April 2026
Version 1.0 EN

DIGITAL SOCIETY

DIGITAL SOVEREIGNTY OF THE FOOD SUPPLY CHAIN

A DIGIGES STORY

Authors: Philippe Gervais, Ryan Kougionis, David Sommer, Alexander Steiner, Marcel Waldvogel

Many things happen before someone can enjoy a fondue. Farmers raise cows and grow wheat, sell their products to various companies before they reach supermarkets like Coop or Migros. Both wheat and milk are transformed into bread and cheese, often by intermediate companies such as Emmi, Swissmill or Fenaco. It is a complex supply chain with many paths, constraints, and regulatory requirements. It would not be able to function without the use of a lot of software. If any of those pieces are unavailable or fail, the table will stay empty. The food supply chain has always been a very important topic for governments around the world, who have been very attentive to possible disruptions. The recent shift in the geopolitical situation has brought to light new software-related risks.

Agricultural machinery depends on software. Modern tractors and other agricultural machines are increasingly computerized and connected to the internet. This allows them to perform tasks like plowing or sowing with minimal human input. Tractors can be programmed to follow precise patterns in a field, improving efficiency and consistency compared to manual operation. Unfortunately, these digital systems also make it possible to remotely disable tractors. As recently as 2022, John Deere has demonstrated that they were able to permanently disable tractors that had been looted by the Russian army from Ukraine. The mechanism they used is not limited to wartime, though: it can be used against any John Deere tractor in the world, including those in Switzerland. Other implications of this situation are that customers are completely dependent on manufacturers when it comes to repairs, replacement parts, or simply software bug fixes. This causes higher costs for farmers and can potentially slow down repairs at crucial times like harvest.

While only John Deere has demonstrated the presence of a 'kill-switch' in their equipment, it is reasonable to assume that others (e.g. Kubota, AGCO, New Holland) have one as well or could deploy it with their next software upgrade. What it means in practice is that a large part of Swiss agriculture could be slowed down or disabled in a matter of hours through computer systems operated by foreign companies, most of them outside the legal reach of Switzerland.

> **Digital sovereignty** of a state or organisation requires full control over stored and processed data, as well as over the applications used to process that data. It encompasses the independent decision of who may access which data. It also includes the capability to develop, modify, control and augment technological components and systems autonomously, and to operate those systems effectively. Digital sovereignty provides protection against a variety of risks such as espionage, extortion, price hikes, and also creates strong negotiation positions.

Efficient logistics needs computers. Logistics includes all the processes needed to distribute the pro-

duced goods. It requires a dizzying array of tools such as inventory tracking, demand prediction, accounting, regulatory compliance, route optimization for delivery vehicles, etc. None of this would work efficiently without software. The market is currently dominated by three actors: SAP (Germany), Oracle (USA), and Microsoft (USA). Similar to tractors, this software is operated only with their manufacturer's permission, which can be revoked at any time, for example if a license fee is not paid. Losing access to logistics software would immediately cripple the companies using it. Dependencies don't stop there: a large part of this runs on datacenters operated by other companies - also mainly from the USA. Shutting down a datacenter would have the same effect as disabling the software entirely, severely disrupting the food supply.

Payment systems rely on USA-controlled infrastructure. Paying with a credit card at a store? These are operated within a duopoly: Visa and Mastercard, both US companies which can block transactions for individuals or countries under US sanctions. For example: in 2022 the US government used this mechanism to cut off services to Russian banks after the invasion of Ukraine. Allied countries are not safe from this practice though: In August 2025, French judge Nicolas Guillou at the International Criminal Court was banned from using his credit card after issuing arrest warrants for Israeli Prime Minister Benjamin Netanyahu. While Switzerland is unlikely to face a full ban, Visa and Mastercard could take more subtle actions like raising fees. It would leave Swiss businesses with little recourse other than using an alternative payment system like Twint. A similar situation exists for international trade, which is essential for Switzerland because it is not self-sufficient for food: international payments rely heavily on the SWIFT system, which is also US-controlled.
All these examples show how a foreign power could take unilateral action and severely disrupt the food supply chain, through software. The risk is particularly high because we don't have alternatives readily available.

How do we address this? By making sure that for all critical software, Switzerland is in full control over stored and processed data, as well as over the applications used to process that data. That means in practice owning and operating our own software infrastructure. In the current situation, it's a tall order. The amount of software used by the food industry is staggering, and replacing it with digitally sovereign solutions (see info box) will take a lot of time and effort. But we can prioritize. Some systems are more vital than others: losing access to a positioning system for delivery trucks will cause some disruption but will not block delivery entirely - drivers will quickly re-learn to locate themselves without a GPS. However, not being able to operate a tractor or a warehouse would be critical, because manually tilling the fields or manually lowering heavy pallets in a high rack warehouse is simply not a realistic option anymore. We thus need to ensure that even in the event of someone activating a kill-switch, we would be able to reset the tractors or the forklifts and continue operating them.

> **Free and Open Source Software (FOSS)** is computer software distributed under terms that grant users four rights:
>
> - to run the software for any purpose
> - to study it, via access to its source code
> - to change it
> - to distribute it and any adapted versions
>
> Free software is a matter of liberty, not price; all users are legally free to do what they want with their copies of free software (including profiting from them) regardless of how much is paid to obtain the program. Examples of Free software are the Firefox browser, VLC, 7-zip, Libreoffice, and the Signal messaging app.

Even with prioritization, no country has the resources to re-create from scratch all the software that it needs, and Switzerland is no exception. Using Free and Open Source Software (FOSS, see info box) is a good solution to this problem because existing FOSS already covers a lot of use cases, and the work of developing it more can be shared across multiple countries. It would virtually eliminate the dependency on a small number of powerful actors. FOSS brings the best of both worlds: development effort is shared - limiting cost - while ensuring that all users can stay in full control of the software they are running. Switzerland has a lot of qualified professionals: encouraging the development of FOSS in general would improve on digital sovereignty and at the same time strengthen Switzerland's economy, innovation, and self-determination.