



INTERVIEW

Interview with Dirk Schrödter and Volker Pötzsch on “Digital Sovereignty: A Question of National Security?”

Walter Brenner · Barbara Brenner · Benjamin van Giffen

© The Author(s) 2026



Dirk Schrödter, Minister and Head of the State Chancellery of Schleswig-Holstein, Germany. Dirk Schrödter, born in 1978, has been Head of the State Chancellery of the State of Schleswig-Holstein since 2017. Since 2022, he has also served as Minister for Digitalization and Media Policy in Schleswig-Holstein. Prior to that, he worked at the Ministry of Finance, where he was responsible for financial planning, budget planning, and federal financial relations. Dirk Schrödter studied economics at the University of Potsdam. He is a lecturer in economics and public finance at the University of Applied Sciences for Administration and Services of the State of Schleswig-Holstein.



Major General Dr. Volker Pötzsch, Chief of Staff Cyber and Information Domain Service Command, Germany. Since 2026, Major General Dr. Pötzsch has been Chief of Staff of the Cyber and Information Domain Service Command and responsible for staff management and coordination. Equipped with extensive knowledge and expertise from various military commands and senior positions, he conducted the digitalization, cyber, IT, Artificial Intelligence, and innovation management in his preceding position as Chief of Division at the Federal Ministry of Defence. Previously he held responsibility for strategic guidance of the Cyber Innovation Hub Bundeswehr and the Agency for Innovation in Cybersecurity at the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support, deepening his expertise on start-ups and innovation. From 2022 to 2023 he was Commander for the Multinational Air Missile Defense Task Force against Russian threats in Slovakia.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

W. Brenner · B. Brenner (✉)
University of St. Gallen, St. Gallen, Switzerland
e-mail: barbara.brenner@unisg.ch

B. van Giffen
University of Liechtenstein, Vaduz, Liechtenstein

Published online: 19 June 2026

Digital Sovereignty¹ is understood as the ability of states, companies, and individuals to use, control, and further develop digital technologies and infrastructures in a self-determined, secure, and independent manner. Over the course of 2025, the topic has evolved into a central issue – particularly when representatives from the corporate sector, public administration, politics, and the military discuss the application of information and communication technology. Against this background, we have conducted two separate interviews to make the various aspects and perspectives regarding digital sovereignty transparent and compiled these interviews into a single conversation. We spoke with Dirk Schrödter, Minister of Digitalization for the state of Schleswig-Holstein and Head of the State Chancellery, and with Brigadier General Dr. Volker Pötzsch, who has served since April 2026 as Chief of Staff of the CIR (Cyber and Information Domain Service Command), the youngest branch of the German Armed Forces (Bundeswehr).

BISE: What is your understanding of digital sovereignty?

Schrödter: Digital sovereignty is also a matter of national security. Digital systems operating within public administration are no longer just technical tools – they have become critical infrastructure. We must be aware: Digital sovereignty is part of state sovereignty. If we lose control over our IT systems, we risk our political and administrative capacity to act. Digital sovereignty therefore means possessing the knowledge, skills, and means to influence IT operational processes, to maintain sovereignty over data storage, and to be able to actively shape solutions. These are times when the very foundations of our rule-based society are being seriously called into question, which must lead to clear – and urgent – consequences for the digital sphere. In light of geopolitical developments, including those in the USA, it is not merely an important state task to maintain independent control over our IT systems. It is essential for guaranteeing internal and external security and for preserving economic independence. This is not about a new form of digital protectionism, but rather about our state's capacity to act.

Pötzsch: For us as armed forces, digital sovereignty means that we can decide on the methods, the data, and everything else that is necessary in a self-determined manner, and that we can operate IT autonomously. In simple terms, digital sovereignty for us implies being capable of acting and making decisions, rather than striving for autarky in IT matters. We have defined six areas in which we strive for digital sovereignty: (1) Core command and control capability, namely the ability to lead troops in a modern digital world at any time and in any place under

any circumstances, (2) trustworthy IT, (3) access to key technologies, (4) innovational capacity, (5) data sovereignty, and (6) digital competencies. I would like to add a comment regarding the so-called 'kill switches'. The Bundeswehr today must live with the reality that every system can be successfully attacked. From the perspective of the Bundeswehr, identifying the attacker is of secondary importance. Whether the actor is a hyperscaler discontinuing services or a military adversary is irrelevant. What matters are the impacts, namely which services we can no longer use and which data have disappeared or been corrupted.

BISE: What is the significance of digital sovereignty?

Pötzsch: Digital sovereignty is of decisive importance for the Bundeswehr. The war in Ukraine shows that armies that sleep through digitalization will not survive, as armed forces are in a specific way depending to all types of information, including classified ones, as information is the ammunition of modern warfare. Specifically, this means that if the German Armed Forces are to fulfill their constitutionally mandated mission for Germany, they must be capable of deploying digitally combat-ready forces to the battlefield. On a digitized battlefield tanks, planes, ships, and other weapon systems are no longer just weapon systems, but nodes in an overall network where information is AI-supported and available in near real-time for everyone in the network who needs them. A fully transparent battlefield depends on the full control of all assets within the network. When using technologies that are 'black boxes', one cannot speak of digital sovereignty, because it remains unknown how these 'black boxes' truly function.

Schrödter: The current situation is characterized by the fact that governments are heavily dependent on proprietary software – frequently provided by only a few global technology corporations. This dominance of a few technology giants within public infrastructure limits our power to shape and our flexibility, threatens our security, and drives up software costs. This constitutes both a technical and an economic threat. With the currently deployed proprietary software, digital sovereignty is unattainable. With open-source solutions, we could attain it. Critical infrastructures can be operated, adapted, and controlled independently with open source. At the same time, the tech giants we are dealing with exploit their technological power economically. Furthermore, the elimination of competition, which can only fully unfold through the use of open standards and open-source software, hinders innovation.

BISE: What are the objectives and measures regarding digital sovereignty?

Schrödter: With the implementation of our 'Open Innovation and Open Source Strategy Schleswig-Holstein', we are, the first federal state in Germany to take a new,

¹ Cf. EU Declaration for European Digital Sovereignty of November 18, 2025, and <https://www.bidt.digital/glossar/digitale-souveraenitaet/>.

sustainable approach for IT infrastructure at the state level – a path that enables us to fulfill our tasks in the digital world independently and securely. Digital sovereignty is the DNA of our strategy: proprietary solutions are being replaced step-by-step with open-source software. In April 2024, with a cabinet resolution, we officially marked the launch of our digitally sovereign open-source standard workplace in Schleswig-Holstein. In this resolution, we announced that Schleswig-Holstein, as a digital pioneer region, will be the first federal state to introduce digitally sovereign IT workplaces for around 30,000 employees in the public administration – a first step toward the state’s full digital sovereignty. Subsequently, we began the broad rollout of LibreOffice as the new standard office solution, and we migrated our email infrastructure to Open-Xchange. Our sovereignty plan is based on further strategic pillars, which we are working on at varying speeds. Currently, we are replacing MS SharePoint with Nextcloud. In the area of telephony, we are developing an open-source solution and are working on replacing MS Windows with Linux. We rely on globally proven and internationally established standard open-source products and adapt them to the requirements of our administration. We think – and this is the further key point in our overall strategy – in terms of ecosystems and have specifically established an Open Source Program Office Schleswig-Holstein. We operate a DigitalHub.SH which, as an operational support unit, provides networking and advisory services in the private sector on the one hand, and manages our state program ‘Open Innovation’ on the other.

Pötzsch: There are the six areas of digital sovereignty mentioned at the beginning of this conversation. For all of these six fields, we have defined concrete goals, operationalized them, and implemented them through a series of measures. Take core command and control capability as an example. One of the concrete goals in this area is to ensure access to digital infrastructures and frequencies. It is of great importance for the Bundeswehr to have secure transmission paths for its data.

BISE: Mr. Schrödter placed open source at the very center of his response. What is the significance of open source for the Bundeswehr, Brigadier General Pötzsch?

Pötzsch: In my view, if we want to increase digital sovereignty, open source is a truly essential step. Open source has enabled self-operation and self-control to an entirely new extent. I can set up open-source software myself and have a company like BWI GmbH,² the Bundeswehr’s IT system house, operate it. In cooperation with BWI GmbH, we have initiatives to enable the widespread use of open source for certain products. A good example of the use of open source is the Bundeswehr Messenger,

entirely new, so that it could be approved for the relevant security levels.

BISE: What role do hyperscalers play when it comes to the digital sovereignty of the Bundeswehr?

Pötzsch: The Bundeswehr has made a conscious decision to adopt a multi-cloud approach. Specifically, we are working with several cloud providers. At the core is our self-operated pCloud BW, a private cloud solution for the Bundeswehr. We have developed our own technology stack for this pCloud BW. The pCloud BW was developed based on VMware products, back when VMware was still under its previous ownership. We also have a Google technology stack within our pCloud BW. To us, a multi-cloud approach means using different technological solutions for different use cases and deciding which provider to choose for each one.

BISE: Minister Schrödter, what strategies have evolved, or are you currently implementing, to strengthen digital sovereignty?

Schrödter: Digital sovereignty can only be achieved through the use of open-source solutions. Only in this way is it possible to maintain a diverse IT vendor landscape that ensures competition and innovation, thereby avoiding both technological and economic dependencies. In summary, the strategic pillars of our digital workplace are the following: LibreOffice replaces Microsoft Office; Open-Xchange and Thunderbird replace the previously used MS Exchange and Outlook; for identity and access management, we are migrating from Microsoft Active Directory to the open-source solution Univention Nubus; Nextcloud is our new collaboration tool and is currently being rolled out step-by-step across all ministries; deployment of the Linux operating system as a replacement for Windows is currently in the pilot phase; the use of the open-source conferencing system OpenTalk for video conferences; and the telephony systems are being redeveloped using an open-source alternative. The open-source software LibreOffice is now the mandatory standard for office applications within the state’s ministries and authorities. In all departments, employees at nearly 80 percent of all workstations other than the tax administration are already using the open-source office suite LibreOffice. Microsoft Office and Outlook have already been uninstalled there or are being removed. Migration paths have been established for the remaining 20 percent of workstations for the coming months. In a six-month migration process involving nearly 44,000 mailboxes and almost 110 million emails and calendar entries, the state administration of Schleswig-Holstein also completed the transition of its email system from Microsoft Exchange and Outlook to the open-source solutions Open-Xchange and Thunderbird on October 2, 2025. In doing so, Schleswig-Holstein has moved a significant step closer to a digitally sovereign IT workplace.

² <https://www.bwi.de/>.

BISE: How much additional effort or investment do you consider justified in order to increase the digital sovereignty of the state of Schleswig–Holstein?

Schrödter: By switching to open source, Schleswig–Holstein is demonstrating that achieving digital independence is both feasible and economically viable. As a result, the state is already saving more than 15 million euros in licensing costs per year. In 2026, this is offset by nine million euros in one-time investments for the migration and further development of open-source solutions. Regardless of that, however, we must ultimately ask ourselves: How much is digital sovereignty worth to us? Can we even quantify the value of digital independence in figures? It is not just about technological autonomy; it is also about economic resilience. A holistic approach – as anchored in our strategy – therefore also encompasses the promotion of the regional digital economy. Instead of spending our IT funds on licensing fees, we are investing in development and support contracts. We in Schleswig–Holstein are convinced that public administration can and must become the driver of innovation in the use of open source and in the introduction of open standards. By doing so, we strengthen the local digital economy and the state of Schleswig–Holstein as a business location as a whole.

BISE: Mr. Brigadier General Pötzsch, has digital sovereignty reached the highest decision-making levels within the Bundeswehr and the Ministry of Defence?

Pötzsch: Yes, absolutely. You can already see this from the fact that we have established the Information Technology Department within the Ministry, which we are continuously expanding. Due to current global and geopolitical events, our forecasts have come true faster than we anticipated. Digitalization plays a key role. As my colleague, General Vetter, always rightly says: ‘He who fails to digitalize, loses’. You can either digitalize sovereignly or dependently. If you digitalize dependently, you are not in a state of freedom and that is something we cannot afford. This is fully understood at the highest levels of the Bundeswehr and within the Ministry of Defence.

BISE: As the Minister for Digitalization of Schleswig–Holstein, what are your demands of the Federal Government and the EU Commission? Which measures must Germany take, and what must the EU do?

Schrödter: We have already established digital sovereignty as a goal in the Federal Government’s coalition agreement. I would like to see us put an even stronger emphasis on this in Germany and launch a clear milestone plan for digital sovereignty. Recently, the federal and state governments approved the so-called Federal Modernization

Agenda. Part of this agenda are also clear statements in favor of a digitally sovereign Germany based on the use of open-source solutions. We must redirect our public budgets and give priority to open-source solutions when awarding IT contracts – also in the interest of an industrial policy for the digital economy. According to studies, even a ten percent increase in EU-wide spending on open-source solutions could generate up to 0.6 percent of additional growth within the EU.

Pötzsch: What is important to me – and this is an appeal I would direct not only to politicians but to society as a whole – is to holistically conceive of and understand digital sovereignty. If our population does not think more deeply about what they consume digitally, how dependent they are on certain applications and providers, and what happens to their data, then we will not be sovereign in a very essential part of our economy and society as a whole. Policy should create frameworks that make it possible to truly achieve innovation capacity, the assurance of the availability of key technologies, and the improvement of digital skills. Society and each one of us as individuals must strengthen our digital skills and act more consciously.

BISE: Thank you very much for taking part in this conversation and providing us with such fascinating insights. This topic will likely continue to occupy us for a long time to come. Against the background of this conversation, the question of whether digital sovereignty is a matter of national security can certainly be answered with a ‘yes’.

A future issue of BISE will feature a further conversation on digital sovereignty.

Funding Open access funding provided by University of St.Gallen.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.