SWP

SWP Research Paper

Alexandra Paulus

An Achilles Heel of Today's Armed Forces

Managing Software Supply Chain Risk in the Military Sector

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

SWP Research Paper 6
November 2025, Berlin

- Today's armed forces are highly dependent on software. Software products are built by complex networks of software components, software vendors, service providers, and other companies that, together, form the software supply chain.
- In "conventional" cybersecurity incidents, threat actors usually gain direct access to their target. But in the case of the software supply chain, the risks originate upstream in the supply chain itself and have an impact on entities downstream — often the end users.
- The armed forces are particularly vulnerable to these risks. Software supply chain incidents in the military sector have caused disruption and allowed malicious actors to engage in industrial espionage, political espionage, and sabotage.
- Policymakers and the Bundeswehr can manage software supply chain risk in the military sector through a set of measures. First, decision-makers should determine the requisite level of protection for the various areas of software use to strike a balance between risk management, on the one hand, and the functionality, cost, and speed of deployment, on the other.
- Thereafter, the Bundeswehr should establish effective risk management. Further, the federal government and the Bundeswehr should ensure that software suppliers reduce the software supply chain risk posed by their products. By doing so, the armed forces can be given adequate protection.

SWP Research Paper

Alexandra Paulus

An Achilles Heel of Today's Armed Forces

Managing Software Supply Chain Risk in the Military Sector

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

SWP Research Paper 6
November 2025, Berlin

SWP Research Papers are
peer reviewed by senior
researchers and the execu-
tive board of the Institute.
They are also subject to
copy-editing. For further
information on our quality
control procedures, please
visit the SWP website:
https://www.swp-berlin.org/
en/about-swp/quality-
management-for-swp-
publications/.
SWP Research Papers reflect
the views of the author(s).

SWP
Stiftung Wissenschaft und
Politik
German Institute
for International
and Security Affairs

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

ISSN (Print) 2747-5123
ISSN (Online) 1863-1053
DOI: 10.18449/2025RP06

(Updated English version of
SWP-Studie 14/2025)

Table of Contents

Dr Alexandra Paulus is an Associate in SWP's International Security Research Division and Head *of the Research Cluster Cybersecurity and Digital Policy.*

An Achilles Heel of Today's Armed Forces. Managing Software Supply Chain Risk in the Military Sector

Today's armed forces are highly dependent on software. That is true not only for administrative tasks and logistics but also for modern weapons systems such as tanks, warships, and fighter jets. The software products used by the military are built by complex networks of software components, software vendors, service providers, and other companies that, together, form the software supply chain.

In "conventional" cybersecurity incidents, threat actors usually gain direct access to their target. But in the case of the software supply chain, the risks originate upstream in the supply chain and have a harmful impact elsewhere — frequently with the end user. For example, in 2019—20, Russian spies did not seek to infiltrate the information technology (IT) systems of the US agency that maintains that country's nuclear weapons stockpile; rather, they gained access to the software vendor SolarWinds, from where they sent an update containing malware to the strictly secured agency, enabling them to collect data at the target.

All the links of the supply chain are connected via software — whether through the software product itself or its components or through access to the software product, which may have been granted, for example, to a service provider. Accordingly, all the links of the supply chain for the software products used by the armed forces can potentially serve as entry points into military systems. In particular, it is small and medium-sized enterprises (SMEs) and smaller open source software (OSS) projects that are often poorly protected and therefore an easy target for attackers. Moreover, it is often the case that the armed forces do not have an overview of all the software products they are using, let alone all the actors and components that constitute the supply chains of those products. And what is more, the armed forces have little or no control over large parts of the supply chain. Thus, the software supply chain is an Achilles heel of the modern-day armed forces: even the most technologically advanced and most securely protected military can fall victim to attacks that exploit the complex structure of software supply chains.

Incidents involving the software supply chain have disrupted military operations and allowed malicious actors to engage in industrial espionage, political espionage, and sabotage. For example, between 2013 and 2018, individuals associated with Chinese intelligence gained access to the systems of the largest US military shipbuilder via its cloud service provider. And in 2022, on the very first day of the Russian full-scale invasion of Ukraine, Russian military intelligence hijacked a software update from a satellite communications provider to disrupt the connectivity of the Ukrainian military on the battlefield. Even inadvertent mistakes can cause significant damage, as demonstrated by the CrowdStrike incident in 2024, which temporarily rendered approximately 8.5 million devices worldwide unusable. Finally, a lack of software maintenance can have profound consequences, too: in March 2025, Ukrainian fighter jets were at risk of becoming inoperable in the absence of software updates provided by the US. In short, software supply chain incidents can jeopardise the combat readiness of the armed forces.

This research paper examines how the armed forces can manage software supply chain risks and ensure they are protected against them. First, the paper describes the structure of software supply chains and the risks that arise from them. Then, it analyses the specific characteristics of the armed forces that render them more vulnerable to such risks and reviews the impact of major incidents to date in the military sector. Subsequently, it identifies how the armed forces can better protect themselves against the prevailing risks. Finally, it looks at what policymakers and the armed forces can do to ensure that software suppliers reduce the risks associated with their products.

In conclusion, this research paper recommends that policymakers and the Bundeswehr should first determine the requisite level of protection for the various software products — depending on the area of application. The Bundeswehr itself should then take the following measures to protect against software supply chain risks:

- Establish a central point of accountability for managing these risks and task it with drawing up guidelines for dealing with software supply chain risk and the military use of OSS;
- Develop processes for managing software supply chain risk across the entire military — for example, Bundeswehr IT staff should check regularly whether the software products they are using still receive security updates and functional upgrades;
- Build expertise on software supply chain risk management so that the measures listed here are effective;
- Identify vulnerabilities in the Bundeswehr's own systems and software products to stave off potential threats; and
- Root out untrustworthy suppliers to prevent insider attacks.

At the same time, policymakers and the Bundeswehr should make software suppliers reduce the risks associated with their products. To this end, they should:

- Establish the requirements that software suppliers must meet — this research paper proposes six such requirements, including the provision of software composition information and vulnerability exploitability information of products supplied; and
- Provide model contract language, adapt procurement requirements, and amend product liability law to ensure that suppliers meet those requirements.

Taken together, these measures can enable the Bundeswehr to reduce software supply chain risk to an acceptable level without having to forego the advantages that software undoubtedly affords the armed forces.

Introduction

The armed forces rely heavily on software for most of their activities — from administrative tasks and logistics to warfare. For example, situational awareness platforms have become indispensable, and there is virtually no tank, warship, or fighter jet that can function without software. Such software products are the result of complex supply chains comprising software components, software vendors, and service providers that are beyond the control of the armed forces. Consequently, the security of the military depends on the security of numerous software vendors, service providers, developers, and maintainers[1] of software components.

Incidents in the military sector have shown how software supply chain risk can jeopardise the combat readiness of the armed forces.

Incidents in the military sector have shown how software supply chain risk can jeopardise the combat readiness of the armed forces. Administrative operations can be disrupted and troops can be exposed to espionage and sabotage. In the 2010s, Chinese intelligence accessed the systems of the largest US naval shipbuilder to steal intellectual property. In 2019—20, Russia spied on the agency responsible for managing the US nuclear weapons stockpile. And in 2022, on the very first day of the Russian full-scale invasion of Ukraine, Russian military intelligence succeeded in shutting down the satellite communications of the Ukrainian military. In each case, the attackers did not directly target the heavily secured armed forces and defence industrial base; rather, they gained access via the software supply chain.[2]

Thus, it is clear that software supply chain risk is an Achilles heel of today's armed forces and presents a strategic challenge. However, the political and military leadership of Germany — like that of other states — has yet to grasp the importance of this issue. While a group of experts from the German security and defence industry and the Federal Ministry of Defence (BMVg) published a whitepaper in 2021 that contained recommendations for improving the security of IT supply chains,[3] the political and military leadership has yet to follow up on those suggestions. Software supply chain risk in the military sector depends largely on which software products are procured (and from which suppliers) and how they are used and managed. Currently, procurement and IT staff make those decisions, usually on an ad hoc basis. This must change.

Instead, the Bundeswehr should adopt a strategic approach to managing software supply chain risk. This research paper outlines the four steps needed for such an approach. First, policy-makers and the armed forces must understand what software supply chains look like[4] and what risks they pose.[5] Second, they need to be made aware that these risks affect the armed forces, in particular;[6] that is because software has become indispensable for military operations, not least as the military seeks to increasingly network its equipment under the banner of "software-defined defence",[7] which significantly enlarges the potential

1 Maintainers are responsible for security updates and functional upgrades for OSS components and products.

2 These incidents are discussed in the sub-section titled "The Impact of Software Supply Chain Incidents on the Armed Forces", beginning on p. 16.

3 BMVg et al., *Ideenpapier "Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr"* (Berlin, 8 June 2021), https://www.bmvg.de/resource/blob/5103740/9cc683ea3fac46f37290590cc41aa1a6/download-sichere-it-lieferketten-data.pdf. Unless otherwise indicated, all websites cited in this research paper were last accessed on 17 September 2025.

4 See the section titled "The Software Supply Chain", beginning on p. 9

5 See the section titled "Software Supply Chain Risks", beginning on p. 11.

6 See the section titled "The Particular Threat to the Armed Forces", beginning on p. 14.

7 Simona Soare et al., *Software-defined Defence: Algorithms at War* (London: International Institute for Strategic Studies, February 2023), https://www.iiss.org/research-paper/2023/

attack surface. The armed forces should learn from the software supply chain incidents that have already affected the military and the defence industrial base. In a third step, this research paper outlines — based on expert assessments[8] and practical examples from various countries — measures that political and military leaders should take to protect the armed forces from software supply chain risk.[9] Fourth, they should ensure that software suppliers manage the software supply chain risk of their products.[10] By following these four steps, political and military decision-makers can protect this Achilles heel of the armed forces so that the latter are able to fulfil their mission.

02/software-defined-defence/; Nand Mulchandani and 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 The policy recommendations in this research paper are based on more than 65 interviews and a workshop with international experts, among other things.

9 See the section titled "How the Armed Forces Can Protect Themselves Against Software Supply Chain Risk", beginning on p. 19.

10 See the section titled "How Policymakers and the Armed Forces Can Make Software Suppliers Take Action", beginning on p. 27.

The Software Supply Chain

Software products have complex supply chains that include all the artifacts (such as programme code), processes, technologies, and, not least, people involved in making a given piece of software (see Figure 1, p. 10).[11] The supply chain of any software product starts with its "raw materials", that is, the software components. These are the independent units of source code, such as libraries.[12] Such pre-existing components account for the larger part of the codebases of many software programmes because IT professionals reuse already developed code.[13] Both the OSS community and commercially available libraries play a key role in this process.

Software-developing entities, which include vendors,[14] have three options for sourcing software components. First, they can use OSS components from a code repository like GitHub. In this case, they have no contractual relationship with the developers of the component (and usually do not know who they are).[15] Second, they can buy a component from another vendor. And third, they can develop the component themselves.

OSS stands in contrast to proprietary software, where the source code is kept secret because it is considered intellectual property. In the OSS ecosystem, individuals develop and maintain software products or components and make them available to the general public, which can examine the source code and use the software.[16] OSS is the foundation of the modern software ecosystem: almost all software products contain OSS components[17] and OSS products are the leading solutions for certain use cases.[18] By contrast, commercially available libraries maintained by software vendors often cannot be audited and rely on the vendor to fix vulnerabilities.

Each software component has its own supply chain because it relies on components or tools such as compilers, which translate human-readable source code into machine-readable binary code. Since software products can inherit the security problems of all their components, assessing the (in)security of a given software product entails scrutinising each of its components and their subcomponents.

During the development process, software vendors frequently rely on external service providers. For example, software as a service (SaaS) providers depend on cloud infrastructure providers. Such companies often have access to their clients' systems in order to be able to provide their services.

11 SAFECode, *Software Integrity Controls. An Assurance-based Approach to Minimizing Risks in the Software Supply Chains* (Arlington, 14 June 2010), 3, https://safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf.

12 Charles W. Krueger, "Software Reuse", *ACM Computing Surveys* 24, no. 2 (1992), 131—83 (141); Fang Hou and Slinger Jansen, "A Systematic Literature Review on Trust in the Software Ecosystem", *Empirical Software Engineering* 28, no. 1 (2023), doi: 10.1007/s10664-022-10238-y.

13 Krueger, "Software Reuse" (see note 12).

14 Other such entities are individuals or non-for-profit organisations such as OSS foundations. For the sake of clarity, this research paper refers simply to vendors.

15 SAFECode, *Software Integrity Controls* (see note 11), 8.

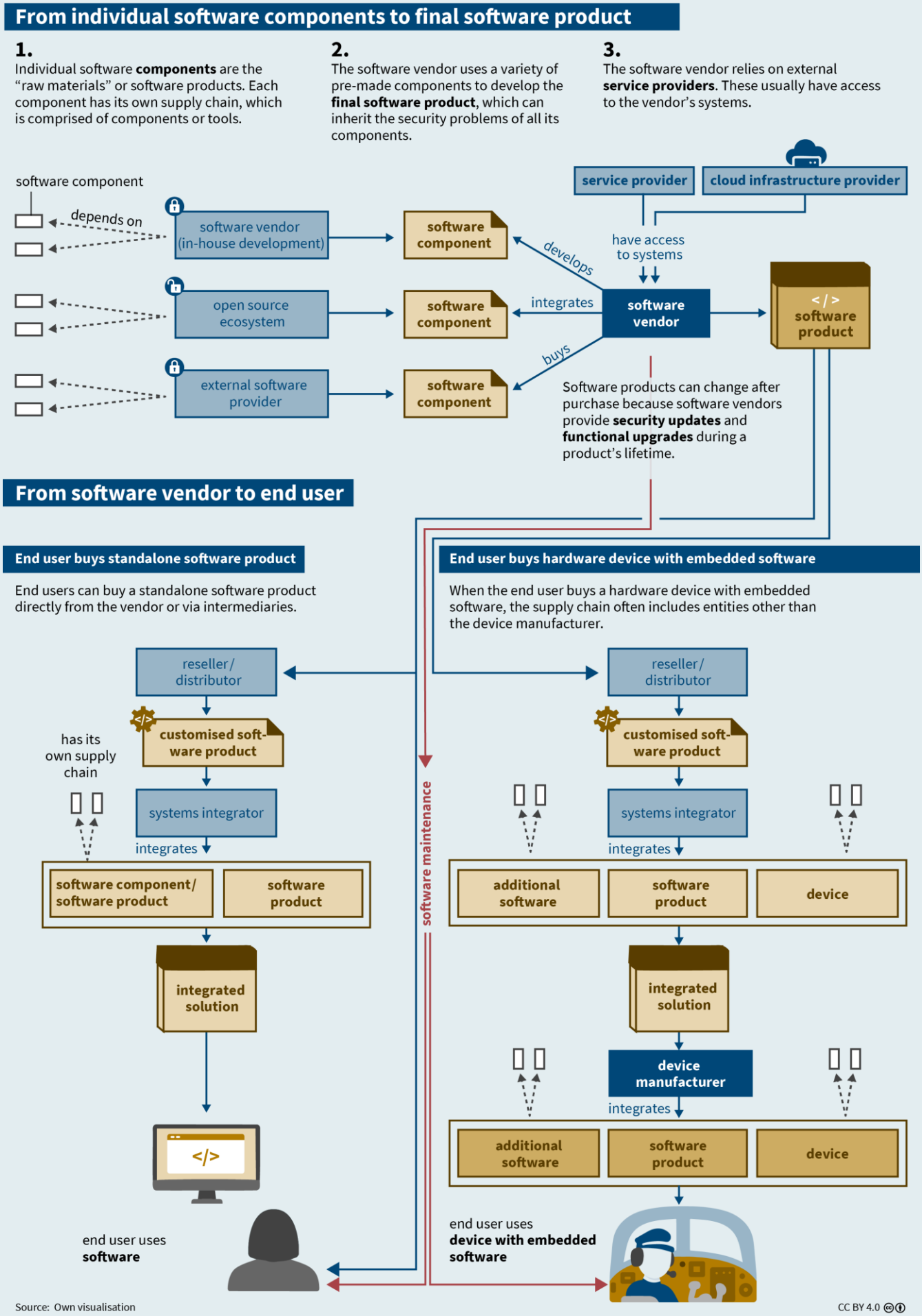
16 There is a debate about whether OSS is, by definition, open for everyone to use (Open Source Initiative, "The Open Source Definition", 16 February 2024, https://opensource.org/osd) or whether OSS licences can exclude certain use cases such as military use (Steve Dierker and Volker Roth, "Can Software Licenses Contribute to Cyberarms Control?" in *Proceedings of the New Security Paradigms Workshop*, ed. Marco Carvalho et al. [New York: ACM, 28 August 2018], 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 et al., "Is Open Source Eating the World's Software?" in *Proceedings of the 19th International Conference on Mining Software Repositories*, ed. David Lo (New York: Association for Computing Machinery, 2022): 561—65, doi: 10.1145/3524842.3528473.

18 Klint Finley, "Linux Took Over the Web. Now, It's Taking Over the World", *Wired*, 25 August 2016, https://www.wired.com/2016/08/linux-took-web-now-taking-world/.

Figure 1

The software supply chain



Source: Own visualisation

Once the software product is finished, it must find its way to the end users —for example, the Bundeswehr. Which path it takes depends initially on whether users are seeking a standalone software product or a hardware device with embedded software. Most devices with information and communication functionalities contain embedded software and will therefore have a software supply chain.

End users can gain access to a standalone software product in three ways: by purchasing either the product, a licence to use the product, or access to a cloud-hosted version (SaaS). Moreover, supply chains differ in terms of whether the end user buys the product (or the right to use it) directly from the software vendor or through intermediaries. The former is often the case for commercial off-the-shelf (COTS) software products, which are made available to a broad customer base without customisation and can often be downloaded directly from the vendor website. Alternatively, there may be other companies that are part of the supply chain, too. These are resellers and distributors (which make the product available to the end customer and often provide additional services such as customisation) and systems integrators (which combine products from various suppliers and adapt them to the customer's needs).

When end users purchase a hardware device with embedded software, they buy the product from the device manufacturer or from the respective reseller, distributor, or systems integrator. For its part, the device manufacturer either develops the embedded software itself or purchases it from one or more software vendors. In the military context, such embedded systems can range from simple COTS devices (such as air-conditioning systems for data centres) to complex weapons systems (such as fighter jets).

Finally, the software supply chain does not end when the purchase is made (or the licence agreement concluded). Rather, software vendors typically offer maintenance for their products in the form of security updates and, in some cases, upgrades that change, add, or remove functionalities. Security updates are essential because most software products contain vulnerabilities,[19] that is, "weakness[es] in an IT system that can be exploited by an attacker to deliver a successful attack".[20] Once vendors learn about a vulnerability, they can provide a mitigation, such as a security update or reconfiguration information.

In short, it is this complex web of software components, software vendors and their suppliers, and service providers that forms the supply chain of every software product.

19 National Cyber Security Centre, A *Method to Assess 'Forgivable' vs 'Unforgivable' Vulnerabilities* (London, 28 January 2025), https://www.ncsc.gov.uk/report/a-method-to-assess-forgivable-vs-unforgivable-vulnerabilities; Black Duck, *Open Source Security & Risk Analysis Report* (see note 17).

20 National Cyber Security Centre, *Vulnerability Management. Advice, Guidance and Other Resources for Managing Vulnerabilities* (London, 12 February 2024), https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities.

Software Supply Chain Risk

Software supply chains harbour a number of risks. These differ from other cybersecurity risks in one important respect: in "conventional" cybersecurity incidents, threat actors typically gain access to their target and cause damage there (see Figure 2). For example, attackers may send a phishing email to infiltrate a company's IT system and install ransomware. By contrast, software supply chain risk originates upstream in the supply chain: for example, attackers may exploit a vulnerability in the IT systems of a software vendor in order to gain control of its update server; and they may go on to "hijack" the update process by inserting ransomware into the software update, which is then installed on the systems of all the vendor's customers.[21]

There are three transmission mechanisms that allow software supply chain risk to move downstream in the supply chain, often to end users:

1. The software product itself can be manipulated, either at the time of installation or through updates;
2. Individual components of the product can be modified — in contrast with the first transmission mechanism, this does not require access to the vendor's systems, making transmission even more difficult to detect; and
3. Access to the product granted to service providers, for example, can be abused.

Not all experts see the last of these transmission mechanisms as a software supply chain problem. That is because in such cases, the software product or its components are not necessarily modified; rather, such incidents tend to be classified as third-party risk. However, despite this technical difference, security incidents resulting from third-party access and those in which third parties manipulate the software product or its components are very similar; and it is often the case that the same measures can mitigate both types of risk. For this reason, abuse of access is classified as a software supply chain risk here.

From the end user's perspective, software supply chain risk poses four issues. First, such events often affect a large number of organisations at the same time — for example, when all customers of a particular software vendor are affected.[22] Second, almost all software supply chains contain entities that lack adequate cybersecurity protection, such as SMEs or smaller OSS projects that are maintained by only a few individuals or even just one person as a hobby.[23] As a result, it is very likely that even software users with rigorous cybersecurity measures in place — such as the armed forces — are highly vulnerable through the supply chains of the software products they use. Third, end users typically have limited visibility into the supply chain and may not even know they are exposed to a cyber threat. And fourth, it is often the case that neither end users nor their immediate suppliers can address the root causes of software supply chain risk because the problem lies far upstream in the supply chain (with smaller software vendors, service providers, or the OSS ecosystem) and it is only there that remedial measures can be implemented.

All these issues mean that managing software supply chain risk is an urgent consideration for software users in general but especially for those which — like the armed forces — particularly value a high level of security. There are four categories of software supply chain risk: third-party supply chain attacks, insider attacks, inadvertent mistakes, and lack of maintenance (see Figure 2).

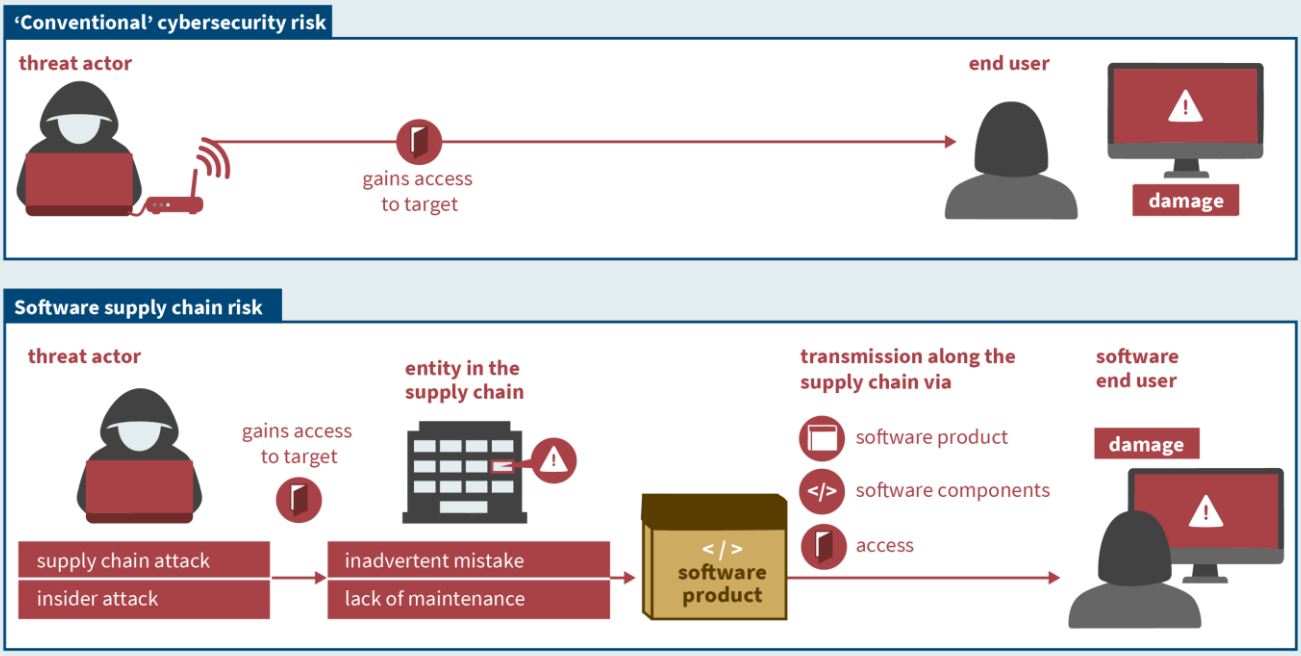
21 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 21 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

22 Trey Herr et al., *Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain* (Washington, D.C.: Atlantic Council, 26 July 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), 4, https://4008838.fs1.hubspotusercontent-na1.net/hubfs/4008838/2024-tidelift-state-of-the-open-source-maintainer-report.pdf.

Figure 2

Software supply chain risk



Source: Own visualisation

Third-party Supply Chain Attacks

In third-party supply chain attacks, threat actors who are not part of the supply chain of a software product gain access to an entity that is part of the chain in order to compromise another entity downstream in the same chain.[24]

Insider Attacks

Insider attacks are carried out by actors who are part of the supply chain of a software product. In non-software-related scenarios, employees turn against their employer, either of their own accord or under the influence of third parties such as foreign intelligence services.[25] At the same time, adversarial actors can become insiders owing to changes in the ownership structure of a company, for example, when a government agency gains control over a company that is part of a particular supply chain. And at international companies, it is also possible for citizens of adversarial states — who are subject to national disclosure requirements or can be instrumentalised — to become part of the software supply chain via subcontractors.[26]

Other scenarios arise from the specific structure of the OSS ecosystem. Since most software vendors who

24 Alexandra Paulus and Christina Rupp, *Government's Role in Increasing Software Supply Chain Security: A Toolbox for Policy Makers* (Berlin: Interface, March 2023), 18, https://www.interface-eu.org/publications/governments-role-increasing-software-supply-chain-security-toolbox-policy-makers. The sub-section of this research paper titled "The Impact of Software Supply Chain Incidents on Armed Forces", beginning on p. 16, contains three analyses of such attacks: the "Cloud Hopper" campaign, the "Sunburst" campaign, and the Viasat incident.

25 See, e.g., Codi Starks et al., "Staying a Step Ahead: Mitigating the DPRK IT Worker Threat", *Google Cloud Blog*, 23 September 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", *The Telegraph*, 2 August 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 July 2025, https://www.propublica.org/article/microsoft-digital-escorts-pentagon-defense-department-china-hackers.

use OSS components will not know who the developers and maintainers of those components are, there is a blind spot in their supply chain that can serve as a gateway for malicious insiders. In the case of the "XZ Backdoor",[27] for example, one or more unknown threat actor(s) took over the maintenance of the OSS component "XZ Utils" between 2022 and 2024 and inserted a backdoor.[28] This popular library is used, among other things, for remote access to Linux servers; and the backdoor would have allowed the perpetrator(s) to seize control of the affected devices, including most servers worldwide.[29] Fortunately, thanks to a series of coincidences, the malicious code was discovered and removed before it could cause damage.[30] Still, malicious OSS components are a widespread problem.[31] Because they are often located at the very beginning of software supply chains, the potential blast radius of a compromise can be huge.

Inadvertent Mistakes

Software supply chain risk can arise even without deliberate acts by third parties, for example, through inadvertent mistakes by entities in the supply chain. Both OSS developers and maintainers can make mistakes, as can proprietary software vendors. And those mistakes potentially lead to vulnerabilities in the software product, which are open to exploitation by malicious actors.[32]

Lack of Maintenance

The fourth category of risk posed by software supply chains arises when a vendor no longer maintains a software product. In the absence of functional upgrades, some products (over time) lose their functionality. And without security updates, software products accumulate known but unpatched vulnerabilities. Thus, over time, unmaintained software becomes an easy target. Furthermore, when SaaS providers stop making their services available for all or certain users, the latter immediately lose access to the software.

Software products can lack maintenance for various reasons: users do not pay for maintenance, the vendor stops providing maintenance,[33] the vendor goes out of business or the (often sole[34]) maintainer of an OSS project stops working on that project, or the vendor chooses not to provide maintenance for certain end users, for example, as a result of sanctions. And even if the vendor is still providing support for a product, an embedded OSS component may no longer be maintained — and the vendor may not be aware of this.

27 This incident is depicted visually in Figure 4 on p. 18.

28 Evan Boehs, "Everything I Know about the XZ Backdoor", *Evan Boehs* (online), 29 March 2024, https://boehs.org/node/everything-i-know-about-the-xz-backdoor.

29 Thomas Roccia, "The XZ Backdoor Story", *Speaker Deck* (online), 8 September 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 May 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", *Lawfare*, 9 April 2024, https://www.lawfaremedia.org/article/backdoor-in-xz-utils-that-almost-happened.

30 Kevin Roose, "Did One Guy Just Stop a Huge Cyberattack?" *The New York Times*, 3 April 2024, https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html.

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

32 The sub-section titled "The Impact of Software Supply Chain Incidents on Armed Forces", beginning on p. 16, explains the 2024 CrowdStrike incident, which is an example of this category of risk.

33 Vendors sometimes make exceptions under paid service agreements or following the discovery of extremely critical vulnerabilities.

34 Tidelift, *The 2024 Tidelift State of the Open Source Maintainer Report* (see note 23), 6.

The Particular Threat to the Armed Forces

The four categories of software supply chain risk can affect all organisations, but the armed forces are particularly vulnerable.

The Importance of Software for the Armed Forces

The armed forces have a broad portfolio of different software products (see Figure 3, p. 16). Like civilian organisations, they use software to support processes and process information; these supporting applications include office programmes and enterprise resource planning systems. At the same time, the armed forces need battlefield applications such as situational awareness platforms and command and control systems. Moreover, they work with classified information and the systems that process such data must meet additional security requirements. All these applications rely on a vast range of other types of software, such as operating systems and databases.

In short, software is indispensable for most activities in the military sector. What is more, most military equipment is dependent on software; for example, software often allows functional enhancements of weapons systems such as warships, whose lifetime can thereby be extended. Consequently, software supply chain risk affects the entire spectrum of military activity. The impact depends on the type of software affected: the compromise of a COTS product can deliver valuable information to intelligence services, but sabotage operations are much more dangerous when their target is battlefield applications such as weapons systems.

A Growing Dependency

Software already plays an important role in today's weapons systems. But so far, many large platforms have only limited connectivity — to other platforms, sensors, and networks such as the internet.[35] To a certain extent, this lack of connectivity mitigates the existing software supply chain risk.[36]

However, the armed forces of many countries, including Germany's Bundeswehr, are striving to further digitise their processes, connect more devices and platforms, and put software at the heart of the battlefield. The concept of "software-defined defence"[37] (SDD) refers to a future in which large weapons platforms can be controlled via a central software platform and the functionality of military equipment can be changed through software updates, instead of hardware modifications.

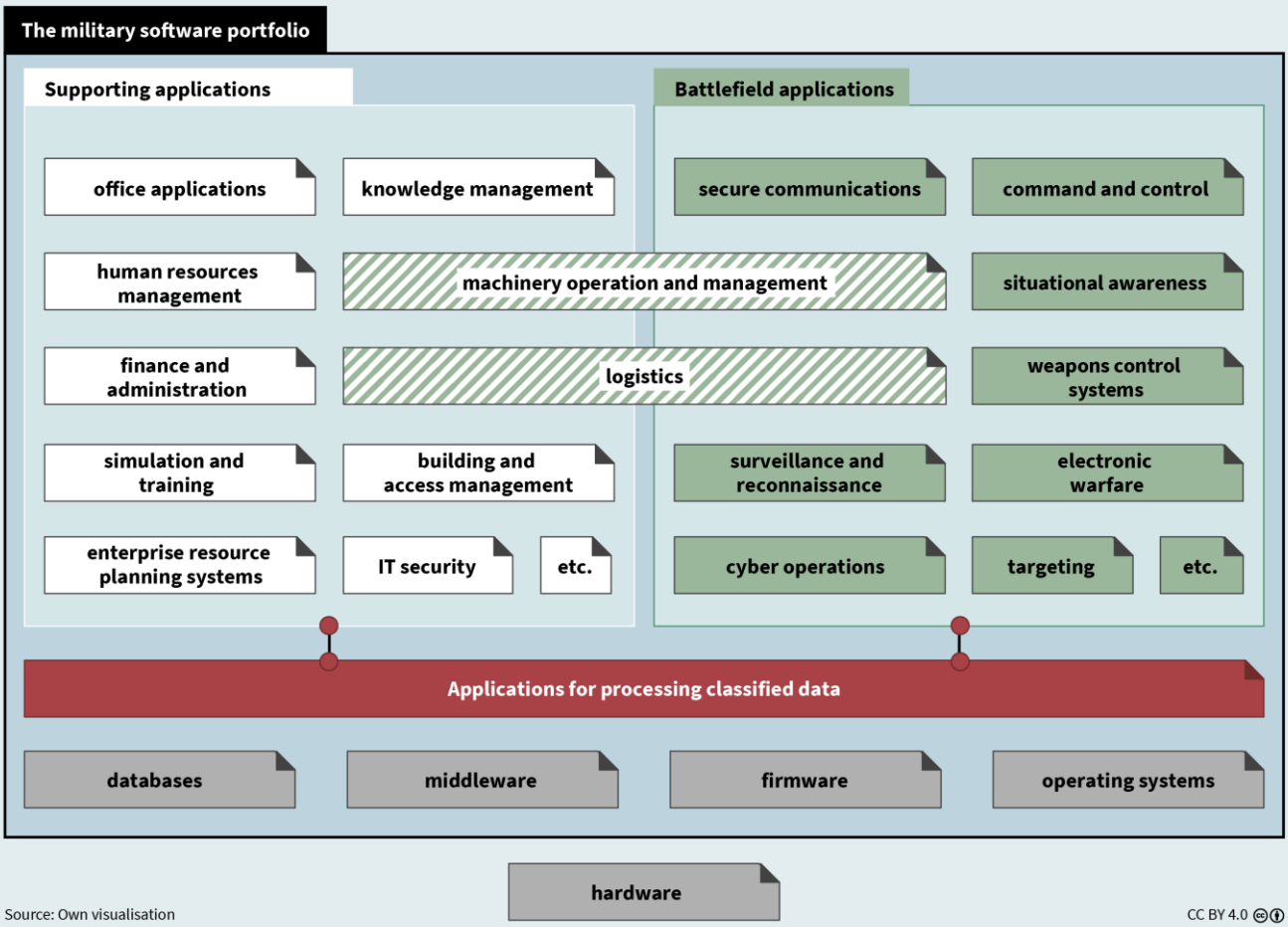
Armed forces that cannot fulfil their mission without software will be even more exposed to software supply chain risk.

Most armed forces are still a long way from realising this concept,[38] but some have already taken the

35 Christian Brose, *The Kill Chain. Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020).
36 However, the Stuxnet incident showed that even air-gapped systems can be vulnerable to attack; see Kim Zetter, *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).
37 Mulchandani and Shanahan, *Software-Defined Warfare* (see note 7); Soare et al., *Software-defined Defence* (see note 7); *Software Defined Defence. Positionspapier des BDSV, BDLI, Bitkom und BMVg* (Berlin, 31 October 2023), https://www.bmvg.de/resource/blob/5711942/6fb70a45412601fdf03f63aeebf72451/cyber-defined-defence-papier-data.pdf. Previously, similar ideas were discussed under the term "network-centric warfare" — see, e.g., Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future", in *Proceedings of the Naval Institute* 124 (1998): 28—35.
38 Soare et al., *Software-defined Defence* (see note 7), 3f.

Figure 3

The military software portfolio



Source: Own visualisation

first steps in this direction.[39] Thus, the following conclusion about the importance of software for the armed forces of tomorrow can be drawn: Armed forces that cannot fulfil their mission without software will be even more exposed to software supply chain risk.

Military Idiosyncrasies Exacerbate the Threat

At the same time, there are four characteristics peculiar to the military that increase software supply chain risk for the armed forces. First, the main task of the armed forces is to prevent war, based on their warfighting capabilities. Accordingly, supply chain incidents in the military sector can endanger people, infrastructure, and resources. The threat can be both direct (such as an attack on software that controls weapons systems) and indirect (for example, adversarial intelligence services gathering information about military bases). Since military operations must continue even under extraordinary circumstances, inadvertent mistakes — such as those that disrupt logistics systems — or a lack of software maintenance can have dramatic consequences.

Second, the armed forces are often dependent on IT systems owned and operated by others.[40] For national

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/.

40 Bundeswehr, *Operations Plan Germany. A Whole-of-Government and Whole-of-Society Task* (Berlin, 2025), https://www.

defence, military logistics frequently rely on and interact closely with critical civilian infrastructure;[41] and within a military alliance, the same applies to allies' systems. Accordingly, the armed forces are confronted with the problem that there are parts of their software supply chain that they do not know about and in which they cannot take steps to manage risk.

Third, the armed forces rely on specialised defence suppliers not only for weapons platforms but also for software, which makes them dependent both on those vendors and on their proprietary technologies ("vendor lock-in").[42] Such dependence puts the armed forces in a weak negotiating position vis-à-vis their suppliers when it comes to enforcing stricter measures for dealing with risk in the software supply chain. Moreover, there is often no alternative available when a software product lacks maintenance.

Fourth, when procuring software, the armed forces have to comply with procurement rules (including at the EU level).[43] The procedures to be followed are not only slow and frequently complex (involving many different entities); they were also developed for hardware devices — namely, weapons systems — and therefore often lack the speed and flexibility that are crucial for software procurement.

Thus, while software supply chain risk affects all organisations, its potential impact on the military is particularly serious.

The Impact of Software Supply Chain Incidents on the Armed Forces

The armed forces of various countries have already felt the devastating impact of software supply chain incidents (see Figure 4, p. 18). Those incidents have led not only to operational disruptions but also to espionage and sabotage.

Operational Disruptions

Even inadvertent mistakes by software vendors can bring the operations of organisations worldwide to a standstill. In 2024, the US software company CrowdStrike, which specialises in cybersecurity applications, released a faulty automatic update for all customers worldwide using its "Falcon" software.[44] Devices that received the update automatically restarted and suffered a system crash during startup, rendering them temporarily inoperable. An estimated 8.5 million affected devices worldwide had to be manually reset — a task that required physical access to each device in the case of those with hard disk encryption.[45] The US Department of Defense (DoD) and several defence contractors were using Falcon,[46] but it was announced that there had been "no impact on DoD operations".[47]

bundeswehr.de/resource/blob/5953068/42312779260a2b14ba61d863e357d9e9/booklet-operations-plan-for-germany-data.pdf.

41 Defense Management Institute, *Department of Defense Dependencies on Critical Infrastructure* (Alexandria, 27 September 2024), https://www.dmi-ida.org/knowledge-base-detail/Department-of-Defense-Dependencies-on-Critical-Infrastructure-Executive-Summary; Annie Fixler et al., *Military Mobility Depends on Secure Critical Infrastructure* (Washington, D.C.: Cyberspace Solarium Commission 2.0, 27 March 2025), https://cybersolarium.org/csc-2-0-reports/military-mobility-depends-on-secure-critical-infrastructure/.

42 Lai Xu and Sjaak Brinkkemper, "Concepts of Product Software", *European Journal of Information Systems* 16, no. 5 (2007): 531—41.

43 See BMVg, *Project-based Procurement and In-Service Use. A-1500/3* (Berlin, 23 May 2024), https://www.bundeswehr.de/resource/blob/1718386/d21a4f590da15adad3aecd560f3cc5cc/cpm-en-data.pdf; European Parliament and Council, *Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC* (Brussels, 25 June 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0081.

44 "Remediation and Guidance Hub: Channel File 291 Incident", *CrowdStrike*, 6 August 2024, https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.

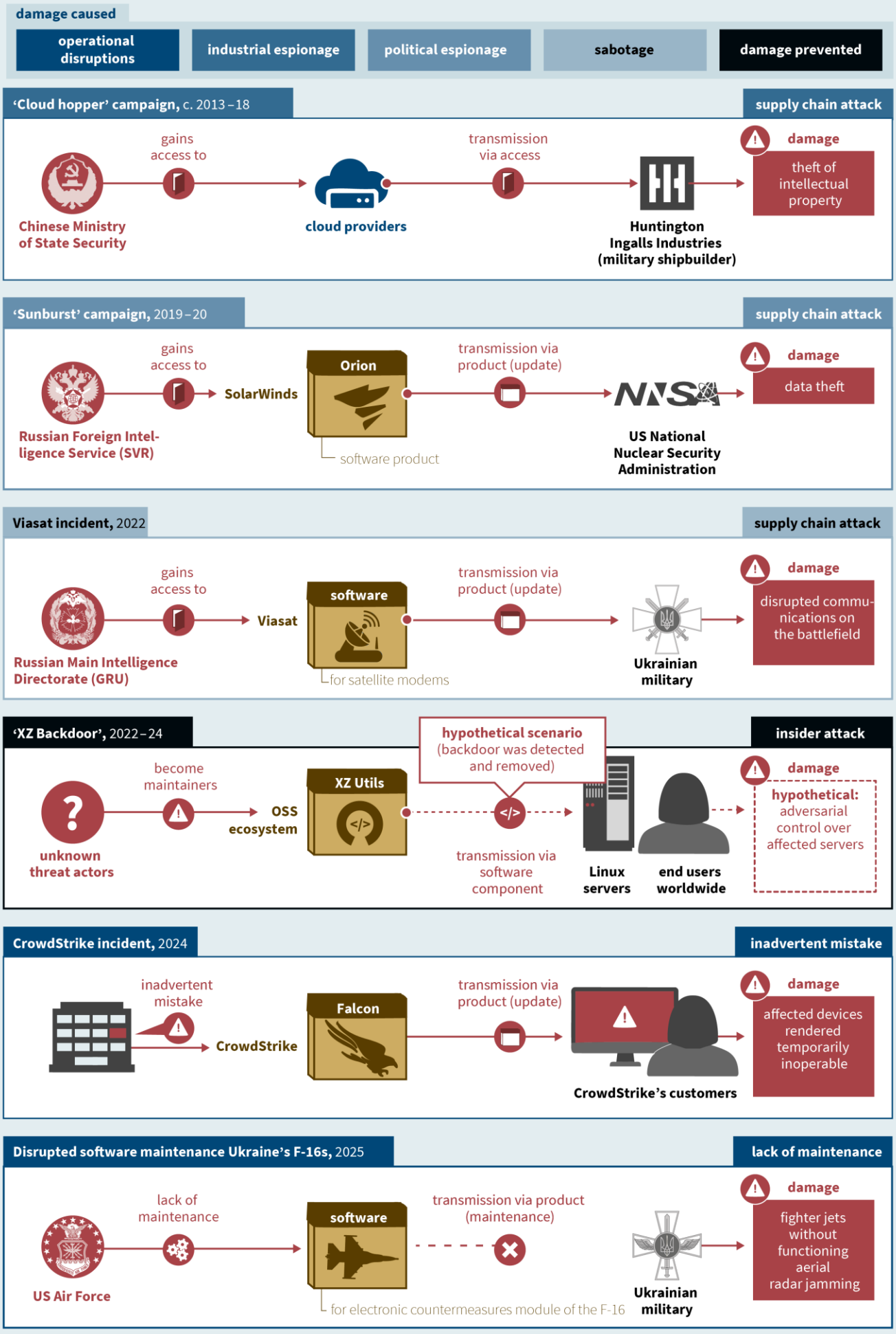
45 James Coker, "CrowdStrike Fault Causes Global IT Outages", *Infosecurity Magazine*, 19 July 2024, https://www.infosecurity-magazine.com/news/crowdstrike-fault-it-outages/; David Weston, "Helping Our Customers through the CrowdStrike Outage", *Official Microsoft Blog*, 20 July 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

46 "CrowdStrike Achieves IL5 Authorization to Secure U.S. Department of Defense", press release, *CrowdStrike*, 31 May 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 July 2024, http://breakingdefense.com/2024/07/joint-chiefs-chairman-says-dod-operations-not-affected-by-widespread-crowdstrike-glitch/.

Figure 4

Major software supply chain incidents with a military dimension



Source: Own visualisation

Nevertheless, the incident demonstrated the potential far-reaching consequences of even an inadvertent mistake being made by an entity in the software supply chain.

Furthermore, certain military equipment is rendered unusable without regular software upgrades. For example, the F-16 fighter jet, which is now part of the Ukrainian military fleet, has an electronic countermeasures module that enables radar jamming during flight.[48] This capability prevents enemy ground stations from targeting aircraft with missiles and shooting them down. For effective radar jamming, the relevant software must be regularly updated to match the radar frequency ranges used by enemy ground stations, which change over time. Without those upgrades, the aircraft lose their defensive capabilities and would presumably remain grounded.[49] For the Ukrainian F-16s, it is only the US Air Force that is able at this time to provide the necessary software updates.[50] In March 2025, the Trump administration temporarily suspended military aid to Ukraine, which included software maintenance for the F-16s.[51] Although Washington quickly reversed course,[52] the episode highlights the impact that the lack of software maintenance can have on the operational readiness of large weapons systems.

Industrial Espionage, Political Espionage, and Sabotage

Besides operational disruptions, which can cause considerable damage without any attackers being involved, the software supply chain offers entry points for malicious actors targeting the armed forces and the defence industry (see Figure 4). First, there are state actors and private companies that engage in industrial espionage, that is, the theft of intellectual property. For at least six years in the 2010s, individuals associated with the Chinese Ministry of State Security stole intellectual property from Western companies as part of the "Cloud Hopper" campaign. They infiltrated cloud providers and exploited the latter's access to their customers' systems.[53] One of the targets of the campaign was Huntington Ingalls Industries, the largest military shipbuilder in the United States, which, among other things, builds nuclear-powered submarines for the US Navy.[54]

Second, intelligence agencies engage in political espionage. In 2019–20, as part of the "Sunburst" campaign, Russia's Foreign Intelligence Service (SVR) injected malware into updates from the US company SolarWinds,[55] whose "Orion" software serves to monitor and manage infrastructures. Using the malicious code distributed to Orion users via updates, the SVR gained access to, among other things, systems of the DoD and the National Nuclear Security Administra-

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", *Forbes*, 7 March 2025, https://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 March 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 August 2024, https://www.acc.af.mil/News/Article-Display/Article/3885756/dominate-the-spectrum-350th-sww-enables-ew-capabilities-for-ukrainian-f-16s/; US Defense Security Cooperation Agency, *Ukraine – F-16 Sustainment Services*, 10 December 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!" (see note 49).

52 "After Trump's Freeze, US Military Aid to Ukraine Resumes — Poland Confirms", *Kyiv Post*, 12 March 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 December 2018), https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion; PwC UK and 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 et al., "Stealing Clouds", *Reuters*, 26 June 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

55 Trey Herr et al., *Broken Trust: Lessons from Sunburst* (Washington, D.C.: Atlantic Council, 29 March 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst.

tion, which oversees the US nuclear weapons stockpile.[56]

Third, some intelligence agencies and armed forces exploit vulnerabilities in software supply chains for sabotage purposes — that is, in order to temporarily disrupt or permanently destroy networks, systems, or services. For example, Russia's Main Intelligence Directorate (GRU), the country's military intelligence agency, hijacked the update mechanism of the satellite communications provider Viasat.[57] On 24 February 2022 — the very first day of the Russian full-scale invasion of Ukraine — the GRU delivered malicious software to the modems of Viasat's customers via an automatic update.[58] The malware overwrote important data in the memory of the modems, rendering those devices inoperable.[59] The presumed target was the Ukrainian military, which was relying on Viasat's services for its connectivity on the battlefield. The exact impact of the attack is unclear, partly because the satellite communication services to the Ukrainian military were also being provided by the company Starlink.[60]

It is also conceivable that cybercriminals target military entities for financial gain. So far, no financially motivated software supply chain attack on military targets has been publicly disclosed. But this could be because such targets are generally better secured than other sectors and because state entities, such as the armed forces, are not inclined to negotiate with criminals (for example, over ransom payments). Furthermore, it is often the case that an attack on a military target is not made public. For this reason, it can be assumed that not only have there been incidents that have simply not become public knowledge but also that some incidents known to the public have had an undisclosed military dimension.

Finally, the software supply chain might not always be the entry point of choice for attacks on military targets. For espionage or sabotage operations, it could be easier to simply pay or bribe insiders. And to achieve military objectives in an armed conflict, it is often cheaper and faster to take out enemy positions through kinetic means rather than through cyber operations.[61]

56 Adam Janofsky, "Cyber Command: 'No Evidence' That SolarWinds Attackers Compromised DoD Networks", *The Record*, 17 November 2022, https://therecord.media/cyber-command-no-evidence-that-solarwinds-attackers-compromised-dod-networks; Natasha Bertrand and Eric Wolff, "Nuclear Weapons Agency Breached Amid Massive Cyber Onslaught", *Politico*, 17 December 2020, https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855; Herr et al., *Broken Trust* (see note 55).

57 "Russia behind Cyber-Attack with Europe-Wide Impact an Hour Before Ukraine Invasion", *Foreign, Commonwealth & Development Office* (London, 10 May 2022), https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion; Nick Saunders et al., "Space Cybersecurity Incident Response Framework: A Viasat Case Study", in *2025 IEEE Aerospace Conference*, 1—15, doi: 10.1109/AERO63441.2025.11068784.

58 Saunders et al., "Space Cybersecurity Incident Response Framework" (see note 57); Katrina Manson, "The Satellite Hack Everyone Is Finally Talking About", *Bloomberg*, 1 March 2023, https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/.

59 Juan Andres Guerrero-Saade and Max van Amerongen, "AcidRain: A Modem Wiper Rains Down on Europe", *SentinelOne*, 31 March 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 December 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 December 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 and Mika Kerttunen, *Cyber Operations in Russia's War Against Ukraine. Uses, Limitations, and Lessons Learned so Far*, SWP Comment 23/2023 (Berlin: Stiftung Wissenschaft und Politik, April 2023), doi: 10.18449/2023C23; Frederik A. Pedersen and Jeppe T. Jacobsen, "Narrow Windows of Opportunity: The Limited Utility of Cyber Operations in War", *Journal of Cybersecurity* 10, no. 1 (2024), doi: 10.1093/cybsec/tyae014.

How the Armed Forces Can Protect Themselves Against Software Supply Chain Risk

Incidents such as those discussed above show how software supply chain risk can impair the combat readiness of the armed forces. Thus, the Bundeswehr should acknowledge that risk and identify possible courses of action to counter it.

The measures proposed in this and the following section stem from a three-stage analysis. First, based on the risks described above, particularly to the armed forces, the analysis establishes which security problems exist. Second, where possible, an international comparison is made to examine the measures that armed forces have successfully implemented. In those cases where no relevant international experience is available, the analysis draws on international expert assessments obtained in more than 65 interviews and one workshop.[62] Third, on the basis of these international examples and expert assessments, recommendations are made about which measures the BMVg and the Bundeswehr should implement.

The proposed measures fall into two categories. First, the armed forces can take measures to protect themselves, as outlined below in this section (see Figure 5, p. 22). Second, policymakers and the armed forces can formulate requirements for software suppliers on how to make their products less vulnerable to software supply chain risk and how to support the armed forces in their risk management. The next section explains what those requirements might be and how policymakers and the armed forces can make suppliers implement them. Effectively dealing with software supply chain risk in the military sector demands that these two (complementary) approaches be combined.

The measures proposed below would entail profound changes for the armed forces of many countries and require considerable resources. Thus, it cannot be ruled out that in some cases, there would be resistance. In such cases, the measures could be tested initially on a small scale — for example, in a suitable military unit.[63]

The Appropriate Level of Protection

Even though the impact of software supply chain risk can be devastating, the Bundeswehr cannot respond by abandoning software use altogether or avoiding any dependency on third parties in the software supply chain. Given the complexity of the software ecosystem, such a response would be virtually impossible to implement and highly inefficient. Instead, the Bundeswehr should consciously seek to manage software supply chain risk.

To this end, policymakers and the Bundeswehr must resolve certain trade-offs.[64] On the one hand, software

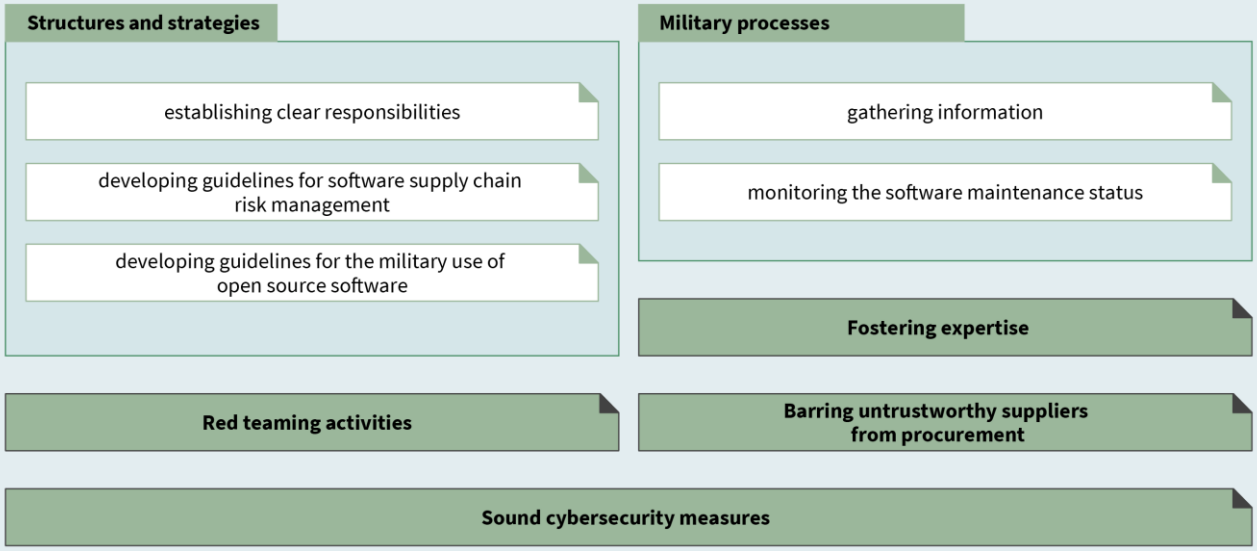
62 The author is very grateful to workshop participants Amy Ertan, Andrew Dwyer, Chris Wysopal, Christoph Lobmeyer, Clotilde Bômont, Colin Topping, Daniel Voelsen, James Shires, John Scott, John Speed Meyers, Jörg Eschweiler, Marc Lanouette, Philip Engelmartin, Sara Ann Bracket, Sebastian Lange, and Simon Stanley.

63 Probasco, "Building the Tech Coalition" (see note 39), 9.

64 Another question is whether the armed forces should focus primarily on managing risk in their own software supply chains or on exploiting vulnerabilities in the software supply chains of their adversaries. While this topic is beyond the scope of this research paper, the arguments are similar to those in the debate on dealing with software vulnerabilities in general; see, for example, Sven Herpig, *Governmental Vulnerability Assessment and Management. Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities* (Berlin: Interface, August 2018), https://www.interface-eu.org/storage/archive/files/vulnerability_management.pdf.

Figure 5

How the armed forces can protect themselves against software supply chain risk



Source: Own visualisation

used by the armed forces should pose only known and acceptable security risks; on the other hand, it should provide a certain functionality, be available at a reasonable price, and lend itself to rapid deployment and updating. These objectives are often at odds with one another: many measures that reduce software supply chain risk make the product more expensive — for example, when a functionality is developed from scratch instead of based on an existing OSS component. In addition, many risk management measures slow down the procurement and deployment process. This is the case, for example, when the armed forces conduct security tests for updates before rolling them out or when they close vulnerabilities in OSS components embedded in a product before deploying it (at considerable personnel expense[65]).

There is no single entity in the Bundeswehr that has overall responsibility for procuring and managing software.

In short, the goal should not be to reduce software supply chain risk at any cost. A software product with very low risk is useless if it does not offer the required functionality, is too expensive, or is simply delivered or updated too late. Rather, the BMVg and the armed forces need to co-determine the appropriate level of protection. Given the military's diverse software portfolio, that level should differ from product to product. For example, products used on the battlefield or for processing classified information require greater protection. Accordingly, the measures proposed below should be applied in a targeted manner to the different parts of the military's software portfolio.

Structures and Strategies

The first step towards effectively managing software supply chain risk is to establish structures and strategies. The BMVg and the Bundeswehr should clearly assign roles and responsibilities to specific departments and individuals and develop guidelines that set appropriate priorities. Even though it is unlikely that a military would restructure itself solely for the purpose of limiting software supply chain risk, the issue should be on the table in the event of a reorganisation. The current reorganisation of the Bundeswehr's Cyber and Information Domain Service (CIR) following its elevation to an independent service is such an event.

65 John S. Meyers, "How to Fix the Military's Software SNAFU", *Defense One*, 4 April 2024, https://www.defenseone.com/ideas/2024/04/how-fix-militarys-software-snafu/395489/.

Clear Responsibilities

Many of the measures proposed here require that one person be responsible for dealing with software supply chain risk in the military sector.[66] Such a clear assignment of responsibility can be found, for example, in the Dutch Ministry of Defence, where a central office is responsible for all IT procurement and software management throughout the entire product life cycle.[67] Accordingly, this office is well positioned to determine how to deal with software supply chain risk. By contrast, there is no single entity in the Bundeswehr that has overall responsibility for procuring and managing software; instead, responsibility is distributed among many different entities (see info box).

The Bundeswehr should follow the example of the Dutch military by assigning responsibility for all aspects of managing software supply chain risk to a single entity. The holder of this position should address the issue with the military leadership and monitor the implementation of the measures proposed here. To avoid creating additional administrative structures, the responsibility should be assigned to the chief information security officer of the Bundeswehr (CISOBw), who oversees information security and can give orders to the whole Bundeswehr in this area. It is crucial that the person responsible has sufficient staff and can assert themself against other officials, for example, when it comes to the distribution of funds.

In addition, the Bundeswehr agencies responsible for software procurement (BAAINBw, BAIUDBw, and BWI) should each appoint a representative whose main task is to deal with software supply chain risk and who enables the agency's procurement staff to put the measures proposed here into practice. Furthermore, there should be someone at the BMVg with explicit responsibility for managing software supply chain risk.

Who in the Bundeswehr is responsible for managing software supply chain risk?

- The Directorate-General for Innovation and Cyber (IC) of the BMVg provides broad political guidance.
- BWI GmbH, an IT service provider owned by the BMVg, is responsible, above all, for the procurement and operation of administrative applications.
- For software products not procured by BWI, the Bundeswehr Centre for Digitalisation and Cyber and Information Domain Service Capability Development (ZDigBw) defines the capability requirements. For devices (including those with embedded software), the Bundeswehr Office for Defence Planning performs this task.
- Based on these capability requirements, project managers at the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw) are responsible for the procurement of products.
- The Federal Office of Bundeswehr Infrastructure, Environmental Protection and Services (BAIUDBw), which is responsible for building and infrastructure construction, procures software and hardware for building technology and IT infrastructure.
- The Bundeswehr Technical Center for Information Technology and Electronics (WTD 81) and a department within the ZDigBw test and assess selected software products.
- The Bundeswehr Cyber Security Centre (ZCSBw) is responsible for cybersecurity incident detection and response. Its tasks also include collecting and evaluating information on software vulnerabilities and accrediting IT products.
- Within each unit and on each project, IT staff are responsible for the life cycle management of the software products in their portfolio.

Guidelines for Software Supply Chain Risk Management

Moreover, international experts believe that a comparison with IT security in general, for example, shows that the armed forces need guidelines for dealing with software supply chain risk. However, no military has yet published comprehensive guidelines on this subject. This research paper argues that the BMVg and the Bundeswehr should draw up such guidelines.

Besides the specific points outlined in the following sub-sections, the guidelines should provide guidance on the desired level of protection, on assessing

66 Federal Office for Information Security (BSI), *Grundlagen des Cyber-Supply Chain Risk Management (C-SCRM)* (Bonn, October 2023), https://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* (The Hague), https://english.defensie.nl/organisation/materiel-and-it-command.

the criticality of a software product to determine the degree of acceptable risk and the resources to be invested, and on identifying and dealing with dependencies on individual components, suppliers,[68] and countries.[69] In addition, the armed forces should ensure that the processes and rules discussed in this and the following section are incorporated into military regulations so that as many of them as possible are binding. And the CISOBw should implement the guidelines and regularly evaluate their effectiveness. There is no need for a separate document to be drawn up, as the guidelines can be integrated into existing IT security guidelines.

Guidelines for the Military Use of Open Source Software

Given the crucial role that OSS plays in almost all software products, the OSS ecosystem should be taken into account in software supply-chain risk management — as a source of both risks and solutions. Since the OSS ecosystem functions differently from that of proprietary software, separate guidelines for the military use of OSS are necessary.[70] For its part, the US DoD has already drawn up comprehensive documents on this issue.[71] The BMVg and the Bundeswehr should similarly draw up guidelines for the military use of OSS.

That document should define the objectives and actions for coordinating and, if desired, promoting the use of OSS products by the armed forces. The first step should be to take stock of the OSS products and components used by the Bundeswehr and assess their criticality and security — a process that should be accompanied by a dialogue with suppliers that use OSS components in their products. In addition, the guidelines should make it easier for technical staff to procure and use OSS products by adapting OSS-specific procurement requirements and providing model contract language, strategies for use, and security assessments. Furthermore, the document should specify how the Bundeswehr can contribute to securing critical OSS components — either by paying other organisations to implement such security measures[72] or by having its own IT specialists participate in OSS projects.[73] Finally, the guidelines should be consistent with general government principles on the use of OSS.[74]

An Open Source Programme Office for the Military

A new structure can help achieve the goals set out in the guidelines — for example, an open source programme office (OSPO), which many companies and some governments have already established.[75] An OSPO is a central point of contact for questions about OSS processes and use within an organisation.[76] In

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

69 See also the sub-section "Barring Untrustworthy Suppliers from Procurement", beginning on p. 26.

70 Sven Herpig, *Fostering Open Source Software Security. Blueprint for a Government Cybersecurity Open Source Program Office* (Berlin: Interface, 31 May 2023), 16, https://www.interface-eu.org/index.php/publications/fostering-open-source-software-security. The military use of OSS has implications far beyond the management of software supply chain risk that are not discussed here.

71 Chief Information Officer (CIO) at the DoD, *Memorandum: Software Development and Open Source Software* (Washington, D.C., 24 January 2022), https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf; id., *Open Source Software FAQ* (Washington, D.C., 28 October 2021), https://dodcio.defense.gov/Open-Source-Software-FAQ/; id., *Open Technology Development (OTD). Lessons Learned and Best Practices for Military Software* (Washington, D.C., 16 May 2011), https://dodcio.defense.gov/portals/0/documents/foss/otd-lessons-learned-military-signed.pdf.

72 For example, the Federal Ministry for Economic Affairs and Energy funds the Sovereign Tech Agency, which, in turn, supports individuals and organisations dedicated to securing OSS; see "Sovereign Tech Agency. Investing in the Infrastructure of the 21st Century", *Sovereign Tech Agency* (online) (Berlin, 25 April 2025), https://www.sovereign.tech/.

73 Herpig, *Fostering Open Source Software Security* (see note 70), 17; Sara A. Bracket et al., *O$$ Security: Does More Money for Open Source Software Mean Better Security? A Proof of Concept* (Washington, D.C.: Atlantic Council, 18 April 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 Planning Council, *Föderale IT-Architekturrichtlinie. Version 1.9.0* (2025), 21—26, http://www.it-planungsrat.de/beschluss/beschluss-2025-17.

75 Herpig, *Fostering Open Source Software Security* (see note 70), 20—21.

76 TODO Group, "Open Source Program Office (OSPO) Definition and Guide", *GitHub*, 9 July 2024, https://github.com/todogroup/ospodefinition.org; OpenForum Europe and OSPO Alliance, *The OSPO. A New Tool for Digital Government* (Brussels, June 2022), 9ff., https://openforumeurope.org/wp-

many armed forces, selected personnel already perform individual OSPO functions; but so far, no military has established its own OSPO.

If the Bundeswehr were to set up an OSPO, it should ensure that the new office has a lean structure and serves as a central point of contact for OSS-related questions of relevant staff including procurement and IT, while the various Bundeswehr entities remain responsible for operational tasks such as the monitoring of critical OSS components. Further, it should be in close contact with the OSPO currently being established at the Federal Office for Information Security (BSI)[77] and the Centre for Digital Sovereignty[78] (ZenDiS, which was established by the Federal Ministry of the Interior to increase OSS use within the public administration).[79] This would allow the Bundeswehr to benefit from the expertise of those two agencies. In addition, "OSPO ambassadors"[80] from the various departments could identify needs for OSS solutions and anchor the work of the OSPO in the Bundeswehr as a whole.

Internal Processes

In addition to developing the structures and strategies discussed above, organisations that want to protect themselves against software supply chain risk must develop internal processes that put such ideas into practice.[81] For the armed forces, two processes have priority: collecting different types of information about software products in use and monitoring their maintenance status. So far, the processes established by the Bundeswehr remain inadequate.

However, it is important to note that the processes described below should not be rigidly rolled out throughout the entire Bundeswehr; after all, like most militaries, the Bundeswehr is organised in a decentralised fashion and the needs of its various units differ. Rather, the CISOBw, together with the ZCSBw, should develop model processes, provide guidance and templates, monitor the implementation of the processes, and regularly evaluate their effectiveness. On this basis, the various organisational entities could proceed to establish their own processes tailored to their specific needs.

In addition to the processes described below, which are geared towards managing software supply chain risk, the Bundeswehr needs robust cybersecurity processes, such as incident response and the monitoring of software vulnerabilities.[82] Both of these tasks fall within the remit of the ZCSBw; thus, it is essential to ensure adequate resources for this body in order to guarantee the cybersecurity of the entire Bundeswehr, including with regard to managing software supply chain risk.

Gathering Information

Many software supply chain attacks are possible because of vulnerabilities in software products. While it is hard to prevent the exploitation of vulnerabilities that remain unknown to the software vendor (so-called zero days), the Bundeswehr can, in many cases, prevent attacks that exploit known vulnerabilities — if the right people have the right information. Above all, this includes:

1. Drawing up an inventory of all software products in use;
2. Gathering information about vulnerabilities in software components;
3. Collecting software composition information, and

content/uploads/2022/06/The-OSPO-A-New-Tool-for-Digital-Government-2.pdf; Herpig, *Fostering Open Source Software Security* (see note 70).

77 BSI, "Vortrag des BSI beim Fachkongress Public-IT-Security im Juni 2025", *FragDenStaat*, (online), 3 June 2025, https://fragdenstaat.de/anfrage/vortrag-des-bsi-beim-fachkongress-public-it-security-im-juni-2025/.

78 See the ZenDiS website, https://www.zendis.de/.

79 This should go beyond the existing cooperation between BWI GmbH and ZenDiS; see "BWI und ZenDiS schließen Rahmenvertrag über souveräne Kommunikations- und Kollaborationslösungen", *ZenDiS* (Bochum, 4 April 2025), https://www.zendis.de/newsroom/presse/bwi-und-zendis-schliessen-rahmenvertrag-ueber-souveraene-kommunikations-und-kollaborationsloesungen.

80 Shilla Saebi and Aison Yu, "Growing Sustainable Contributions through Ambassador Networks", in *FOSDEM '20* (Brussels, February 2020), https://archive.fosdem.org/2020/schedule/event/ambassadornetworks/; Michael Picht, "How SAP Manages Open Source Software with an Open Source Program Office", *SAP* (online), 28 October 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* (see note 66).

82 Id., *IT-Grundschutz. A Systematic Basis for Information Security* (Bonn, 22 October 2024), https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

4. Gathering vulnerability exploitability information.[83]

The Bundeswehr IT staff need to close a vulnerability only if they determine the use of a product that is based on a component in which a specific vulnerability exists and can be exploited.

So far, the Bundeswehr has developed a reliable process for just one of the above four tasks, namely, obtaining information about vulnerabilities and sharing it with others. This task is undertaken in sharing communities within the framework of NATO and in collaboration with national cybersecurity authorities such as the BSI, and under bilateral or multilateral arrangements with military or civilian entities from other countries.

As regards the three other forms of information gathering, the Bundeswehr has yet to establish and automate the necessary processes. In the case of the software inventory, the Bundeswehr, like many other armed forces, does not have a full overview of all the software products it uses — not least because its software procurement is (to a certain extent) decentralised. A central register should not be used for such an inventory, given the potential for compromises; rather, each organisational entity should maintain its own inventory in a standardised format that allows data to be easily retrieved and compared.

Similarly, most armed forces — including the Bundeswehr — lack information about the composition of the software products they are using. This is because software is usually supplied without comprehensive information about its components.[84] Suppliers and OSS projects can share such information in the form of a so-called *software bill of materials* (SBOM), that is, "a machine-processable file containing supply chain relationships and details of the components used in a software product".[85] Military organisations can obtain SBOM data either from their suppliers or from OSS projects or they can use paid third-party tools to create SBOMs.[86] Since the data quality of many current SBOMs is poor,[87] the CISOBw should define minimum SBOM requirements for software suppliers. These requirements should be based on a framework document[88] issued by the BSI. Furthermore, the CISOBw should ensure that all Bundeswehr entities have processes in place for evaluating software composition information and that they share and consolidate that information.

Finally, as regards vulnerability exploitability information, the Bundeswehr IT staff — much like those of other militaries — currently compile such information manually, as most software suppliers do not provide this data in a machine-readable format. The armed forces should therefore make suppliers provide such information (as described in the following section). As long as the Bundeswehr does not receive this information from suppliers, the CISOBw should offer tools and develop model processes to facilitate data collection and processing. And when suppliers start providing these data, the CISOBw should ensure that a model process and guidance is available so that all Bundeswehr entities can establish appropriate processes of their own.

Monitoring the Software Maintenance Status

Organisations that want to protect themselves against software supply chain risk should also monitor whether the software products they are using continue to be actively maintained. Currently, suppliers do not provide this information in a standardised, machine-

83 Even if a software product contains a component with a known vulnerability, there is no security risk if the vulnerability cannot be exploited — for example, because there are protective measures elsewhere in the code or because the way the component is integrated does not allow exploitation; see National Telecommunications and Information Administration (NTIA), *Vulnerability-Exploitability eXchange (VEX) – An Overview* (Washington, D.C., 27 September 2021), 1, https://www.ntia.gov/sites/default/files/publications/vex_one-page_summary_0.pdf.

84 Boming Xia et al., "An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead", *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)* (New York: IEEE, 2023), 2630–42, doi: 10.1109/ICSE48619.2023.00219.

85 BSI, *Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products.* Part 2: *Software Bill of Materials (SBOM)* (Bonn, 20 August 2025), 7, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2_v2_1_0.pdf?__blob=publicationFile&v=5.

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 et al., "A Viewpoint on Knowing Software: Bill of Materials Quality When You See It", *IEEE Security & Privacy* 21, no. 6 (2023): 50–54.

88 BSI, *Technical Guideline TR-03183* (see note 85).

readable format.[89] Thus, when time permits, Bundeswehr IT staff have to manually check supplier websites for end-of-maintenance notices.

To enable the Bundeswehr to monitor the maintenance status of the software products they are using, the CISOBw should first define what "active maintenance" means.[90] The definition should take into account that software products with different security requirements need different levels of software maintenance (accordingly, the definition should be tiered to account for those various levels). In addition, the CISOBw should provide both guidance to facilitate manual searches and a template for processing the data. Furthermore, as outlined in the following section, the Bundeswehr should make suppliers provide those data so that the process can be automated.

The Bundeswehr should urgently seek to further build expertise among its procurement and IT staff in managing software supply chain risk.

But, above all, the CISOBw must determine what happens when a product is no longer being actively maintained. In this case, there are two possibilities: IT staff can identify and introduce a viable alternative product or they can take the maintenance of the orphaned product into their own hands — by using their own resources or by contracting third parties. For the armed forces, it is often difficult to switch to another product because complex military processes are geared towards specific products and personnel are trained accordingly. The guidelines for managing software supply chain risk should therefore provide guidance on the circumstances under which it is advisable for the Bundeswehr to replace an unmaintained product.

Fostering Expertise

In general, Bundeswehr procurement and IT staff are not trained to manage software supply chain risk. For this reason, the Bundeswehr should urgently seek to further build such expertise.

Given the IT workforce shortage in Germany[91] and the difficulties the public sector faces in recruiting and retaining IT talent, the Bundeswehr should teach software supply chain risk management at its academies for civilian and military education and training. The aim should be that personnel are proficient in three "languages"[92]: military, IT, and procurement terminology. In addition, the armed forces should ensure that the entities mentioned in this research paper have adequate resources to hire skilled personnel.

Red Teaming Activities

Furthermore, companies and government agencies alike have had good experience with so-called red teaming activities. These involve in-house IT specialists taking on the role of attackers to find vulnerabilities in their own systems or the software products they are using. Typically, the focus is on critical OSS products and components and proprietary software. If the supplier of proprietary software grants a red team access to the source code, the team can check the products for known vulnerabilities, assess the maturity of integrated OSS components, and determine whether secure software development practices[93] have been followed. But even without access to the source code, red teaming activities can reveal weaknesses in software configurations, among other things.

Some armed forces — in the case of the Bundeswehr, the ZCSBw — have already set up teams that scrutinise the code of selected software products.[94]

89 Omar Santos et al., *OpenEoX. A Standardized Framework for Managing End of Life and Other Product Lifecycle Information*, 24 April 2025, https://docs.oasis-open.org/openeox/standardization-framework/openeox-standardization-framework-technical-report.pdf.

90 Such a definition can be based on maturity metrics such as Linux Foundation, "OpenSSF Scorecard", https://securityscorecards.dev/; OpenCode, "Badge Program" (Bochum, 9 May 2025), https://badges.opencode.de/de/introduction/. Compliance can be contractually agreed, see J. C. Herz, "Crumbling Bridges: The Failed Economics of Software Maintenance", *Cyber Security: A Peer-Reviewed Journal* 8, no. 2 (2024): 150—59 (157).

91 Ralf Wintergerst, *IT-Fachkräfte 2040: Wo steht die deutsche Wirtschaft?* (Berlin: Bitkom, 11 April 2024), https://www.bitkom.org/sites/main/files/2024-04/240411Bitkom-Charts-IT-Fachkraftemangel-2040final.pdf.

92 Probasco, "Building the Tech Coalition" (see note 39), 8.

93 These are discussed in the following section.

94 Emily Dreyfuss, "Pentagon Weapons Systems Are Easy Cyberattack Targets, New Report Finds", *Wired*, 10 October 2018, https://www.wired.com/story/us-weapons-systems-easy-cyberattack-targets; Bundeswehr, "CIR 2.0. Von der Idee zur Dimension", *cpm Forum für Rüstung, Streitkräfte und Sicherheit* (September 2022), 83, http://www.bundeswehr.de/resource/

The ZCSBw should expand these activities. First, its staff should scrutinise critical OSS products and components.[95] Second, they should take measures that provide insights even without access to the source code. To be able to perform these tasks, the team at the ZCSBw should be expanded. In addition, the guidelines for software supply chain risk management should make clear on which software products these efforts should focus.

Barring Untrustworthy Suppliers from Procurement

Public procurement processes are generally based on functional requirements for the product and security requirements for the product and/or the supplier. However, there are cases in which a software product that meets all requirements should nonetheless be excluded from procurement; one such case is when the supplier is considered untrustworthy — for example, because of its foreign ownership or the control and influence risk posed by adversarial governments.[96] Among other things, the latter can make suppliers insert harmful hidden functions into a product, either from the outset or at a later date (including through updates).[97]

In some cases a software product that meets all requirements should nonetheless be excluded from procurement.

Many military procurement processes, such as that of the Bundeswehr, do not provide for barring products that formally meet all requirements. Moreover, the information that serves as the basis for classifying a supplier as untrustworthy is often not made public. Thus, procurement staff are frequently faced with having to adapt the functional requirements in such a way that they cannot be met by untrustworthy suppliers — an extremely inefficient strategy that takes place in a legal grey area.

Legislators should therefore amend public procurement law and the BMVg should adapt procurement regulations to provide for the exclusion of untrustworthy suppliers from public procurement.

blob/5519316/29945909e7ed8cc36f2c9ff4ecd53186/download-sonderheft-cir-2-0-data.pdf.

95 John S. Meyers et al., "The US Military Should Red-Team Open Source Code", *Defense One*, 10 August 2022, http://www.defenseone.com/ideas/2022/08/military-should-red-team-open-source-code/375635/.

96 As in the case of 5G telecommunications technology, the decision on which vendors are considered (un)trustworthy is ultimately a political one; see 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 May 2020), https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

97 Kim Zetter, "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors", *Wired*, 19 December 2015, https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/.

How Policymakers and the Armed Forces Can Make Software Suppliers Take Action

However, the armed forces cannot protect themselves against software supply chain risk on their own. They depend on software suppliers[98] taking action, too — by managing the risks posed by their products and supporting customers in their risk management. Political and military decision-makers have several policy instruments at their disposal to make suppliers take action (see Figure 6, p. 30).

Requirements for Software Suppliers

Before decision-makers select any policy instruments, they must identify what actions they expect from suppliers. The Bundeswehr has developed a "software engineering framework"[99] for this purpose; but since that document is classified, it is not publicly known what it contains. Based on expert assessments, this research paper argues that suppliers who meet the following six requirements can significantly reduce the supply chain risk posed by their software products:

1. Adhere to secure software development practices[100]: specifically, software suppliers should fix exploitable known vulnerabilities in the components of their products,[101] (re)write software in memory-safe programming languages,[102] ensure a secure build process (which converts human-readable source code into machine-readable binary code) for both the components they use[103] and their own products,[104] and sign their code.

98 Here the term "supplier" refers not only to software vendors but to any entity in the software supply chain that adapts the software, such as resellers/distributors (if they customise the product), systems integrators and hardware manufacturers; see CISA, *Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)*, 3rd ed. (Washington, D.C., 3 September 2024), 26, https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdfi.

99 Rolf Hager, "Software Defined Defence. Schnellere Softwareentwicklung für die Bundeswehr mit der 'Platform42'", *Europäische Sicherheit & Technik*, 19 March 2024, https://esut.de/2024/03/fachbeitraege/47794/it-news-software-defined-defence-schnellere-softwareentwicklung-fuer-die-bundeswehr-mit-der-platform42/.

100 See, e.g., Murugiah Souppaya et al., *Secure Software Development Framework (SSDF) Version 1.1. Recommendations for Mitigating the Risk of Software Vulnerabilities* (Gaithersburg: National Institute of Standards and Technology [NIST], February 2022); "Fundamental Practices for Secure Software Development. Essential Elements of a Secure Development Lifecycle Program", *SAFECode*, March 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, 12 September 2025), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-1.pdf?__blob=publicationFile&v=10.

101 "Reduce Supply Chain Risk. Continuous SBOM Analysis Platform", *Dependency Track*, https://dependencytrack.org.

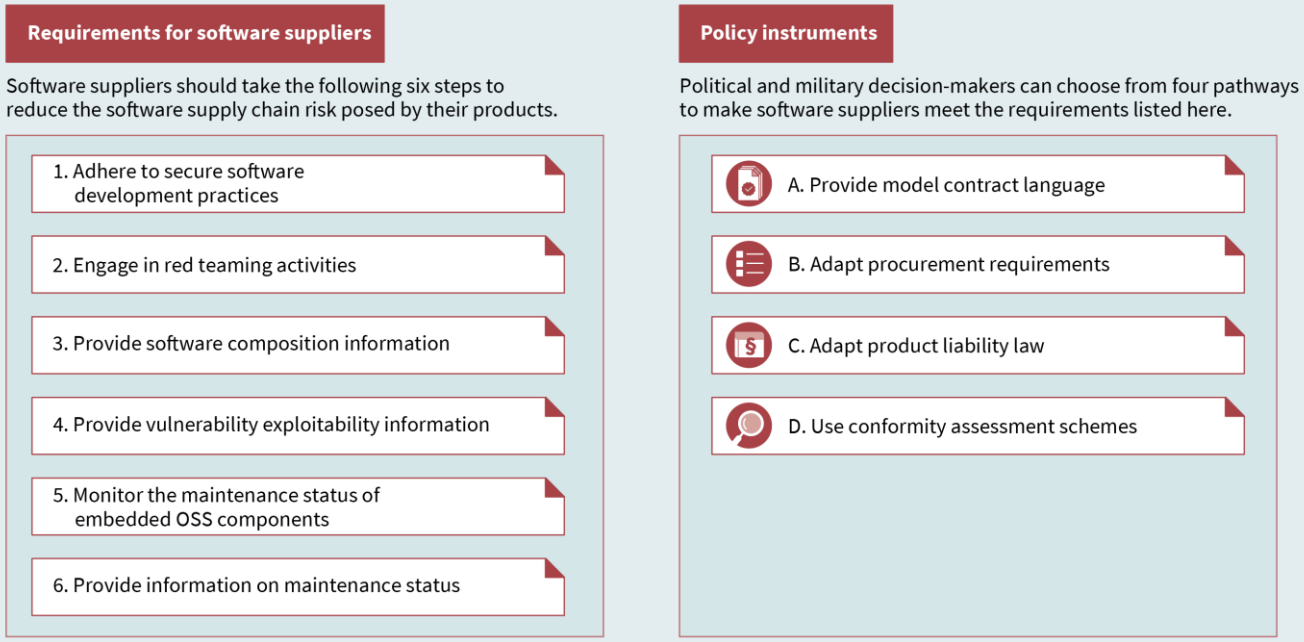
102 Alex Gaynor, "Introduction to Memory Unsafety for VPs of Engineering", *alexgaynor.net*, 12 August 2019, https://alexgaynor.net/2019/aug/12/introduction-to-memory-unsafety-for-vps-of-engineering/#what-is-memory-unsafety.

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

104 "Definitions", *Reproducible Builds*, https://reproducible-builds.org/docs/definition/; Chris Lamb and Stefano Zacchiroli, "Reproducible Builds: Increasing the Integrity of Software Supply Chains", *IEEE Software* 39, no. 2 (2022), 62—70;

Figure 6

How policymakers and the armed forces can make software suppliers take action



Source: Own visualisation

2. Engage in the red teaming activities recommended above: it should not just be the Bundeswehr that conducts red teaming activities; suppliers should also carry out those activities (either themselves or through third parties) within their own systems and ask their suppliers and service providers to do the same.
3. Provide the Bundeswehr (and, ideally, all their customers) with software composition information for their products — for example, in the form of SBOMs: these data should comply with one of the established standards[105] and, eventually, include all levels of dependency,[106] as an exploitable vulnerability can be buried deep within the supply chain.
4. Provide vulnerability exploitability information for their products in a standardised, machine-readable data format[107] and via a defined distribution mechanism.
5. Monitor the maintenance status of the embedded OSS components throughout the entire life cycle of their products: at the development stage, suppliers should integrate only those components that meet the Bundeswehr definition of "active maintenance". If, at some point, a component that has already been integrated into a product no longer meets those requirements, suppliers should replace the component and maintain it themselves, or pay a third party to do so. Suppliers whose products fall under the EU Cyber Resilience Act (CRA) will be

openCode, ZenDiS, and BSI: *Sichere Softwarelieferketten: openCode als Baustein einer souveränen digitalen Infrastruktur* (Bochum, March 2025), https://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), https://www.ntia.gov/sites/default/files/publications/sbom_formats_survey-version-2021_0.pdf.

106 CISA, *Framing Software Component Transparency* (see note 98), 10f. Such a requirement would go beyond the provision of the CRA that stipulates only the first level of components is to be included; see European Parliament and Council, *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*, 23 October 2024, Annex I, Part I(1), https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:32024R2847.

107 *Common Security Advisory Framework (CSAF)*, https://www.csaf.io/; NTIA, *Vulnerability-Exploitability eXchange* (see note 83).

required to do this from 2027 onwards.[108] However, the regulation does not apply to products developed exclusively for military purposes or for processing classified information.[109]

6. Provide information on the maintenance status of their products in a standardised, machine-readable format.[110]

Many of the above measures are not yet widespread among software suppliers. For this reason, generous implementation timelines will be needed for the corresponding requirements. In addition, software suppliers should be required to implement general cybersecurity measures that are not specifically aimed at software supply chain risk but can nonetheless reduce or mitigate it. Such measures include network segmentation and a so-called zero trust architecture,[111] vulnerability management,[112] regular installation of software updates[113] and the detection and handling of cybersecurity incidents.[114]

Should policymakers or the military leadership use these requirements as the basis for incentive structures or regulations, they should take account of the fact that SMEs and smaller OSS projects generally have fewer resources available with which to implement exacting requirements. Thus, such requirements can have unintended consequences: for example, SMEs and smaller OSS projects might abandon their software products or suppliers might isolate the OSS components they integrate into their products.[115] Decision-makers should therefore examine whether SMEs and OSS projects could be subject to less exacting requirements and how they might be supported during the fulfilment of those obligations.

Model Contract Language

Once policymakers and the Bundeswehr have defined the requirements for software suppliers, they must decide how to enforce them. Procurement contracts are a low-threshold option that does not impose regulation. Indeed, as an example from the private sector shows, software suppliers can be contractually obliged to regularly check the maintenance status of the OSS components they have integrated into their products and to take remedial action if necessary.[116] However, the Bundeswehr, like the armed forces of other countries, makes little use of this option so far.

The current Bundeswehr procurement process does not take software supply chain risk into account.

To remedy this, Bundeswehr procurement personnel should be provided with model contract language — for example, in the form of service level agreements.[117]

Procurement Requirements

The current Bundeswehr procurement process does not take software supply chain risk into account.[118] By contrast, the US already has procurement rules to ensure that software suppliers better protect their products from software supply chain risk.[119] For

108 European Parliament and Council, *Cyber Resilience Act* (see note 106), Art. 13(5).

109 Id., *Cyber Resilience Act* (see note 106), Art. 2(7).

110 Santos et al., *OpenEoX* (see note 89).

111 Scott Rose et al., *Zero Trust Architecture* (Gaithersburg: NIST, August 2020), doi: 10.6028/NIST.SP.800-207.

112 Allen D. Householder et al., *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 and 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, 26 February 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

115 John S. Meyers and Paul Gibert, "Questioning the Conventional Wisdom on Liability and Open Source Software", *Lawfare*, April 2024, http://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 October 2022, https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/.

116 Herz, *Crumbling Bridges* (see note 90), 157.

117 For an example from the civilian sector, see Der Beauftragte der Bundesregierung für Informationstechnik, *Aktuelle EVB-IT* (Berlin, 2 November 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, *Project-based Procurement and In-Service Use* (see note 43).

119 See, e.g., The White House, *Executive Order on Improving the Nation's Cybersecurity (EO 14028)* (Washington, D.C., 12 May 2021), https://bidenwhitehouse.archives.gov/briefing-room/

example, the US Army requires its suppliers to provide SBOM data.[120] The planned update of European procurement regulations offers a window of opportunity to incorporate the corresponding requirements.[121]

Specifically, the Bundeswehr should adapt military procurement rules in three ways:

1. Draw up horizontal minimum requirements for suppliers' management of software supply-chain risk: the CISOBw should undertake this task, together with all entities involved in software procurement. The Bundeswehr has already formulated minimum requirements for suppliers — for example, in the case of cybersecurity. Those requirements should be tiered to account for the different levels of criticality.
2. Remove barriers to OSS procurement, especially for products without commercial service contracts.[122]
3. Simplify the procedure for contracting (security-cleared) service providers for cybersecurity tasks that cannot be covered by Bundeswehr resources, such as red teaming activities: not least, this measure would take into account the current shortage of IT workers.

Product Liability Law

At present, the Bundeswehr — like many other armed forces and end users outside the EU — can hold software suppliers liable mainly for breach of contract, for intent, or for gross negligence. However, software supply chain incidents are often caused by supplier practices or omissions that lie outside the categories mentioned above. Product liability regulation for software products used by the armed forces would allow the Bundeswehr to hold suppliers liable for defects in the software product and/or development process that cause harm: for example, non-compliant companies would be required to pay damages.[123]

German product liability law does not cover software products;[124] and the 2024 EU Product Liability Directive allows only natural persons to claim damages.[125] From 2027 onwards, the Bundeswehr will be able to hold suppliers liable on the basis of the EU CRA; however, that regulation does not apply to many of the software products that it uses.[126] To date, no jurisdiction other than the EU has developed a product liability regime for software that allows claims by legal entities such as the armed forces.

Legislators should consider introducing a product liability regime that is applicable to software used by the armed forces.

For this reason, legislators should consider introducing a product liability regime that is applicable to software used by the armed forces or to software in general. The EU Product Liability Directive, which member states must transpose into domestic law by 2026, will offer a window of opportunity: since legislators will have to amend domestic product liability law in any case, they could go beyond the requirements of the directive by making legal entities such as the Bundeswehr eligible for claims. The requirements for software suppliers listed above could serve as a reference for determining the conditions under which suppliers are to be held liable.[127] At the same

presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

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

121 Francesco Nicoli, *Mapping the Road Ahead for EU Public Procurement Reform* (Brussels: Bruegel, 31 March 2025), https://www. bruegel.org/first-glance/mapping-road-ahead-eu-public-procurement-reform.

122 For an overview of these barriers, see, e.g., Iain G. Mitchell, "Public Sector and Open Source", in *Open Source Law, Policy and Practice*, ed. Amanda Brock (Oxford: Oxford University Press, 2022), 429—68, https://academic.oup.com/book/44727.

123 Trey Herr et al., *Buying Down Risk: Cyber Liability* (Washington, D.C.: Atlantic Council, 15 January 2025), https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-liability/; Gergely Biczók et al., *Realigning Incentives to Build Better Software: A Holistic Approach to Vendor Accountability*, 10 April 2025, http://arxiv.org/pdf/2504.07766v1.

124 *Gesetz über die Haftung für fehlerhafte Produkte (ProdHaftG)*, 15 December 1989, https://www.gesetze-im-internet.de/prodhaftg/BJNR021980989.html.

125 European Parliament and Council, *Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC*, 23 October 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L2853.

126 Id., *Cyber Resilience Act* (see note 106), Art. 2(7).

127 Maia Hamin et al., "Three Questions on Software Liability", *Lawfare*, September 2023, https://www.lawfaremedia.

time, the CRA criteria should be taken into account to narrow the regulatory gap between the civilian and military sectors.

Conformity Assessments

If policymakers and armed forces want to ensure that software suppliers are complying with specific requirements, they can use a conformity assessment scheme. In such assessments, an attesting party — the supplier (self-assessment) or an independent, government-accredited entity (third-party assessment) — verifies compliance with a requirements baseline.[128] Those requirements can be laid down, for example, in a technical standard, and the result of the assessment recorded in a certification report.

The US DoD has developed a conformity assessment scheme that focuses on how its suppliers handle sensitive, albeit unclassified information.[129] The CRA contains such a scheme for software products that ranges from self-assessments to third-party assessments, depending on the criticality of the product, and combines product- and process-based evaluations.[130] In Germany, conformity assessment schemes already exist for suppliers of software products that process classified information; while these take software supply chain risk into account, they cannot be evaluated here because they are not publicly available. In addition, the BSI has developed the "IT security label"[131] as a conformity assessment scheme for COTS IT products.

Conformity assessment schemes for software are costly for both suppliers and policymakers. Furthermore, the assessment must be regularly renewed owing to frequent software updates while product-based standards that take into account software supply chain risk — and thus could serve as the basis for assessment — are mostly lacking. For this reason, the political and military leadership should be cautious about establishing further conformity assessment schemes. Instead, Bundeswehr procurement staff should refer to the criteria of the IT security label and the CRA when selecting products.

If, nevertheless, the Bundeswehr were to decide to introduce a conformity assessment scheme, it should:

1. Opt for a process-based approach to ensure that the assessment remains valid for longer;
2. Develop a tiered scheme to facilitate participation by SMEs and the OSS ecosystem;
3. Seek harmonisation with CRA requirements and the schemes of other NATO allies to create a level playing field across the Alliance; and
4. Require third-party assessments — at least at the highest security level — to ensure robustness.

org/article/three-questions-on-software-liability; Chinmayi Sharma and John S. Meyers, "Bugs in the Software Liability Debate", *Just Security*, 18 July 2023, http://www.justsecurity.org/87294/bugs-in-the-software-liability-debate/.

128 Paulus and Rupp, *Government's Role in Increasing Software Supply Chain Security* (see note 24), 32f.

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

130 European Parliament and Council, *Cyber Resilience Act* (see note 106).

131 BSI, *Transparent Security through the IT Security Label* (Bonn, 9 February 2023), https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html.

Priorities for German Political and Military Leaderships

The software supply chain incidents discussed in this research paper paint a grim picture. They highlight the potentially devastating impact of operational disruptions and attacks. And it is likely that they represent only a fraction of such incidents to date, as most are probably not made public.

However, the Bundeswehr should not seek to minimise software supply chain risk at any cost. What is essential is to define an appropriate level of protection — depending on the software product. The focus should be on those products that are used on the battlefield, play a mission-critical role for supporting functions, or, if compromised, would allow adversarial intelligence services access to sensitive information.

Keeping, above all, these products in mind, the BMVg and the Bundeswehr should take measures to reduce software supply chain risk to an acceptable level. Many of the measures identified here are complex and would require significant resources. Given the narrow bandwidth of leadership, the shortage of IT workers, and finite financial resources, German policymakers and the Bundeswehr should focus on the three steps that need to be taken most urgently.

First, the Bundeswehr should establish structures through which software supply chain risk can be dealt with in the first place. Specifically, the CISOBw's portfolio should be expanded to include managing these risks so that a central point of accountability can be established. Furthermore, the Bundeswehr should appoint focal points at the BAAINBw, BAIUDBw, and BWI to support the procurement staff of these agencies in the implementation of further measures. In addition, the BMVg and the relevant Bundeswehr entities should jointly formulate guidelines for software supply chain risk management and, where possible, make those guidelines binding by incorporating them into service regulations. Finally, the Bundeswehr should foster the expertise of its procurement and IT staff in managing software supply chain risk — for example, through the Bundeswehr academies.

Second, policymakers and the Bundeswehr should ensure that software suppliers provide the military with information that is essential for effective risk management. This includes information on software composition, vulnerabilities exploitability and the maintenance status of their products. The easiest way to achieve this is through model contract language, which the CISOBw should make available to all procurement personnel. However, such model language does not always appear in the final contract; thus, a more reliable approach would be to establish horizontal minimum procurement requirements for software supply chain risk management.

Third, the Bundeswehr should establish its own internal processes in order to monitor software supply chain risk based on the information they receive from software suppliers, and to be able to respond to threats as necessary. This includes maintaining inventories of all software products being used, monitoring their maintenance status, and constantly checking whether they contain known exploitable vulnerabilities.

If the Bundeswehr were to take these three steps, it would be able to identify risks in the software supply chain and respond to threats as necessary. If the German government and the Bundeswehr want to further reduce such risks, there are other steps they should take as well. For example, the Bundeswehr and its software suppliers (and their suppliers) should engage in red teaming activities to identify vulnerabilities in products and configurations. In addition, policymakers and the Bundeswehr should make suppliers adhere to secure software development practices. This includes closing exploitable known vulnerabilities in product components, switching to memory-safe programming languages, securing the build process, and signing their code. Furthermore, suppliers should not only check the maintenance status of the OSS components that are part of their products at the time of development; they should also monitor that status

throughout the product's lifecycle and take action if a component is no longer actively maintained. And to ensure that suppliers take these measures, the Bundeswehr can turn to procurement requirements, which are much easier to implement than the other potential policy instrument — namely, product liability law.

The BMVg and the Bundeswehr need to act swiftly to take advantage of the windows of opportunity that are currently wide open. The ongoing reorganisation of CIR following its elevation to an independent service branch of the armed forces lends itself to the creation of new structures. The recent change in public debt regulation[132] gives legislators more leeway in authorising investments that will significantly improve the security of the Bundeswehr. And opportunities are also afforded by the EU procurement regulations currently being revised, while software suppliers are reviewing the software supply chain security of their products in preparation for the CRA provisions entering into force in 2027.

To reduce the costs of the measures proposed here, the federal government and the Bundeswehr should join forces with their counterparts in like-minded countries. The Bundeswehr is more likely to be able to persuade software suppliers to meet certain requirements if these are harmonised internationally. International dialogue on this subject could take place within NATO, the Organisation for Economic Co-operation and Development (OECD), and the recently established G7 Cybersecurity Working Group. Moreover, an international multi-stakeholder forum on managing (military) software supply chain risk could further raise awareness of the issue and promote operational cooperation.

Dealing with software supply chain risk demands that policymakers and the armed forces perform a difficult balancing act. On the one hand, they have to invest significant resources to prevent, or mitigate the impact of, potentially devastating attacks or disruptions to military operations. On the other hand, they must pave the way for software-defined defence through the simplified and accelerated procurement, deployment, and updating of software and through the promotion of a domestic defence tech ecosystem that is both dynamic and innovative.[133] Although this research paper focuses on managing software supply chain risk, putting the Bundeswehr on the right track for software-defined defence is just as important.

Abbreviations

BAAINBw	Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support
BAIUDBw	Federal Office of Bundeswehr Infrastructure, Environmental Protection and Services
BMVg	Federal Ministry of Defence (Germany)
BSI	Federal Office for Information Security (Germany)
CIO	Chief Information Officer
CIR	Bundeswehr Cyber and Information Domain Service
CISA	Cybersecurity and Infrastructure Security Agency (US)
CISOBw	Chief Information Security Officer of the Bundeswehr
COTS	Commercial off-the-shelf
CRA	Cyber Resilience Act (EU)
DoD	Department of Defense (US)
GRU	Main Intelligence Directorate (Russia)
IC	Innovation and Cyber (directorate-general of the BMVg)
IT	Information technology
NIST	National Institute of Standards and Technology (US)
NTIA	National Telecommunications and Information Administration (US)
OECD	Organisation for Economic Co-operation and Development
OSPO	Open source programme office
OSS	Open source software
SaaS	Software as a service
SBOM	Software bill of materials
SDD	Software-defined defense
SMEs	Small and medium-sized enterprises
SVR	Foreign Intelligence Service (Russia)
WTD 81	Bundeswehr Technical Center for Information Technology and Electronics
ZCSBw	Bundeswehr Cyber Security Centre
ZDigBw	Bundeswehr Centre for Digitalisation and Cyber and Information Domain Service Capability Development
ZenDiS	Centre for Digital Sovereignty (Germany)

132 Deutscher Bundestag, "Mehrheit für Reform der Schuldenbremse: 512 Abgeordnete stimmen mit Ja", 18 March 2025, https://www.bundestag.de/dokumente/textarchiv/2025/kw12-de-sondersitzung-1056916.

133 Probasco, *Building the Tech Coalition* (see note 39).