



FOLKETINGET
STATSREVISORERNE



FOLKETINGET
RIGSREVISIONEN

September 2025
– 24/2024

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

The Ministry of Defence's protection of information on weapons

1. Introduction

1.1. Purpose and conclusion

1. This report examines how the Danish Ministry of Defence protects its information on weapons, ammunition and explosives that employees have access to in the ministry's IT systems. We collectively refer to weapons, ammunition and explosives as weapons.

Information on weapons include details about the types and quantities held by the Danish Defence, as well as the locations of the weapons. The weapons are stored in many different locations including barracks, depots outside the barracks and the homes of Danish Home Guard volunteers.

2. Weapons are important for the military capability of the Danish Defence and their misuse can have fatal consequences. According to the Ministry of Defence's own security regulations, weapons require special protection.

To protect the Danish Defence's weapons, it is crucial that the ministry restricts access to information on weapons in the ministry's IT systems strictly to employees who need it for work purposes. It is also crucial that the ministry monitors the employees' system use in order to detect suspicious activity. Failure to protect information on weapons adequately increases the risk that it could fall into the hands of unauthorised persons and, for instance, be exploited for purposes of espionage, sabotage or other criminal activity.



Shooting exercise.

Photo: Henning Bagger
/Ritzau Scanpix

The Ministry of Defence operates two IT systems contain information on weapons. The systems are used by employees across the ministry. Employees with access to the information can view a significant portion of the Danish Defence's stock of weapons.

3. In 2024, the Danish Defence Intelligence Service (DDIS) reported that the threat against Denmark had become more serious. The report is based, among other things, on the assessment that *"Russia is acting more boldly towards countries in Europe and, among other things, has carried out sabotage actions."* According to DDIS, foreign states – especially Russia and China – are engaged in espionage against Denmark. DDIS assessed that *"Both Russia and China are trying to gain access to information about political processes, foreign, security and defence policy and military capabilities."*

According to the Centre for Cyber Security, employees represent a potential entry point into any organisation, since they may – intentionally or unintentionally – spread, damage or alter information. Employees who unintentionally act harmfully are, according to the Centre for Cyber Security, involved in up to half of all security incidents.

It is publicly known the Danish Defence's weapons have previously been stolen and subsequently used in criminal activities.

4. The purpose of the study is to assess whether the Ministry of Defence has ensured adequate protection of employees' access to information on weapons in the ministry's IT systems.

Rigsrevisionen initiated the study in August 2024.

The Ministry of Defence acknowledges that weapons require special protection. Information on weapons is classified but, according to the ministry, common in the Danish Defence and does not require special protection. Thus, the ministry does not protect information on weapons differently than information on other items such as socks and uniforms.

Rigsrevisionen notes that, the security circular and the Ministry of Defence's security regulations require the ministry to protect classified information – including information on weapons. To protect the information, the ministry should limit access to employees who need it for work purposes. The ministry's security regulations are intended, among other things, to protect the ministry's IT systems against espionage, sabotage and other criminal activity.

5. The Ministry of Defence has assessed that some of our findings cannot be disclosed publicly. According to the ministry, the findings concern security conditions relating to the ministry's IT systems, and Rigsrevisionen's descriptions of them could potentially facilitate criminal activity. Rigsrevisionen has complied with the ministry's request for confidentiality. The report, while being based on comprehensive and detailed material, therefore provides only general and summarised descriptions of the issues.



Conclusion

The Ministry of Defence's protection of employees' access to information on weapons is highly unsatisfactory. The ministry has granted many employees access to information on weapons in the ministry's IT systems without assessing whether they need the information for work purposes. Additionally, the ministry does not adequately monitor who accesses the information. Consequently, the Ministry of Defence fails to comply with several requirements of the international information security standard and several of the requirements of the ministry's own security regulations.

The consequence is an increased risk that employees could intentionally or unintentionally disclose information on the Danish Defence's weapons, which can be used for purposes of espionage, sabotage and other criminal activity.

Some of the employees with access to the IT systems have access to detailed information on weapons such as the quantity of weapons, types of weapons and their locations. The ministry has not assessed whether the employees need this information for work purposes. The ministry also does not adequately monitor who searches for information in the IT systems and which information is being searched for.

The Ministry of Defence has stated that all employees with access to the IT systems have a security clearance. The ministry has also stated that access to information on weapons in the IT systems cannot be considered in isolation but must be seen alongside the protection of the military areas where the Danish Defence stores weapons. This is because unauthorised persons can only gain access to the weapons by breaching those areas. Rigsrevisionen's report on the Ministry of Defence's protection of military areas shows that the ministry's protection of the areas warrants criticism.

Rigsrevisionen assesses that the Ministry of Defence should determine whether employees with access to information on the Danish Defence's weapons actually need the information for work purposes. This applies regardless of whether the employees have a security clearance and regardless of whether the military areas are sufficiently protected. Rigsrevisionen emphasises that information on weapons, either in isolation or combined with other sources, can be used for purposes of espionage, sabotage and other criminal activity and therefore must be protected.

The Ministry of Defence has stated that it intends to strengthen its IT security and its protection of the military areas.

Military areas

Military areas are land and buildings used by authorities under the Ministry of Defence. Military areas include, among others, barracks, naval bases, air bases, training areas and shooting ranges.