Conclusions of the National Audit Office

Cyber protection arrangements

The purpose of the audit was to investigate whether cyber protection in central government has been arranged as effectively and cost-efficiently as possible. The audited entities included the authorities governing cyber protection in central government (the Prime Minister's Office, the Ministry of Finance, the Ministry of Transport and Communications) and the authorities handling centralised cyber protection tasks and centralised IT services in central government (the National Cyber Security Centre Finland of the Finnish Communications Regulatory Authority, Government ICT Centre Valtori, the Population Register Centre). Functionality of steering was also assessed by investigating central government units that offer electronic services (the Population Register Centre, the Finnish Transport Safety Agency Trafi, the National Administrative Office for Enforcement and the authority governing it, the Ministry of Justice, and Legal Register Centre, the ICT service centre of the Ministry of Justice's administrative sector).

Operative management of extensive cyber security violations has not been determined

The division of labour and responsibilities in case of a cyber security violation complies with the rules of procedure of the Government. In ambiguous cases, responsibilities in case of a cyber security violation have been determined through negotiations between ministries. However, negotiations during an ongoing cyber security violation can take too much time when taking into account the time available for retaining control of the situation. Planning operational management of extensive cyber security violations and division of related responsibilities could allow for faster reactions and appropriate coordination and resource allocation for countermeasures.

The current operating model is that each agency is responsible for its own cyber protection. There is not enough expertise in cyber protection available, however, which hinders the creation of cyber protection on one's own and the creation of cyber protection based on purchased services. Operations for which state agencies are responsible that were previously handled by the agencies themselves have been centralised to state service centres in connection with service centre projects. The need for more standardised and comprehensive risk management has increased due to the centralisation. The risk management practices used by the agencies vary, however. The lack of standardisation in risk management may cause gaps in the protection of confidential information, for example. No information that supports the prioritisation of service protection in case of a comprehensive cyber security violation have been collected from central government services.

Some Cyber Security Strategy goals have not been achieved

The implementation programme for the Finnish Cyber Security Strategy (2013) has improved cyber protection. The strategy has drawn attention to a uniform vision, integration of preparation as part of operations and cyber protection capacity.

Some of the goals of the first implementation programme were not reached, because the level of commitment to the actions varied and the level of commitment could not be improved in a centralised manner.

Only actions to which the competent authorities and other actors have clearly committed were included in the new implementation programme. The level of commitment and available resources are linked. Monitoring of the programme has been improved to offer government leaders a better idea of the current status of cyber security.

At present, a key uniting force in the development of cyber security is cooperation between the Cyber Security Centre and the National Emergency Supply Agency.

Appropriateness of cyber protection funding solutions is unclear

The differences in the development of cyber protection are partially due to the differences in the amount of development resources the organisations have at their disposal. Regardless of the size of the state and the organisation, certain basic cyber security issues must be in order. Lack of information critical to cyber protection and lack of cyber protection expertise hamper the protection from cyber security violations whose effects are severe and extensive. The significance of critical expertise and networking is especially pronounced in the Finnish central government, because its systems are decentralised.

The Committee of Transport and Communications has issued an opinion (27/2013 vp) where it requires monitoring of the required cyber security operations resources in order to ensure that the increased number of tasks due to changes in the operating environment is taken into account when determining resources and funding. Based on the audit observations, it is unclear whether the opinion has been taken into account to a sufficient extent.

No procedures to ensure that funds are allocated to the targets most important for cyber protection have been identified in the regulations on the preparation of the state budget or the preparation process. The agencies budget cyber protection funds in the budget article for operating expenses as a non-itemised part of expenses from the operations of the agency. The fact that cyber protection services are subject to a charge influences both the demand for the Cyber Security Centre's cyber protection services and the Centre's opportunity to offer the services and retain its high level of expertise. Ultimately, the fact that the agencies are dependent on each other via the service centres, among others, and the opportunity of the agencies to obtain the cyber protection services subject to a charge from the Cyber Security Centre with the funds included in their budget articles for operating expenses influence the Cyber Security Centre's operating conditions.

Actions in compliant with the Finnish Cyber Security Strategy are only implemented as far as the funds allow. However, funding for the National Emergency Supply Agency has ensured implementation of actions pertinent to the national emergency supply, as well as cyber protection of central government by indirect means.

Cyber protection should also be taken into account in changes of the ICT organisation

Changes in the central government ICT organisation have influenced the cyber protection arrangements. Administrative and practical cyber protection actions have been centralised to Valtori, but the startup phase of Valtori was longer than planned and difficulties in retention of the original level of cyber protection arrangements were encountered during the startup phase. Development of the centralised cyber protection in Valtori has proven difficult. There have been deficiencies in the assessment of the adequacy of the practical cyber protection procedures and the implementation of new arrangements.

Operational situational awareness on cyber security should be improved

The situational awareness on cyber protection available to the authorities supports the arrangement of cyber protection. The Cyber Security Centre maintains nation-wide situational awareness on cyber security. With the help of the situational awareness provided by the Cyber Security Centre, authorities can correct information security vulnerabilities in their software, as well as prepare for and react to ongoing cyber security violations.

The more comprehensive the situational awareness, the better it will serve the arrangement of cyber protection. At present, there is no obligation to report cyber security violations to the Cyber Security Centre. If central government organisations were obligated to report cyber security violations, situational awareness would improve. Another measure that would improve situational awareness would be increasing the coverage of centralised cyber security violation detection methods.

Recommendations of the National Audit Office

Recommendations of the National Audit Office:

1. The Ministry of Finance must determine and implement an extensive operational control and management model in case of cyber security incidents in central government ICT services.
2. The Ministry of Finance must study how cyber protection of services should be taken into account in the funding of services throughout their lifecycle.
3. Valtori must improve the implementation, assessment and development of cyber protection procedures and the detection of cyber security violations.
4. The Ministry of Finance must improve the operative situational awareness that serves cyber protection by creating instructions for the authorities on the reporting of cyber security violations to the Cyber Security Centre.