BÄR & KARRER BRIEFING APRIL 2024

SWISS CYBER DEFENCE: FORCED RECRUITMENT OF PRIVATE IT EXPERTS AND INFRASTRUCTURE CONSIDERED

The Swiss Military Act revision proposes granting the Swiss Federal Council power to requisition IT experts and infrastructure for military resilience, especially against cyber threats. It includes an extension to peacetime, requires Swiss Federal Council approval, and provides for compensation provisions. The consultation ended in March 2024. The provision, under review post-consultation, advises companies to monitor updates and prepare strategies for potential requisitions.

In Switzerland, there is an ongoing revision to the Swiss Military Act which, among others, will give the Swiss Federal Council the right to recruit private IT experts and requisition IT infrastructure, if required to protect the Swiss Armed Forces' supply chains and military information and communication technology and to maintain operational continuity and resilience in the face of threats, in particular in the cyber area.

In detail, the previously non-existent article 95 of the consultation draft of the Swiss Military Act reads as follows (unofficial English translation, emphasis added):

Art. 95 Business continuity and resilience

[1] In order to protect the Armed Forces' supply chains and military information and communication technology and to maintain operational continuity and resilience in the face of threats, in particular in the cyber area, the Military Administration and the Armed Forces may, with the exception of radio frequencies:
a. restrict or prohibit the use of requisitioned goods;
*b. **requisition requisition goods**.*

[2] Such measures require the approval of the Federal Council.

[3] The Confederation shall pay appropriate compensation for the restriction or prohibition of use and the requisition of the requisitioned property.

[4] Restrictions and bans on use and requisitions shall be issued by the competent bodies of the Military Administration and the Armed Forces. The procedure shall be governed by the Administrative Procedure Act of 20 December 1968.

[5] The Federal Council shall designate the competent bodies of the Military Administration and the Armed Forces and describe their tasks in more detail.

In military terms, requisition means the confiscation of civilian property for military purposes.

According to the consultation draft, the extension of requisition rights to intangible property applies in **times of crisis** as well as in **times of peace**.

It can have **considerable consequences** for companies in the private sector and is accompanied by a **loss of legal and planning certainty**: Large and small tech companies in particular, but also all other private companies that employ cyber or other IT experts, could be confronted with the reality that their employees are recruited from one day to the next and that they need to make their IT infrastructure (e.g., servers, software, network resources and services) available for the Swiss Armed Forces – assuming the approval of the Swiss Federal Council.

A protective mechanism to ensure that the company itself still has the cyber or other IT experts and infrastructure required to ensure the continuity of its own operations is not provided for in the consultation draft. The sudden loss of key cyber or other IT personnel and IT infrastructure could disrupt the operations of companies. With the possibility of requisition looming, companies may find it challenging to plan long-term strategies, which is crucial for maintaining a competitive edge. In addition, companies may need to invest in redundant systems or hire additional cyber or other IT personnel as a buffer against potential requisition, leading to increased operational costs.

On a positive note, if managed well, such requisitions could lead to stronger public-private partnerships, with companies collaborating closely with the government on cybersecurity and national defence projects.

The procedure for requisitions under the revised article 95 of the Swiss Military Act shall be governed by the Federal Act on Administrative Procedure of 20 December 1968 (APA). Firstly, this means that the procedural rights provided for in the APA apply, *i.e.*, that the companies affected by the requisition have, for example, a **right to inspect the files** and must be **heard before the order is issued** (article 30). Secondly, this means that the companies concerned have the **right to appeal** against an order. The Swiss Federal Administrative Court (*Bundesverwaltungsgericht*) will be the appellate authority according to a newly introduced article 33 lit. h^{bis} of the Federal Act on the Swiss Federal Administrative Court of 17 June 2005.

According to the consultation draft, the federal government would pay compensation if it exercised its right of requisition, but only **appropriate compensation** would be paid, i.e., arguably not full compensation.

This new legal provision is **not yet set in stone**. The consultation process was completed in March 2024 (*see* https://fedlex.data.admin.ch/eli/dl/proj/2023/26/cons_1 for the full file). The Federal Department of Defense, Civil Protection and Sport DDPS (*VBS*) is currently reviewing the comments received and will then present a draft revised act.

Large and small tech companies in particular, but also all other private companies that employ cyber or other IT experts or operate IT infrastructure, should keep a close eye on further developments and, should article 95 be retained in the form envisaged in the consultation draft, take appropriate measures to prepare for the requisition, such as developing contingency plans, enhancing training for other staff members or exploring temporary replacements.

AUTHORS

Dr. Christian Kunz

Partner, Prosecutor of the Swiss Armed Forces

christian.kunz@baerkarrer.ch

T: +41 58 261 52 66

Christian Kunz co-heads Bär & Karrer's Data Protection & Digital Economy as well as Technology, Media & Telecommunications (TMT) practice groups. He is an expert in the field of data, data protection, cybersecurity and technology law. He advises clients on data strategies and related processes, the use and monetisation of data, (cloud) outsourcings, international data transfers, data disclosure requests, and data breach incident management and recovery. He also advises on data-driven business models and platform solutions (XaaS, cloud services, IoT) and advanced technology projects (AI, Machine Learning, etc.).

Eric Stupp

Partner, former Prosecutor of the Swiss Armed Forces

eric.stupp@baerkarrer.ch

T: +41 58 261 53 90

Eric Stupp heads Bär & Karrer's financial services department and co-heads the internal investigation and cross-border proceedings team. His practice focuses on advising banks, insurance companies, asset managers and other financial intermediaries on regulatory matters, enforcement proceedings and on M&A transactions. In recent years, he has regularly advised financial institutions and regulatory bodies in connection with internal investigations on cross-border issues. In particular, he has assisted clients in numerous proceedings initiated by the US Department of Justice, the New York Department of Financial Services and other US and European authorities.