Audit of the effectiveness of the fight against cybercrime

Federal Office of Police

Key facts

Digital crime has fluid boundaries, elusive perpetrators and often involves an international dimension. It represents a challenge for the prosecution authorities. In nine out of ten cases, these crimes fall under cantonal jurisdiction. However, the Federal Office of Police (fedpol) plays an important role in this fight: as the central office and international contact point, it supports the cantonal police forces. In addition, fedpol supports the Office of the Attorney General of Switzerland (OAG) in complex cybercrime proceedings under federal jurisdiction.

The Swiss Federal Audit Office (SFAO) audited the effectiveness of fedpol's fight against cybercrime. The SFAO visited the cantons of Aargau, Bern, Vaud, Ticino and Zug as well as the OAG to gain an insight into the environment in which fedpol operates and the views of its partners. The services of the Federal Criminal Police (FCP) – its Forensic IT & Cybercrime Division and its Economic Crime Division – are appreciated by the cantons and the OAG. The fight against online paedophlia is still under discussion between the cantons and the Confederation. However, the SFAO identified ways to improve the efficiency of the FCP's case management, its analytical capabilities and its cooperation with the OAG.

Adequate resources at fedpol and good marks from the cantons for its services

The analysis of a sample of the Forensic IT & Cybercrime Division's personnel files shows that employees' skills are in line with their tasks, although there are differences depending on the role. The SFAO sees a risk of demotivation among Forensic IT & Cybercrime Division employees who have only recently joined the organisation and/or have specialised training, due to the fact that salary progression is based on seniority.

The cantons which the SFAO visited appreciated the Forensic IT & Cybercrime Division's services and its assistance in international cooperation. Due to a lack of resources, these cantons identified a need for cybercrime analyses that fedpol could develop in the future. In addition, the Forensic IT & Cybercrime Division also screens the reports of prohibited images submitted by its partners – such as the National Center for Missing and Exploited Children – and refers them to the cantons. In the SFAO's view, under the current legal framework, fedpol should improve its follow-up of these referrals to its cantonal partners.

Cooperation and differences with the OAG, appropriate centralisation of procurement at the federal level

Together with fedpol, the OAG's Cybercrime Sub-Division handles complex cybercrime cases. It cooperates with the FCP without any significant problems. However, the OAG and fedpol disagree on the creation of a "cyber office" within the FCP, as a counterpart to the OAG's Cybercrime Sub-Division. To increase efficiency, these authorities reorganised themselves over the last ten years and aligned their structures ("mirror effect"). However, this ceased to be the case with the creation of the OAG's Cybercrime Sub-Division at the end of

2019. Communication between these authorities was not optimal either. The SFAO recommends that fedpol analyse the advantages and disadvantages of a "cyber office" at the FCP or any other solution to ensure the availability of resources for the OAG's cybercriminal proceedings by July 2021.

The federal entities – including fedpol and the OAG – and the cantons spend several million francs a year on forensic IT services from a single company. This company generates around 80% of its turnover from the public sector. The SFAO recommends that fedpol establish a competence centre for the Federal Administration, especially in the area of forensics, and thus centralise the needs to provide a cost-effective and efficient response in this field.

Priority should be given to strengthening the application environment and digital processing of files

At the Forensic IT & Cybercrime Division and the FCP, the digital processing of investigation data is not without risks. Fedpol management identified this at the beginning of 2019. The situation should be improved through the investigation system (ErmSys) programme, which has an ambitious deadline of 2022. The SFAO recommends that fedpol prioritise the ErmSys programme in order to ensure an adequate, secure framework for the traceability of information for the FCP's federal and cantonal partners and to provide effective support for its teams.

Without efficient and automated management tools, the FCP is exposed to the risk of insufficiently structured case management, limiting its room for manoeuvre and anticipation of problems. These difficulties are illustrated by the analysis of around 170 phishing cases. This analysis was requested by the OAG in 2017 and was completed in October 2020. The OAG is still waiting for the delivery of the police reports. In the future, the FCP plans to create a modern monitoring system as part of the improvements planned by fedpol. The SFAO recommends that fedpol strengthen the tools for steering the FCP's activities by means of a monitoring system (cockpit and indicators) for case management, including the follow-up of fedpol's reports to the cantons (prohibited images).

Clarifications welcome in the fight against online paedophilia

At the end of 2019, Parliament allocated four posts to fedpol for internet paedophilia. The documents received by the SFAO show partial traceability in the creation of these positions, two of which were not within the FCP. It is not clear from the documents whether or not fedpol complied with Parliament's wishes. The SFAO recommends that fedpol examine and justify the allocation of posts so that the parliamentary decision and the needs expressed by the cantons can be met.

Online pedophilia falls under the jurisdiction of the cantons. Since 2001, however, fedpol has been actively investigating this crime on behalf of the cantons. The SFAO found that undercover investigations against paedophiles on the internet were paused for nine months in 2018. With effect from 1 January 2021, these active investigations were transferred to the cantons under an agreement between the Conference of Cantonal Justice and Police Directors and the Conference of Cantonal Police Commanders of Switzerland. Implementation is the responsibility of the cantons, whose resources to meet this challenge are being developed. The SFAO welcomes this clarification of the work done by fedpol and the cantons.

Performance indicators for the national strategy for the protection against cyber-risks

The SFAO audited the criminal law component of the national strategy for the protection of Switzerland against cyber-risks (NCS II) and the implementation of the related measures. The National Cybersecurity Centre (NCSC) coordinates these activities and carries out strategic management control. It recognises that there are risks in relation to criminal matters that are not fully covered. However, these risks are subject to an assessment process to evaluate what further measures should be taken.

The NCS II measures to be implemented to combat cybercrime are of a general nature and their timetables need to be clarified. The NCSC does not critically monitor their implementation. For a future NCS III, the SFAO recommends that a system of performance indicators be developed to assess whether the objectives of each measure have been achieved.

Original text in French