about: [redacted] intel

European Voices on Surveillance

Finnish intelligence overseers' right of access supersedes Originator Control

23. October 2023

The NATO Information Security Treaty was brought into force in Finland on 23 August 2023, roughly four months after Finland became a member of the Alliance. Because information is king, this treaty was the first to which Finland acceded among the NATO treaty package. This post discusses the risk that the Information Security Treaty might push classified information which has been exchanged between NATO intelligence bodies and Finnish intelligence authorities beyond the reach of Finnish intelligence oversight.

The security environment in Finland changed fundamentally when Russia launched its brutal war of aggression against Ukraine in February 2022. After the invasion, Finland reassessed its security situation and applied for NATO membership. Finland became a member of NATO on 4 April 2023, when Finland's instrument of accession was deposited with the US government.

The Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (from now on Information Security Treaty) is one of the six treaties to which Finland has committed to accede within 12 months of becoming a NATO member. The 1997 Information Security Treaty contains articles on the mutual protection and safeguarding of classified information applicable between the parties to the North Atlantic Treaty. The Foreign Affairs Committee of the Finnish Parliament has considered it important that the Information Security Treaty enters into force as soon as possible so that Finland can fully receive classified information from NATO and participate in the exchange of information between the members of the Alliance. The Information Security Treaty and the NATO Security Policy were brought into force in Finland by decree (923/2023) on 23 August 2023.

Originator control

From the outset, NATO documents are not subject to the principle of public access. On the contrary, NATO classified documents are subject to the specific provision of the Act on International Information Security Obligations (588/2004) on absolute secrecy. A starting point of the Information Security Treaty is that information will not be disclosed to third parties without the consent of the originator of the information (originator control, Orcon). Orcon's core purpose is to protect the original owner of the information – the originator – by guaranteeing the originator the right to decide on the classification and onward dissemination of the information. The purpose of the principle is to prevent a so-called Trojan horse situation, in other words a situation where the recipient redistributes information to a third

party that does not meet the security requirements of the original originator or where disclosure to such a third party is otherwise contrary to the interests of the originator.

Orcon is not without its challenges. One example is the risk of a loss of political control and accountability in the exercise of public power. Orcon, namely, emphasises the centralisation of information control and restrictions on access to it. What is the nature of this risk in the intelligence context in particular: Does the Information Security Treaty push classified information exchanged between NATO intelligence bodies and Finnish intelligence authorities beyond the reach of Finnish intelligence oversight?

NATO information exchange and Finnish intelligence oversight

Alliance collaboration in the field of intelligence takes mainly place in the Joint Intelligence and Security Division, which in turn serves the needs of the civilian and military intelligence committees. NATO members are represented on these committees by their civilian and military intelligence services. The Finnish Security and Intelligence Service participate in the work of the NATO Civilian Intelligence Committee and the military intelligence authorities (the Defence Command Intelligence Division and the Finnish Defence Intelligence Agency) in the operation of the NATO Military Intelligence Committee.

The two main watchdogs of intelligence operations in Finland are the Intelligence Oversight Committee of Parliament and the Intelligence Ombudsman. The Committee exercises parliamentary control over intelligence activities whereas the Ombudsman supervises the legality of such activities. In practical terms, ensuring that the disclosure, reception, storage and destruction of information complies with the provisions of the Finnish Intelligence and Data Processing Acts, and the Information Security Treaty falls to the Intelligence Ombudsman given his legal role. The Intelligence Oversight Committee, given its parliamentary viewpoint, is concerned of broader issues, such as the role and policy of the Finnish intelligence authorities in the Alliance and the resourcing needs for NATO information exchange.

Access to information by overseers

The Finnish Security and Intelligence Service and the military intelligence authorities do provide, on their own initiative, both the Intelligence Ombudsman and the Intelligence Oversight Committee with the information they require on intelligence activities. The Ombudsman and the Committee also have equally extensive access rights to all intelligence-related information. These rights of access do not depend on the secrecy of the information or documents but extend to all levels of classification. It is also within the exclusive competence of the here mentioned overseers to assess what information is necessary for the purpose at hand. The Finnish intelligence overseers' access rights are among the most extensive in a European comparison.

In return for strong access rights, the officials of the overseers are subject to extensive security clearance vettings. These officials are also bound by the obligation of secrecy and confidentiality: classified documents may not be disclosed or divulged to third parties and the confidentiality also covers non-recorded information, such as conversations intended to be private. The balance between these rights and obligations is a constant one. For example, in a report adopted in January 2023, the Intelligence Oversight Committee has encouraged the Intelligence Ombudsman to increase the informative nature of the annual report in terms of

supervisory findings and observations. In the future, carefully considered intelligence activity statistics could be compiled and published by the Ombudsman.

Conclusions

The Council of Europe's Commissioner for Human Rights has long called for ensuring that the Orcon does not restrict the overseers' access to information. The German Constitutional Court has ruled along the same lines that even if the government and the intelligence service do remain bound by the assurances they have given, the bodies conducting legal oversight must no longer be considered "third parties".

The preparatory works to the Act on the Oversight of Intelligence Gathering (121/2019) explicitly states that a prohibition on the disclosure or use of information by another state authority does not restrict the Intelligence Ombudsman's right of access to information. The same conclusion applies to a prohibition on disclosure or use of information imposed by an international organisation. Consequently, the Intelligence Ombudsman has access to all material relating to the Finnish intelligence authorities' cooperation with NATO in order to carry out his duties. If the Orcon cannot be implemented simultaneously with the overseers' right of access to information, the collision will be resolved in favour of the overseers' superior right.



Mikael Lohse is Chief Specialist and Deputy Intelligence Ombudsman at the Office of the Intelligence Ombudsman in Finland. He is an Adjunct Professor of Legal Informatics and Intelligence Studies.