SWP Comment
NO. 21 JUNE 2026

Cybersecurity Needs Secure Software

How Policymakers Can Hold Software Vendors Accountable – and Why They Should

Alexandra Paulus

Cybersecurity incidents cause harm – for example, when adversarial states paralyse critical infrastructure or steal sensitive data. Many such incidents are only possible because many software products have known vulnerabilities. Software vendors could fix these, but they have little incentive to invest in the security of their products. To date, cybersecurity policy and protective measures have primarily addressed the symptoms of insecure software, rather than the root cause, namely software insecurity itself. This calls for regulation, specifically in the areas of product safety law, product liability regulations, and cybersecurity requirements for providers of software services. The European Union (EU) has already adopted initial rules, but regulatory gaps remain, and it is unclear whether member states will strictly enforce them. The German government should therefore now advocate for comprehensive European product liability regulations for software, and the Federal Office for Information Security (BSI) should impose fines on companies that violate existing rules.

Cybersecurity incidents cause significant damage. In 2025, cyberattacks cost German companies more than 200 billion euros, equivalent to 4.5 per cent of gross domestic product. Particularly serious are attacks on critical infrastructure: In December 2025, a Russian cyber operation came close to paralysing parts of Poland's energy infrastructure. In the spring of 2026, it became known that Iranian actors were preparing attacks on the water sector and other critical infrastructure in the United States, after the People's Republic of China had carried out similar operations against US targets in 2024. Furthermore, Chinese and Russian actors have used cyber operations to spy on and sabotage Western armed forces and their suppliers and service providers, or to restrict the availability of services. Russian intelligence services also regularly use cyber operations to obtain sensitive information from civilian targets. Last but not least, cybercriminals pose a threat to the German economy, particularly small and medium-sized enterprises (SMEs), as well as to public administration. In short: in digitalised societies, cybersecurity is a necessary prerequisite for "security, freedom, and prosperity", the current German government's guiding principle.

Many cybersecurity incidents are only possible in the first place because software products contain known vulnerabilities. A key reason for this is that software vendors

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

currently have little incentive to invest the time and money needed to make their products secure. This is a market failure.

Cybersecurity policy has so far mainly tackled the symptoms

The market for commercial software products differs from other markets in one key respect: Software vendors generally do not face significant consequences if their products cause harm. Instead, the majority of regulations introduced to date place responsibilities on operators, such as those of critical infrastructure, and other key entities. Similarly, many common cybersecurity measures target users, for example in the form of warnings, awareness campaigns, or training.

Indeed, users and operators can ensure that their software is up to date and securely configured; they can also set up their IT systems in ways that limit risk. But such measures can do little to tackle the problem of insecure software. Therefore, German and European cybersecurity policy should focus on compelling commercial software vendors to develop secure products.

Vendors lack incentives to develop secure software

For years, the majority of discovered software vulnerabilities go back to vendors making the same long-known and often easily avoidable errors. At the same time, software developers know how to design secure development processes and products, given the wealth of practical guidance available on the subject. For example, vendors should monitor vulnerabilities in open-source components that they integrate into their products and patch them as needed. They can even use AI applications to simplify this process. Furthermore, they should integrate only actively maintained open-source components. Likewise, they should use memory-safe programming languages to avoid a common type of vulnerability.

Case study: How insecure software causes cybersecurity problems

One incident illustrates the extent to which software vendors bear responsibility for cybersecurity incidents. Notably, no malicious actor was involved, but the incident still caused tremendous harm. In July 2024, the US software company CrowdStrike released a faulty update for its cybersecurity application "Falcon". CrowdStrike automatically installed the update on the devices of customers that used the Windows operating system. As CrowdStrike has a large market share, the impact was enormous: The faulty update crashed 8.5 million devices worldwide, temporarily rendered them inoperable, and forced users to reset them. The resulting damage is estimated at more than 5.4 billion US dollars.

The software vendor caused the incident through a chain of errors. First and foremost, there was a coding error. Individual developers can make mistakes, and internal testing may miss these errors. Standard verification mechanisms would have detected the error and prevented a system crash, but the application lacked such mechanisms. Furthermore, CrowdStrike released the update to all its Windows customers worldwide simultaneously, even though best practice would have required a staged rollout to individual customer segments and checks for any resulting problems. In short, the vendor could have prevented the enormous damage to its customers by relatively simple means.

Why do commercial software vendors not simply implement these best practices? There are four interrelated reasons. First, software vendors often want to bring their products to market as quickly as possible. After all, they can always patch vulnerabilities later via a security update. Second, users find it difficult to assess the security of software products, as there is no widely recognised IT security label for software. Furthermore, when users — including corporate customers — make buying decisions, they usually focus on functionality and price while disregarding security. Third, cybersecurity incidents have little

long-term impact on a company's reputation or share price. And fourth, vendors face no legal or financial consequences for making insecure products. Policymakers should address this last point.

How policymakers can create the right incentives

Currently, users generally bear the costs when insecure software causes cybersecurity incidents. But policymakers have different regulatory options at their disposal to ensure that vendors are held accountable instead, as demonstrated by the incorporation of the polluter pays principle into environmental law. Users may also bear some responsibility for cybersecurity incidents — for instance, if they fail to install security updates — and regulatory frameworks should reflect this. Even so, there are several regulatory points of leverage.

To date, injured parties of faulty software can generally bring claims against vendors under warranty law — but only if they have a contract with them. As a result, the vendor may have to refund the purchase price, but this offers at best limited consolation if the cybersecurity incident in question caused significant harm. To pursue further claims, users usually need to prove that the software did not meet the necessary security requirements and that this specific deficiency caused the damage. In practice, this proof is often difficult to provide, as security incidents are frequently attributable to multiple factors. In sum, without further regulation, there are significant hurdles to holding vendors accountable for insecure software.

However, policymakers have three regulatory options at their disposal. First, the legislature can formulate product safety law requirements that vendors must meet in order to be permitted to place their products on the market. Market surveillance authorities monitor compliance and impose fines for violations. Such regulation is intended to prevent vendors from offering unsafe products in the first place.

The second instrument is product liability law. If a party suffers harm from a defective product, such regulation allows them to bring claims against the vendor of the product. Product liability provisions can therefore not only provide the legal basis for compensating individual damages, but also — given that vendors face significant financial losses — create incentives for vendors to invest more in the security of their products. Experience from the automotive and pharmaceutical sectors shows that the introduction of product liability regulation tends to correlate with safer products. Product liability law does not require a contractual relationship between the vendor and the injured party, and it also allows injured parties to claim consequential damages.

Software vulnerabilities can be exploited not only when the software is purchased and installed on users' own systems ("on premises"). The same applies when it is procured as a service, usually as a cloud solution ("Software-as-a-Service", or SaaS). Product liability and product safety law often does not apply to such usage models. In addition, legislators can therefore establish cybersecurity requirements for these providers.

The Federal Government should not pursue these three regulatory avenues on its own. Rather, it should focus its efforts primarily at the EU level to drive forward European regulations. Once European legislation is enacted, responsibility returns to the Federal Government: EU directives must then be transposed into national law, and EU regulations often need to be accompanied by implementing legislation.

The special role of open-source software

Open-source software (OSS) forms the backbone of virtually all software products. AI applications such as the large language model Mythos Preview have successfully identified vulnerabilities in numerous OSS components. Although this analysis focuses

on commercial software vendors, OSS should be taken into account as well.

Regulating non-commercial OSS developers could have unintended consequences. For instance, hobbyist developers might cease their activities for fear of liability or increased security-related burdens. One possible solution would make commercial software vendors that use OSS components responsible for fixing vulnerabilities in them. Similarly, governments could compile an inventory of critical OSS components and then (have a third party) secure them.

Trade-offs in placing obligations on vendors

Regulating software vendors has both advantages and disadvantages. First, the dynamic and relatively low-cost software sector has become the foundation of modern digitalised societies and economies. Not all, but some, of the measures that help vendors make their software products more secure require time and resources, and sanctions or liability risks can create additional costs. Vendors would likely pass on these increased costs to their customers, leading to rising software prices. Ultimately, this would mean that a software product's price would start to reflect its security: The less secure the software, the more a vendor would have to spend to secure it or reserve for liability risks, and the more expensive the product would become. On the one hand, rising software prices could trigger domino effects such as inflation. On the other hand, if the prices of software products reflect their security, this would make more secure products more competitive. As a result, buyers would select products also based on security, which should raise the level of cybersecurity in the long term.

Second, additional obligations for commercial software vendors could also have unintended consequences. A key factor here is that the market for software products is heavily dominated by US companies — particularly in operating systems, office applications, cybersecurity products, and AI applications. Accordingly, US vendors have a decisive influence on the level of cybersecurity in Germany. If Germany or the EU passed strong regulation in this field, international companies might decide to leave the market. As a result, these (presumably less secure) products would no longer be available on the German or European market. This could, on the one hand, have the positive side effect of improving the market position of those vendors that prioritise cybersecurity. On the other hand, Europe is heavily dependent on US companies in the technology sector as a whole, and specifically in the field of cybersecurity, while for some products there are no European alternatives. Despite all efforts to reduce these dependencies, a withdrawal of major US software vendors from the EU market could lead to operational disruptions. Furthermore, stricter European rules for US companies would likely strain transatlantic relations.

Third, additional regulation would run counter to the current mood in Brussels, which favours reducing and streamlining existing market interventions, particularly in the digital sector.

Fourth, cybersecurity requirements place a disproportionately heavy burden on small and medium-sized software vendors — which play a particularly important role in Europe — because they have fewer resources available for implementation than large technology companies. Relief measures for SMEs can mitigate this effect.

Overall, policymakers considering obligations for software vendors need to balance cybersecurity against efficiency and innovation. The question is whether the costs of cybersecurity incidents justify such measures. Given the current threat landscape, the answer is likely yes.

Existing product safety regulation for software

In recent years, the EU has adopted legislation for each of the regulatory options

mentioned above — product liability, product safety law, and cybersecurity requirements for service providers. However, these regulations contain some gaps, and there are indications that the German government does not plan to enforce them strictly.

In Europe, there is currently no comprehensive product safety regulation in force for software. However, there are sector-specific requirements for medical devices, in vitro diagnostic medical devices, radio equipment, motor vehicles, and high-risk AI systems. In December 2027, the main provisions of the new EU Cyber Resilience Act (CRA) will come into force. This legislation sets out obligations for vendors of "products with digital elements", that is, software and products with embedded software such as Internet of Things (IoT) devices. The German government has already initiated the corresponding implementing legislation.

Once the CRA comes into force, all vendors wishing to offer their products on the European market will have to comply with the cybersecurity obligations set out therein. For example, during a product's lifecycle, vendors will have to remedy vulnerabilities that are being actively exploited. For many products, vendors themselves can attest to their compliance with the rules. For particularly "important" and "critical" products, such as firewalls, independent bodies must verify compliance before the product can be placed on the market. If companies violate the rules, they must pay fines and rectify the defects or withdraw their product from the market. Furthermore, customers can bring claims against vendors who violate the CRA rules.

However, the regulation does not apply to products "developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information", as the EU has no competence in this area (dual-use products, however, remain within the scope of the regulation). In this field, member states can either conduct initiatives under the Common Security and Defence Policy or put forward national measures. The CRA calls on EU member states to ensure, for defence and security products, a level of protection that reaches or surpasses the CRA requirements. Indeed, products in this sector are often already subject to stringent security requirements, for example through procurement directives or mandatory certifications. Some of these requirements are classified and therefore cannot be assessed here; however, authorities can often deviate from them in justified cases. It is thus questionable whether these instruments are suitable for raising the security of these products overall.

Existing product liability regulation for software

Even if the CRA were to be rigorously enforced following its entry into force at the end of 2027, insecure software products will likely continue to cause harm. This is where product liability law may come into play. When considering such regulation, policymakers must carefully balance different interests: Liability regulation protects consumers, but it also restricts entrepreneurial freedoms, as it may influence liability costs, insurability, and recall and litigation risks.

The current German Act on Liability for Defective Products does not apply to software. However, a new version of the EU Product Liability Directive, on which the German law is based, was passed in 2024. Members of the Bundestag's Committee on Legal Affairs and Consumer Protection are currently deliberating a draft law that transposes the Directive into national law.

The previous 1985 Directive did not apply to software due to its intangibility, but the recast applies. As the Directive forms part of consumer protection law, it imposes three significant restrictions: Only natural persons may bring claims, only software used exclusively for private purposes qualifies, and claims arise only in cases of personal injury, property damage, or data damage. Conversely, this means that neither companies nor public author-

ities (such as municipalities) nor natural persons using software for professional purposes can bring claims. Purely financial losses also fall outside the scope of the Directive.

These restrictions apply because the directive governs strict liability: Vendors can be held liable without claimants having to prove intent or negligence on their part. The limitations are meant to ensure that the law does not give rise to uninsurable liability risks that could threaten software vendors' business models. Compared with natural persons, companies and public authorities are deemed to be less in need of protection because they can usually safeguard their interests by formulating their contracts accordingly.

However, these restrictions make little sense for the software market. Many products are used by private and professional users alike. Major software vendors often have such tremendous market power that they can dictate the terms of the contract (and, for example, exclude liability). This is particularly true when SMEs purchase products from large US vendors. Furthermore, cybersecurity incidents primarily cause financial damage. For instance, when cybercriminals encrypt company data and demand a ransom, they often disrupt operations and cause firms to miss out on profits. Against this backdrop, the limitations of EU product liability law are problematic.

Apart from the EU, no country has adopted product liability regulations that entitle users of software products to bring claims. In the United States, there had been discussions under the Biden administration about introducing product liability for software, but the Trump administration is seeking deregulation in the digital sector. In 2022, the European Commission had presented a proposal for its own product liability directive for AI applications. However, the Commission withdrew this proposal in October 2025 for various reasons.

Existing requirements for SaaS providers

Product liability law generally applies only to on-premises software solutions, not to Software-as-a-Service (SaaS), as the latter is not a product. The CRA applies to SaaS if the service forms part of the product as a "remote data processing solution". In addition, SaaS providers must comply with the requirements of the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Germany implemented the NIS 2 Directive late, in December 2025. The law stipulates that providers must offer secure services, including the management of software vulnerabilities.

The problem with NIS 2 is not so much that it contains regulatory gaps — it has a broad scope and applies to all providers offering services on the European market. The exemption for small businesses is hardly relevant in the SaaS sector. The problem is that there are doubts about its enforcement in Germany. The Federal Office for Information Security (BSI) is responsible for imposing fines in cases of non-compliance. However, the President of the organisation stated that her agency would generally not impose fines on companies that violate these requirements. But will companies adapt their cybersecurity practices if they have no sanctions to fear? If German authorities do not strictly enforce the rules even against German or European companies, how likely are they to ensure that US SaaS providers make their cloud solutions more secure? And what questions does this reluctance to enforce NIS 2 raise regarding the imposition of fines or product recalls for breaches of the CRA, for which the BSI will also be the enforcing agency?

Four tasks for German policymakers

If policymakers want to improve the dire cybersecurity situation, they must ensure that software becomes more secure. To

create the right incentives for software vendors, policymakers should do four things.

First, at the national level, the competent authorities should strictly enforce the existing rules. Both the NIS 2 Directive, which is already in force, and the CRA, which will enter into force in late 2027, can only be effective if vendors know that they face sanctions if they violate the rules. As a first step, the BSI should require all companies covered by NIS 2 to register in the relevant portal — so far, only around half have done so. The BSI should then impose fines for violations, including for US firms. This could encourage companies to prioritise compliance with the regulation. The US administration has recently shown greater openness to regulation aimed at limiting the cybersecurity risks of AI applications. Before taking action against US firms, European policymakers should lay the political groundwork through a dialogue on AI and software security risk. At the same time, European governments should prepare for defensive or retaliatory measures from Washington.

Second, European governments should comply with the CRA's call to develop strict cybersecurity requirements for vendors of software products in the security and defence sectors, and enforce these without exception. In the defence sector, governments can do this in various ways: The Ministry of Defence and the Bundeswehr could provide model contract language to the many Bundeswehr units responsible for procuring and operating software. In addition, policymakers could formulate corresponding horizontal minimum requirements for procurement and ideally apply them equally to the Bundeswehr and critical civilian sectors.

Third, on the EU level, the German government should advocate for a product liability law specifically for software. In theory, the Bundestag could also close the gaps described above in the draft bill for the national implementation of the EU Product Liability Directive. However, the European Court of Justice has set strict limits on member states' ability to engage in so-called gold-plating, that is, introducing national regulations that go beyond EU legislation. Furthermore, unilateral national initiatives to regulate the globalised software market are not particularly effective. A European law is therefore the better option. This law should allow companies, public authorities, and individuals who use software in a professional capacity to bring claims against vendors. Purely financial harms should also give rise to claims. It could also cover the security and defence sectors.

There is precedent for product liability laws for specific product groups. To justify the need for a liability law specifically for software, policymakers should refer to the particular characteristics of the software market. Given the serious cybersecurity threat landscape, support for such a proposal in Brussels is likely. Such a law could cap liability amounts to avoid creating uninsurable claims. To protect SMEs, these caps should be tiered according to company size. Such a proposal should account for its implications for transatlantic relations.

And fourth, European policymakers should first pass a comprehensive product liability law for software before considering a regime specifically for AI applications. Even though the latter pose particular challenges, they are, first and foremost, software. Presumably, comprehensive product liability law for software would also cover many conceivable cases of damage caused by AI applications. It therefore makes sense to establish comprehensive product liability for software first and then proceed to examine whether AI systems need further regulation. Such a legal framework would also be in line with the European Commission's recent efforts to streamline EU digital regulation.

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

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

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2026C21

(English version of SWP-Aktuell 27/2026)