclosure*, Pittsburgh: Carnegie Mellon University, August 2017, <https://insights.sei.cmu.edu/documents/1945/2017_003_001_503340.pdf>.

113 Murugiah Souppaya / Karen Scarfone, *Guide to Enterprise Patch Management Planning. Preventive Maintenance for Technology (NIST SP 800-40 Rev. 4)*, Gaithersburg: NIST, 2022, doi: 10.6028/NIST.SP.800-40r4.

114 NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, Gaithersburg: NIST, 26.2.2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.

115 John S. Meyers / Paul Gibert, »Questioning the Conventional Wisdom on Liability and Open Source Software«, in: *Lawfare*, April 2024, <www.lawfaremedia.org/article/questioning-the-conventional-wisdom-on-liability-and-open-source-software>; Olaf Kolkman, »The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem«, *Internet Society*, 24.10.2022, <www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/>.

116 Herz, *Crumbling Bridges* [wie Fn. 90], S. 157.

117 Für ein Beispiel aus dem zivilen Bereich siehe Der Beauftragte der Bundesregierung für Informationstechnik,

Anpassung von Anforderungen im Beschaffungsprozess

Der aktuelle Beschaffungsprozess der Bundeswehr berücksichtigt Software-Lieferketten-Risiken nicht.[118] Die USA hingegen nutzen bereits Beschaffungsregeln, um Software-Anbieter dazu zu bewegen, ihre Produkte besser vor Software-Lieferketten-Risiken zu schützen.[119] So verpflichtet etwa die US Army ihre Lieferanten zur Bereitstellung von SBOM-Daten.[120] Die aktuell laufende Überarbeitung der deutschen zivilen und militärischen Beschaffungsgesetze und die geplante Neufassung der europäischen Beschaffungsvorschriften bieten eine gute Gelegenheit, entsprechende Änderungen mit aufzunehmen.[121]

Konkret sollte die Bundeswehr die Regeln für die militärische Beschaffung in dreierlei Hinsicht anpassen:

1. Zusammen mit allen für Softwarebeschaffung verantwortlichen Stellen sollte der oder die CISOBw horizontale Mindestanforderungen zum Umgang von Anbietern mit Risiken der Software-Lieferkette erarbeiten. Solche Mindestanforderungen hat die Bundeswehr bereits etwa für Cybersicherheit formuliert. Auch diese Vorgaben sollten durch ein Stufensystem auf die Kritikalität des jeweiligen Produkts zugeschnitten werden.
2. Hindernisse für die Beschaffung von OSS, besonders von Produkten ohne kommerziellen Supportvertrag, sollten beseitigt werden.[122]
3. Angesichts des IT-Fachkräftemangels sollten Hürden beseitigt werden, (sicherheitsüberprüfte) Dienstleister mit Cybersicherheitsaufgaben zu betrauen, für die die Ressourcen der Bundeswehr nicht ausreichen, wie zum Beispiel Red-Teaming-Aktivitäten.

Anpassung des Produkthaftungsrechts

Aktuell kann die Bundeswehr — ähnlich wie Endnutzer:innen außerhalb der EU und viele andere Streitkräfte — Software-Anbieter hauptsächlich bei Vertragsbruch, Vorsatz oder grober Fahrlässigkeit haftbar machen. Die Ursachen von Sicherheitsverletzungen, bei denen die Software-Lieferkette eine Rolle spielt, liegen jedoch häufig in (unterlassenen) Maßnahmen der Anbieter jenseits der genannten Kategorien. Produkthaftungsregelungen für Softwareprodukte, die von Streitkräften verwendet werden, würden es der Bundeswehr erlauben, Anbieter zu belangen, wenn Unzulänglichkeiten im Softwareprodukt oder im Entwicklungsprozess einen Schaden verursachen, und würden sie etwa zur Zahlung von Schadenersatz verpflichten.[123]

Das geltende deutsche Produkthaftungsrecht findet keine Anwendung auf Software.[124] Und die neue EU-Produkthaftungsrichtlinie ist zwar anwendbar, sieht aber nur Ansprüche natürlicher Personen vor.[125] Ab

Aktuelle EVB-IT, Berlin, 2.11.2023, <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-einkauf/evb-it-und-bvb/evb-it/evb-it-node.html>.

118 BMVg, *Projektbezogene Bedarfsdeckung und Nutzung* [wie Fn. 43].

119 Siehe etwa The White House, *Executive Order on Improving the Nation's Cybersecurity (EO 14028)*, Washington, D.C., 12.5.2021, <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

120 DoD, Department of the Army, *Memorandum: Assistant Secretary of the Army (Acquisition, Logistics and Technology) Software Bill of Materials Policy*, Washington, D.C., 17.10.2024, <https://api.army.mil/e2/c/downloads/2024/10/17/4072ab1e/asaalt-software-bill-of-materials-policy-signed.pdf>.

121 Deutscher Bundestag, *Vorgang – Gesetzgebung: Gesetz zur beschleunigten Planung und Beschaffung für die Bundeswehr*, Berlin 2025, <https://dip.bundestag.de/vorgang/gesetz-zur-beschleunigten-planung-und-beschaffung-f%C3%BCr-die-bundeswehr/324833>; Francesco Nicoli, *Mapping the Road Ahead for EU Public Procurement Reform*, Brüssel: Bruegel, 31.3.2025, <https://www.bruegel.org/first-glance/mapping-road-ahead-eu-public-procurement-reform>; Deutscher Bundestag, *Vorgang – Gesetzgebung: Gesetz zur Beschleunigung der Vergabe öffentlicher Aufträge*, Berlin 2025, <https://dip.bundestag.de/vorgang/gesetz-zur-beschleunigung-der-vergabe-%C3%B6ffentlicher-auftr%C3%A4ge/324928>.

122 Für einen Überblick dieser Hindernisse siehe etwa Iain G. Mitchell, »Public Sector and Open Source«, in: Amanda Brock (Hg.), *Open Source Law, Policy and Practice*, Oxford: Oxford University Press, 2022, S. 429—468, <https://academic.oup.com/book/44727>.

123 Trey Herr u.a., *Buying Down Risk: Cyber Liability*, Washington, D.C.: Atlantic Council, 15.1.2025, <www.atlanticcouncil.org/content-series/buying-down-risk/cyber-liability/>; Gergely Biczók u.a., *Realigning Incentives to Build Better Software: A Holistic Approach to Vendor Accountability*, 10.4.2025, <http://arxiv.org/pdf/2504.07766v1>.

124 *Gesetz über die Haftung für fehlerhafte Produkte. (ProdHaftG)*, 15.12.1989, <https://www.gesetze-im-internet.de/prodhaftg/BJNR021980989.html>.

125 Europäisches Parlament und Rat, *Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung*

2027 wird die Bundeswehr Ansprüche gegenüber Software-Anbietern auf der Grundlage des europäischen CRA geltend machen können, doch auf viele von der Bundeswehr genutzte Produkte ist diese Vorschrift nicht anwendbar.[126] Abgesehen vom CRA hat bisher kein Land ein entsprechendes Produkthaftungsregime entwickelt.

Der Gesetzgeber sollte in Erwägung ziehen, eine Produkthaftungsregelung für Software einzuführen, die von Streitkräften genutzt wird.

Der Gesetzgeber sollte daher in Erwägung ziehen, eine Produkthaftungsregelung für Software einzuführen, die von Streitkräften genutzt wird, oder für Software im Allgemeinen. Eine gute Gelegenheit dafür bietet die erwähnte EU-Produkthaftungsrichtlinie, die die Mitgliedstaaten bis 2026 in nationales Recht umsetzen müssen. Da der Gesetzgeber dadurch ohnehin das Produkthaftungsrecht ändern muss, könnte er über die Erfordernisse der EU-Richtlinie hinausgehen und auch juristische Personen wie die Bundeswehr anspruchsberechtigt machen. Dabei könnten die oben genannten Vorgaben für Software-Anbieter als Maßgabe dafür dienen, unter welchen Bedingungen Anbieter haftbar gemacht werden können.[127] Auch die Kriterien des CRA sollten berücksichtigt werden, um die regulatorische Kluft zwischen dem zivilen und dem militärischen Sektor zu verkleinern.

Konformitätsbewertungen

Wenn Politik und Streitkräfte sichergehen wollen, dass Software-Anbieter spezielle Anforderungen erfüllen, können sie auf Konformitätsbewertungen zurückgreifen. Dabei überprüft eine bescheinigende Partei — der Anbieter selbst (Selbstbewertung) oder eine unabhängige, staatlich zugelassene Stelle (Fremdbewertung) —, ob bestimmte Vorgaben eingehalten werden.[128] Diese können etwa in einem technischen Standard definiert sein. Das Ergebnis der Bewertung wird beispielsweise in einer Zertifizierung festgehalten.

Das US-Verteidigungsministerium hat ein Konformitätsbewertungssystem entwickelt für den Umgang seiner Lieferanten mit Informationen, die keine Verschlusssachen, aber dennoch sensibel sind.[129] Der CRA sieht ein Konformitätsbewertungssystem für Softwareprodukte vor, das je nach Kritikalität des Produkts von Selbst- bis zu Fremdbewertungen reicht und produktbezogene mit prozessbezogenen Bewertungen kombiniert.[130] In Deutschland gibt es solche Systeme für die Anbieter von Software, die Verschlusssachen verarbeiten. Diese berücksichtigen auch Software-Lieferketten-Risiken, doch da die Konformitätsbewertungssysteme nicht öffentlich sind, können sie hier nicht beurteilt werden. Darüber hinaus ist das »IT-Sicherheitskennzeichen«[131] des BSI ein Konformitätsbewertungssystem für COTS-IT-Produkte.

Solche Konformitätsbewertungssysteme für Software sind für Anbieter und Politik kostspielig, die Beurteilung muss wegen häufiger Software-Updates regelmäßig erneuert werden, und es fehlt — als Grundlage für die Bewertung — häufig an produktbezogenen technischen Standards, die Software-Lieferketten-Risiken einbeziehen. Daher sollten politische und militärische Entscheidungsträger:innen mit der Einrichtung weiterer Konformitätsbewertungssysteme zurückhaltend sein. Stattdessen sollte das Beschaffungspersonal der Bundeswehr bei der Produktauswahl die Kriterien des IT-Sicherheitskennzeichens und des CRA berücksichtigen.

Sollte die Bundeswehr dennoch ein Konformitätsbewertungssystem einführen wollen, sollten die Verantwortlichen:

1. sich für einen prozessbezogenen Ansatz entscheiden, um sicherzustellen, dass die Bewertungen länger gültig bleiben;

der Richtlinie 85/374/EWG des Rates, 23.10.2024, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024L2853>.

126 Europäisches Parlament und Rat, *Cyberresilienz-Verordnung* [wie Fn. 106], Art. 2(7).

127 Maia Hamin u.a., »Three Questions on Software Liability«, in: *Lawfare*, September 2023, <www.lawfaremedia.org/article/three-questions-on-software-liability>; Chinmayi Sharma / John S. Meyers, »Bugs in the Software Liability Debate«, *Just Security*, 18.7.2023, <www.justsecurity.org/87294/bugs-in-the-software-liability-debate/>.

128 Paulus / Rupp, *Government's Role in Increasing Software Supply Chain Security* [wie Fn. 24], S. 32f.

129 DoD, CIO, *About CMMC*, Washington, D.C., <https://dodcio.defense.gov/CMMC/About/>.

130 Europäisches Parlament und Rat, *Cyberresilienz-Verordnung* [wie Fn. 106].

131 BSI, *Transparente Sicherheit durch das IT-Sicherheitskennzeichen*, Bonn, 9.2.2023, <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html>.

2. ein abgestuftes System entwickeln, um die Teilnahme von KMU und des OSS-Ökosystems zu erleichtern;
3. eine Harmonisierung mit den CRA-Anforderungen und mit den Bewertungssystemen anderer Nato-Verbündeter anstreben, um gleiche Wettbewerbsbedingungen im gesamten Bündnis zu schaffen; und
4. zumindest auf der höchsten Sicherheitsstufe Bewertungen durch Dritte fordern, um belastbare Bewertungen zu erhalten.

Prioritäten für Bundespolitik und Bundeswehr

Bereits die in dieser Studie diskutierten Vorfälle, die Streitkräften die Auswirkungen von Unterbrechungen im Betriebsablauf oder von Angriffen über die Software-Lieferkette vor Augen geführt haben, zeichnen ein düsteres Bild. Dabei stellen diese mutmaßlich nur einen Bruchteil der tatsächlich stattgefundenen Ereignisse dar, denn die meisten werden vermutlich nicht publik.

Trotz der potentiell verheerenden Auswirkungen sollte die Bundeswehr nicht danach streben, die Risiken der Software-Lieferkette um jeden Preis zu minimieren. Stattdessen gilt es, ein angemessenes Schutzniveau zu definieren — je nach Softwareprodukt. Der Fokus sollte dabei auf denjenigen Produkten liegen, die auf dem Gefechtsfeld zum Einsatz kommen, entscheidend für das Funktionieren des Unterstützungsbereichs sind oder deren Kompromittierung gegnerischen Nachrichtendiensten weitreichende Einblicke erlauben würde.

Besonders mit Blick auf diese Produkte sollten BMVg und Bundeswehr Maßnahmen ergreifen, um die Risiken der Software-Lieferkette auf ein akzeptables Niveau zu senken. Allerdings sind viele der in dieser Studie diskutierten Maßnahmen komplex und ressourcenintensiv. Angesichts der begrenzten Aufmerksamkeit von Entscheidungsträger:innen in der Politik wie in der Bundeswehr, des Mangels an IT-Fachpersonal und endlicher finanzieller Mittel sollten Bundespolitik und Bundeswehr drei Schritte mit größter Dringlichkeit angehen.

Erstens sollten in der Bundeswehr Strukturen aufgebaut werden, um den bewussten Umgang mit den Risiken der Software-Lieferkette überhaupt erst zu ermöglichen. Konkret sollte das Portfolio des CISOBw um diesen Aufgabenbereich erweitert werden, um eine zentrale Zuständigkeit für das Thema zu schaffen. Dieser Prozess sollte flankiert werden durch die Berufung von Beauftragten bei BAAINBw, BAIUDBw und BWI, die das Beschaffungspersonal dabei unterstützen, weitere Maßnahmen zu implementieren.

Des Weiteren sollten BMVg und die involvierten Stellen bei der Bundeswehr gemeinsam Leitlinien zum Umgang mit Risiken der Software-Lieferkette formulieren, deren Inhalte möglichst auch in Dienstvorschriften verankert werden sollten. Schließlich sollte die Bundeswehr ihrem Beschaffungs- und IT-Fachpersonal einschlägige Expertise zum Umgang mit den Risiken der Software-Lieferkette vermitteln, etwa über die Akademien der Bundeswehr.

Zweitens sollten Politik und Bundeswehr die Software-Anbieter dazu bewegen, der Bundeswehr diejenigen Informationen zur Verfügung zu stellen, die für ein effektives Risikomanagement unabdingbar sind. Dazu zählen Informationen zu Softwarekomponenten, zu Schwachstellen und ihrer Ausnutzbarkeit und zum Support-Status der Produkte. Am unbürokratischsten kann dies über Muster-Vertragsbausteine erreicht werden, welche der oder die CISOBw zentral dem Beschaffungspersonal zur Verfügung stellt — allerdings ist offen, ob diese in den endgültigen Verträgen mit den Anbietern auch berücksichtigt werden. Zuverlässiger wäre daher der Weg über horizontale Mindestanforderungen im Beschaffungsprozess.

Drittens sollte die Bundeswehr eigene Prozesse etablieren, um auf Basis der von den Software-Anbietern erhaltenen Informationen die Risiken der Software-Lieferkette im Blick behalten und gegebenenfalls auf Vorfälle reagieren zu können. Dazu zählen die Pflege von Inventaren aller von der Bundeswehr verwendeten Softwareprodukte, die Überwachung des Support-Status dieser Produkte und die konstante Beobachtung, ob darin bekannte Schwachstellen vorhanden und ausnutzbar sind.

Zusammengenommen erlauben es diese drei Schritte der Bundeswehr, handlungsfähig zu werden und die Risiken der Software-Lieferkette im Blick zu behalten und auf Vorfälle reagieren zu können. Wenn die Bundesregierung und die Bundeswehr die Risiken zudem weiter reduzieren möchten, sind zusätzliche Schritte nötig. So sollten die Bundeswehr selbst und

ihre Software-Anbieter sowie deren Zulieferer Red-Teaming-Tests durchführen, um Schwachstellen in Produkten und Konfigurationen offenzulegen. Außerdem sollten Politik und Bundeswehr die Anbieter dazu bringen, Praktiken sicherer Software-Entwicklung einzuhalten. Dazu zählen das Schließen ausnutzbarer bekannter Schwachstellen in den Komponenten der Produkte, der Wechsel zu speichersicheren Programmiersprachen, die Absicherung des Build-Prozesses und das Signieren des Programmcodes. Des Weiteren sollten Anbieter den Maintenance-Status der OSS-Komponenten, die Teil ihrer Produkte sind, nicht nur zum Entwicklungszeitpunkt prüfen, sondern auch darüber hinaus überwachen und — wenn keine Maintenance mehr gegeben ist — Abhilfemaßnahmen ergreifen. Auch für diese Maßnahmen sind angepasste Mindestanforderungen im Beschaffungsprozess eine Möglichkeit, die — im Vergleich zu einer Änderung des Produkthaftungsrechts — vergleichsweise leicht umzusetzen sind.

Entscheidend ist, dass BMVg und Bundeswehr die gewählten Maßnahmen zeitnah implementieren, damit sie Eingang in laufende Reformbemühungen finden können: Die Reorganisation des CIR nach seiner Erhebung zur Teilstreitkraft ist ein guter Zeitpunkt, um neue Strukturen zu schaffen. Und mit der Reform der Schuldenbremse[132] stehen die Chancen günstig für Investitionen, die die Sicherheit der Bundeswehr deutlich verbessern. Schließlich befinden sich verschiedene Beschaffungsregelungen derzeit in Überarbeitung und Software-Anbieter müssen sich mit Blick auf das Inkrafttreten des CRA 2027 ohnehin mit der Sicherheit ihrer Produkte befassen.

Um die Kosten der hier vorgeschlagenen Maßnahmen zu senken, sollten Bundesregierung und Bundeswehr sich mit gleichgesinnten Staaten zusammentun. Die Bundeswehr kann Software-Anbieter eher davon überzeugen, bestimmte Maßnahmen umzusetzen, wenn es sich um international harmonisierte Anforderungen handelt. Ein internationaler Austausch zu diesem Thema könnte neben der Nato auch im Rahmen der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) oder der kürzlich eingerichteten G7-Arbeitsgruppe für Cybersicherheit stattfinden. Ein internationales Multi-Stakeholder-Forum, das sich mit dem Handling der Risiken (militärischer) Software-Lieferketten befasst, könnte das Bewusstsein für dieses Thema weiter schärfen und die operative Zusammenarbeit fördern.

In jedem Fall wird der Umgang mit Software-Lieferketten-Risiken ein Balanceakt für Politik und Bundeswehr: Einerseits müssen sie in signifikantem Umfang Ressourcen investieren, um potentiell verheerende Angriffe oder sonstige Unterbrechungen in militärischen Betriebsabläufen zu verhindern oder deren Auswirkungen zu mindern. Andererseits müssen sie die Weichen für »Software-defined Defense« stellen — durch vereinfachte und beschleunigte Beschaffung, den Einsatz und die Aktualisierung von Software und die Förderung eines dynamischen und innovativen Defense-Tech-Ökosystems im eigenen Land.[133] Auch wenn sich diese Studie auf Ersteres konzentriert, bleibt auch Letzteres bedeutsam.

132 »Mehrheit für Reform der Schuldenbremse: 512 Abgeordnete stimmen mit Ja«, *Deutscher Bundestag*, 18.3.2025, <www.bundestag.de/dokumente/textarchiv/2025/kw12-de-sondersitzung-1056916>.

133 Probasco, *Building the Tech Coalition* [wie Fn. 39].

Abkürzungen

BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BAIUDBw	Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr
BMVg	Bundesministerium der Verteidigung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIO	Chief Information Officer
CIR	Cyber- und Informationsraum (Teilstreitkraft der Bundeswehr)
CISA	Cybersecurity and Infrastructure Security Agency (USA)
CISOBw	Chief Information Security Officer der Bundeswehr
COTS	Commercial off-the-shelf
CRA	EU Cyber Resilience Act
DoD	Department of Defense (USA)
GRU	Militärischer Nachrichtendienst (Russland)
IC	Innovation und Cyber (Abteilung im BMVg)
IT	Informationstechnologie
KMU	Kleine und mittlere Unternehmen
NIST	National Institute of Standards and Technology (USA)
NTIA	National Telecommunications and Information Administration (USA)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OSPO	Open Source Program Office
OSS	Open-Source-Software
PwC	PricewaterhouseCoopers
SaaS	Software as a Service
SBOM	Software Bill of Materials
SDD	Software-defined Defense
SVR	Auslandsgeheimdienst (Russland)
WTD 81	Wehrtechnische Dienststelle für Informationstechnologie und Elektronik
ZCSBw	Zentrum für Cyber-Sicherheit der Bundeswehr
ZDigBw	Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum
ZenDiS	Zentrum für Digitale Souveränität der Öffentlichen Verwaltung