SWEDISH NATIONAL AUDIT OFFICE

REPORT NUMBER: RIR 2015:21
DATE: 17 DECEMBER 2015

Summary:

Cyber crime – police and prosecutors can be more efficient

The Swedish NAO has audited whether the Swedish Police Authority and the Swedish Prosecution Authority have a preparedness to process and investigate cyber crime appropriately and efficiently.

Audit background

Cyber crime is a growing problem. For all crime, the proportion of person-based clearances fell from 18 to 15 per cent during 2006–2014, which is the lowest level to date. The proportion of person-based clearances for the audited cyber crimes is constantly at a lower level and was 7 per cent in 2014. It is important that the Swedish Police Authority and other parts of the judicial system are able to keep up with developments in the area in order to prevent any deterioration in the field of criminal investigations. Confidence in the judicial system risk declining when people are affected by crime and their cases are discontinued instead of being investigated.

The audit covers three categories of crime; online fraud, online child pornography crime and attacks on infrastructure. The Swedish NAO assesses that these three categories can illustrate how cyber crime as a whole is being processed and investigated. The main focus in the audit is the process from a crime being reported to the decision on whether to prosecute or not. The audit covers the Government, the Swedish Police Authority and the Swedish Prosecution Authority.

Audit findings

All in all the audit shows that the lack of recognised methodology support, developed working methods, sufficient skills and specialisation in the area mean that the police and the prosecutors do not have preparedness and capacity to investigate and process cyber crime efficiently and appropriately. The deficiencies identified also risk leading to cyber crime not being processed consistently and uniformly, thus making the way a crime is

investigated more dependent on individuals. Moreover, the audit shows that altered working methods could possibly improve the proportion of person-based clearances.

Cyber crime requires altered working methods

The number of reported cyber crimes is increasing substantially, while the proportion of person-based clearances is falling and many cases are discontinued without investigation. Cyber crime is often complex to investigate, digital evidence is often difficult to secure and it is possible to commit crimes online anonymously. Police and prosecutors therefore face major challenges in handling the criminal development.

The police and the Swedish Prosecution Authority have been late in emphasising cyber crime, but the area has been raised more in internal policy documents and strategies since 2013. Cyber crime has thus not been paid any greater attention at management level. The Swedish NAO finds that the agencies' recent actions to increase their capacity in the area are a positive change, but considers that long-term and sustained work is required to achieve results.

Agencies lack national guidelines and methodology support

The audit shows that the Swedish Police Authority lacks methodological support, recognised national guidelines and manuals for investigating cyber crime. For example, digital aspects are not part of the National Investigation Concept of the Police. Many Public Prosecution Areas are unaware of the Swedish Prosecution Authority's manuals that refer to the area.

Low level of skills in agencies

The level of education concerning investigation of cyber crime is generally low in the Swedish Police Authority and the Swedish Prosecution Authority. Only a few of the leaders of preliminary investigations, investigators, digital investigators, digital forensic experts and prosecutors have completed programmes on digital investigations. In addition, the basic police training does not generally include any segment on cyber crime. Some police officers are self-taught in cyber crime investigations and have a good knowledge of the area. Without a larger element of formal education, individual police officers will not have the skills required to carry out sound investigations, and implementing uniform working methods will be more difficult. The Swedish NAO's survey also shows that the training programmes within the Swedish Police Authority and Swedish Prosecution Authority in the area of cyber crime are not sufficient. There is

a demand for both more of the digital aspects in the basic police training and more further training, for example in internet surveillance. Lack of time, costs and a limited number of training places constitute obstacles to attending the existing programmes.

Specialised units may be a success factor

The audit shows that 92 per cent of the preliminary investigations that led to person-based clearance were investigated by a specialised unit, compared with 30 per cent of the discontinued preliminary investigations. For example, fraud cases were often investigated by fraud units. According to the Swedish NAO, this may indicate that specialisation in the investigative operations can improve the conditions for solving crime.

There must be increased cooperation and exchange

Many of the cases audited by the Swedish NAO were discontinued based on the crimes being committed abroad. However, international legal assistance was not requested in any of the cases included in the case file review. It could be possible to use international legal assistance more, despite the view of representatives of the agencies that this procedure is time-consuming and administratively complicated. Furthermore, there are indications that the Swedish desk at Europol in The Hague could be used to a greater extent.

The Swedish Police Authority often requires information from foreign companies in order to investigate cyber crime. The cooperation with foreign companies has been partly facilitated by the agency having developed a consensus for cooperation with certain central foreign companies delivering internet-based services.

The Swedish NAO's survey shows that the Police Regions have a different understanding of how cooperation and interaction between regions functions. According to representatives of the Swedish Police Authority, it can be difficult to reach out into the police organisation since contacts are often founded on personal networks. The Swedish NAO considers this an indication that clearer structures for cooperation and interaction within the Swedish Police Authority are needed. There has been a recent clarification of the Swedish Prosecution Authority's structures for exchange of experiences between prosecutors knowledgeable in investigation of cyber crime.

REPORT NUMBER: RIR 2015:21
DATE: 17 DECEMBER 2015

Many cyber crimes are difficult to investigate

Many cases are discontinued due to the crime being committed abroad, that there are no investigation leads or that the crime was too minor for certain investigation measures, such as secret coercive measures, to be used. The type of crime also has a decisive significance for whether it is investigated or not. Some types of data security breaches perpetrated via the internet and online fraud are by and large never investigated. These are a part of a criminality where the chances of successful criminal investigations in individual cases are almost non-existent today. The Swedish NAO thus notes that there are some types of crimes where, under current legislation and using current working methods, the police and the prosecutors have more or less no framework for taking investigative measures.

The police and the prosecutors can work more efficiently and more uniformly

The Swedish NAO notes that many cyber crimes are generally difficult to investigate. At the same time, the audit shows that altered working methods would enable improvements to the proportion of person-based clearances. The Swedish NAO notes for example that the police and the prosecutors have succeeded in reversing the trend in online child pornography crime, where the proportion of person-based clearances has improved continuously since 2006. Probable contributory factors are changed legislative conditions, that the Swedish National Police Academy started to offer a specialised programme in the area in 2006 and that this type of crime was given special priority by the police leadership in 2014.

The police and the prosecutors must initiate the first investigative measures faster to ensure that digital evidence does not disappear. A prerequisite for preventing delay or obstruction of investigative measures is that the police reports contain all the relevant information. The case file review shows that the IP address was noted incorrectly in about 20 per cent of the reports containing an IP address, the consequence being that the information cannot be used. The Swedish NAO's case file review also shows that there were earlier investigative measures in the preliminary investigations that led to person-based clearance than in those that were discontinued.

The police and the prosecutors take few digital investigative measures in the preliminary investigations. Traditional investigative measures, such as tracing bank accounts, are instead the most common. It is not always necessary, or even possible, to take digital measures in every individual case in order to solve that crime. However, the Swedish

REPORT NUMBER: RIR 2015:21
DATE: 17 DECEMBER 2015

NAO's case file review shows that it is possible to take more digital investigative measures. Such measures may also contribute valuable intelligence information. For example, storing IP addresses in one place could enable the Swedish Police Authority to work more systematically on serial crime as well as improving the conditions for solving crimes. There may also be a reason to involve more different actors in the preliminary investigations; digital forensic experts and companies have for example participated to a greater extent in the preliminary investigations that led to person-based clearance than in those that were discontinued.

The Swedish National Audit Office's recommendations

Recommendations to the Swedish Police Authority

- Identify national development needs and develop the strategic competency management to ensure that operational needs are met. Plan, encourage and create opportunities for skill enhancing measures in the cyber crime area.
- Ensure that the basic police training corresponds to the needs of the operations with regard to technological development and its impact on criminal activity.
- Develop and gain acceptance for national working methods and methodology support for investigating cyber crime.
- Review the structure for crime coordination and interaction between Police Regions.
- Use the forums available for international coordination and cooperation.

Recommendations to the Swedish Prosecution Authority

- Identify national development needs and develop the strategic competency management to ensure that operational needs are met. Plan, encourage and create opportunities for skill enhancing measures in the cyber crime area.
- Develop and implement methodological support for investigating cyber crime and opportunities for exchange of experience between Public Prosecution Areas.