SWP Comment
NO. 44 NOVEMBER 2025

Europe's Cybersecurity Depends on the United States

Europe Can and Must Do More

Alexandra Paulus

The cybersecurity of governments, companies, and individuals in Europe is heavily dependent on the United States. Specifically, US companies dominate the global markets for cybersecurity applications and information on cyber threats. The US military also plays a role in data-gathering. In addition, Washington provides financial support for vulnerability databases and the open source ecosystem. Taken together, these seemingly isolated technical issues mean that Europe's ability to act in the field of cybersecurity is limited. This would even remain the case if Europe built its own "EuroStack." These dependencies can become a problem for Europe in various situations – if the US government ends its financial support for cybersecurity, if it changes its political priorities, or if it openly weaponizes these dependencies in a conflict with Europe. German and European decision-makers should act now to reduce these dependencies and protect Europe's cybersecurity in the long term.

Europe's digitalization has made cybersecurity a prerequisite for functioning democracies and thriving economies. One little-discussed aspect is gaining traction in light of the current transatlantic tensions: the global cybersecurity ecosystem is highly dependent on the United States. This ecosystem comprises individuals, companies, and NGOs involved in developing secure software, protecting systems and devices from threats, fixing known software vulnerabilities, and collecting and sharing information about threat actors. Within this ecosystem, Europe depends on US-based companies and on the US government itself. In this context, it is notable that many US technology companies are growing closer to the administration of President Donald Trump, fueling European concerns about their reliability. Such economic dependencies could potentially be exploited politically.

Europe's dependencies on the United States in the field of cybersecurity are fundamental and go beyond the individual aspects that currently dominate public debate. The latter currently focuses on dependency on cloud providers, software-as-a-service offerings such as Microsoft 365, and security updates. The concern is that US-based entities could withhold updates or deny access to those services. In this context, there have

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

been calls for Europe to develop its own "tech stack" encompassing core hardware, operating systems, and software applications.

But even if Europe succeeded in developing a "EuroStack," large parts of the cybersecurity information ecosystem and markets for cybersecurity products would remain dominated by the United States, as explained below. As a result, Europe depends on the decisions of the US government — which could exploit these dependencies or make political decisions that have implications for Europe.

The Cybersecurity Ecosystem Depends on the United States

American companies and the US government play a central role in the global cybersecurity ecosystem. Five aspects are particularly significant.

US companies dominate the market for cybersecurity applications. US-based companies dominate the European market for cybersecurity software, which is particularly important for individuals and the private sector. The applications include:

- Antivirus software;
- Firewalls, which block unwanted network traffic;
- Endpoint Detection and Response (EDR) services, which monitor endpoints (such as computers or mobile phones); and
- Security Information and Event Management (SIEM) systems, which consolidate information about incidents across an organization's network.

European users of these products rely primarily on US suppliers such as Broadcom, Cloudflare, IBM, and Microsoft. While there are also suppliers outside the United States offering such applications, switching would require significant resources.

US companies dominate the market for information about cyber threats. In order to protect their own systems and devices from cyber threats, IT professionals need appropriate software applications and information about vulnerabilities (described below) as well as information about current and potential threats (cyber threat intelligence, or CTI). CTI allows them to assess the current threat landscape and allocate protective measures accordingly.

The market for CTI is also dominated by US companies, including CrowdStrike, IBM, Google (Mandiant), and Recorded Future. Large companies that also offer other cybersecurity products — especially those that collect data on incidents, such as EDR and SIEM — can more easily provide CTI. The market therefore favors vertically integrated companies. Although there are CTI providers based outside the United States, they tend to have small market shares or be excluded for political reasons, as in the case of the Russian company Kaspersky.

Without CTI from leading US companies, European IT professionals would lose access to information about particularly advanced threat actors. This would leave them without the data required to allocate their cybersecurity resources.

US armed forces gather intelligence on cyber threats. The US military also generates CTI. Specifically, US Cyber Command conducts so-called "hunt forward" operations, in which members of the US military are invited to search for threats in the networks of partner countries.

European countries benefit from this intelligence in various ways. First, Cyber Command may take direct action against adversarial infrastructure and US suppliers of cybersecurity applications improve their products on the basis of the gathered information. Second, previous "hunt forward" operations have focused on Europe, especially the Baltic states and Southeast Europe, thus directly providing European countries with valuable CTI. Third, the US military has shared information obtained through its operations with European allies and published some of it. Such intelligence is presumably a valuable source of information for European defense.

The US government funds vulnerability databases. Due to the sheer number of software products and their vulnerabilities, it is important that the same problem is not recorded multiple times and that all parties involved in fixing vulnerabilities can easily communicate with each other. This requires a global system for identifying and naming vulnerabilities. The Common Vulnerabilities and Exposures (CVE) database serves this purpose.

This database is operated by the US nonprofit organization MITRE, which in turn is funded by the Cybersecurity and Infrastructure Security Agency (CISA), the US cybersecurity authority within the Department of Homeland Security. When a vulnerability is discovered, an affiliated entity checks whether it was already known. If it was not, it is assigned a CVE number. Once the vendor has developed a software update or other mitigation measures, they publish a security advisory referring to the CVE number.

The US National Institute of Standards and Technology (NIST), the standardization authority within the Department of Commerce, operates the National Vulnerability Database (NVD). This database is based on the CVE numbers, which it enriches with additional information, such as the criticality and root causes of the respective vulnerability. Many cybersecurity applications automatically distribute machine-readable NVD data to end users.

Loss of the CVE database would presumably slow the global process of closing software vulnerabilities. Threat actors could take advantage of such delays to carry out more cyberattacks and automated tools would be less reliable and produce errors. Similarly, without NVD data, certain cybersecurity applications would cease to function and cybersecurity teams would lose access to many automated workflows.

The US government supports the security of open source software. Open source software (OSS) is the foundation of the modern software ecosystem. Almost all software applications contain OSS components. If a software product uses a component that has a vulnerability, this is highly likely to become a problem for the product's end users, too. Thus, the security of critical OSS components is crucial for the security of many (open or proprietary) software applications.

Some of these widely used components are maintained by just one person in their spare time, and their resources for IT security are limited. The US government is working to fill this capability gap by providing financial support for securing important OSS projects. Funding comes from the interdepartmental Open Source Software Security Initiative (OS3I), CISA, the National Science Foundation (NSF, which supports foundational research), and the military research agency DARPA. Washington is thus contributing significantly to securing important OSS components.

Cybersecurity Dependencies as a Problem for Europe: Three Scenarios

Critical parts of the global cybersecurity ecosystem — Europe included — are dependent on the United States. Given the current difficulties in the transatlantic relationship, these dependencies — which are intrinsic to a globalized world — could nevertheless become a problem for Europe. The most relevant risks are laid out in the following three scenarios. None of these scenarios has been realized yet, but Washington has already taken decisions that pave the way for the first two.

Scenario 1: **Washington ceases financial support for cybersecurity projects.** One likely scenario is that the US government might reduce or end its support for cybersecurity projects. The Trump administration is committed to reviewing and cutting government spending, specifically through the newly created Department of Government Efficiency (DOGE). CISA and the State Department's cybersecurity units have already experienced significant cuts.

Without US government support, numerous OSS projects would lack the funds to

secure their products and components. This would also indirectly impact all proprietary software products using the affected OSS components. The Trump administration took a first step in this direction in March 2025 when it withdrew funding from the Open Technology Fund (OTF). The OTF supports OSS projects for secure communication and internet freedom, such as the encrypted messenger app Signal. The fund took legal action against the cut and won its case, but it is still unclear whether the government has resumed payments.

Something similar happened with the CVE database. In April, MITRE announced that Washington would be discontinuing its financial support for the vulnerability database, which would therefore cease operating. Probably in response to the collective outcry among the global cybersecurity community, the Trump administration backtracked the following day and announced that funding would continue — but only for eleven months and on a limited basis.

In both cases, the cybersecurity ecosystem narrowly dodged a bullet. If the US government were to cut its financial support for cybersecurity altogether, the effects would be felt worldwide — including in Europe. Such cuts would erode the security of OSS projects and tremendously complicate the processes for finding, reporting, and closing vulnerabilities.

Scenario 2: The US government changes its political priorities. It is also conceivable that the political leadership in Washington could change its political priorities, for example by focusing even more strongly on its rivalry with China. This could lead Washington to turn its back on Europe and, at the same time, to disregard Russian cyber threats.

In that event, Cyber Command's "hunt forward" operations could shift from Europe to countries in China's sphere of influence. That would mean Europe receiving less information about Russian cyber activities. Commercial CTI could follow suit, as US government agencies are important customers for many vendors. If the latter no longer request information about Russian cyber activities, the supply will decline — much to the chagrin of European states, which will likely continue to face threat actors with links to Russian organized crime and the Russian government.

In March 2025, reports that such a scenario might be approaching caused a stir. US Secretary of War Pete Hegseth had reportedly instructed Cyber Command to suspend planning for cyber operations against Russia. In addition, CISA had apparently told its staff to stop pursuing information about Russian cyber threats. While subsequent denials by both organizations cast doubt on the accuracy of these reports, the ensuing discussions illustrate how easily Washington could shift its political priorities and how far-reaching the effects would be.

Scenario 3: The US government weaponizes Europe's dependencies. In the third scenario, Washington deliberately uses Europe's dependencies as a weapon, for example to obtain concessions in other policy fields such as security and defense policy, or in the context of a fundamental deterioration in transatlantic relations. This scenario is less likely than the first two, but still conceivable in light of recent disputes.

In such a case, in addition to the points mentioned in scenario 2, Washington could leverage the market dominance of US cybersecurity companies. For example, they could impose export restrictions to deny Europe access to relevant products. In the past, for example, Washington has severely restricted the export of encryption software, and in October President Trump announced controls on the export of "critical software" to China. If the same was applied to Europe, users there would have to look for new suppliers at short notice and would remain temporarily unprotected.

Possible Effects

Any delay in closing vulnerabilities, reduction in OSS security, or loss of access to cybersecurity applications and information

about the main threat actor would have significant consequences for Europe. Under such circumstances, cyber attacks would be much easier to carry out — whether by criminals or by adversarial state entities (intelligence services and militaries).

Even in the absence of such developments, the cybersecurity situation in Germany has been tense for years and security incidents are on the rise. This affects both private individuals and large and small companies, including critical infrastructure providers, such as airports. Furthermore, public administration and the Bundeswehr are regularly targeted. For example, ransomware incidents have paralyzed German municipalities for months, and cyber attacks on administrative bodies are increasing across Europe. Moreover, cyber operations for espionage purposes have targeted a university and suppliers of the German armed forces.

To protect organizations and users from such threats, IT staff across Europe rely on the aforementioned elements of the global cybersecurity ecosystem. If they no longer had access to these services and information, or if the ecosystem were to become successively less functional, more successful cyberattacks on European targets could follow. Accordingly, the threat exposure is expected to worsen significantly in all three scenarios.

What Action Should German and European Policymakers Take?

European policymakers should not treat the aforementioned dependencies as immutable. Instead, they can and should resolve many of them in order to be prepared for the scenarios outlined above. And even if these scenarios fail to materialize, assuming greater responsibility for the global cybersecurity ecosystem would make European governments, businesses, and societies more secure. Three steps are crucial to achieving this.

Gathering Information About Cyber Threats

To reduce Europe's dependence on US CTI vendors, public procurement projects could, in accordance with the applicable rules, give preference to European CTI vendors. Alternatively, EU policymakers could create a legal framework for companies to share cybersecurity incident data with government agencies — similar to the US Cybersecurity Information Sharing Act (which expired in October). Even without legislation, European cybersecurity authorities could seek closer contact with CTI vendors and promote networking opportunities; they could also draw on research projects such as the European Repository of Cyber Incidents (EuRepoC, whose consortium includes the SWP).

To prepare for the possible discontinuation of US Cyber Command's "hunt forward" operations in Europe, EU member states should carry out such operations themselves. The EU established a corresponding project, Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT), in 2018. This is a so-called PESCO project, in which EU member states and partner countries collaborate in the field of security and defense. Lithuania leads this project, which includes eleven other states (Germany is not among them). However, it has only carried out two missions so far, in Moldova.

CRRT provides a framework for EU member states and partner countries to carry out protective cyber operations, also at the invitation of third countries. Germany should join the project in order to allow experts from the Federal Office for Information Security (BSI) to support it and contribute to the collection of CTI.

Creating Legal Protections for Security Researchers

In relation to the collection of CTI, the German government should also improve the legal situation of security researchers. In many countries, they face legal uncertainty

if not outright criminalization. In Germany, reform proposals have been on the table for years. The last government had started preparing legislation, but the coalition collapsed before the bill was passed. The current government is pursuing no such plans, but it should do so in order to ensure that critical vulnerabilities in software products that are important for European users continue to be reported.

Investing in the Cybersecurity Ecosystem

Unlike the other dependencies, the vulnerability databases represent a crucial single point of failure — but one that is relatively easy to mitigate. They are currently financed by Washington, but Europe could easily take its place. The same is true of financial support for OSS security.

In concrete terms, the European Union Agency for Cybersecurity (ENISA) or the BSI could take over the financing of the CVE database, potentially in collaboration together with other national cybersecurity agencies in Europe. Additionally, the European Union Vulnerability Database (EUVD) was launched in May 2025. While ENISA is keen to present the initiative as complementary to the NVD, it could also replace the US database in the future. However, like the NVD, the EUVD is currently based on information from the CVE database, which makes it all the more urgent to secure the reliable functioning of the latter.

To cushion the blow of the US withdrawing its funding for the OSS ecosystem, Europe should launch its own financing vehicles to support the security of OSS projects. The Sovereign Tech Agency, which is supported by the German Federal Ministry for Economic Affairs and Energy, is an important model. However, with an annual budget of €17 million in 2024, its impact so far has been rather weak. It would be helpful if other EU countries were to join and support it or jointly set up a European counterpart.

If Washington were to discontinue its financial support for cybersecurity projects, European investments could mitigate the negative effects relatively easily. Such funding would also be useful in the other two scenarios outlined above and should therefore be prioritized.

Further Challenges

Europe has the potential to free itself from the dependencies mentioned above. More problematic is the fact that US companies dominate the market for cybersecurity applications. Although smaller European players do exist in this field, their American rivals are likely to retain their dominant position due to network effects. This market constellation could become a problem for Europe if Washington's political priorities changed or the US government chose to weaponize the dependency. In the long run, creating an environment conducive to the emergence of more European CTI companies will require policymakers to prioritize promotion of OSS and support for a European tech ecosystem.

At the same time, however, Europe's dependency on cybersecurity vendors could also be a source of leverage. To this end, European decision-makers should evaluate whether some of the dependencies are mutual — for example, large CTI providers rely heavily on their customers' data on global cyber threats. In the event of a conflict, Europe would therefore have additional instruments at its disposal, such as market access restrictions.

Germany and Europe also face other challenges. First, their strong dependence on US companies is also problematic when the companies in question leave the market (for example, because they go bankrupt). European decision-makers and users should also consider this possibility.

Second, even though the current dependency debate focuses on the United States, Europe remains heavily reliant on China — for example in the area of rare earths for semiconductor production — which is even more problematic. Thirdly, this raises the question of who Europe would turn to if it were to turn away from the US and in the

absence of a “EuroStack”. If software suppliers from China and Russia are not an option, the main options outside Europe vendors are based in Israel, Canada, Australia, and other Asian states.

Experience shows that reducing such dependencies requires political will, resources, and time. And even when these are in place, success is far from guaranteed, as the case of Chinese network infrastructure technology shows. Political decision-makers in Berlin and Brussels should therefore act now to guarantee their future security.

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

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and 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
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: 10.18449/2025C44

(English version of SWP-Aktuell 48/2025)