# Summary

This thesis investigates risk assessment and standardization by standard-setting organizations (SSOs), key governing practices in many societies today. It does so by studying the development of a security risk assessment approach into a Norwegian standard by the SSO Standards Norway (SN 5832:14). The first part investigates the institutionalisation of the standard as a policy process, while the second part investigates sensemaking by security professionals on questions of security risk assessment. The thesis asks how the establishment of the security risk assessment approach as a Norwegian standard can be accounted for.

The study is exploratory, and takes an abductive, puzzle-driven approach. It combines data from 40 interviews with document analysis and fieldwork on five courses in risk assessment, security management, and standardization.

The first part of the study investigates the standardization process as a policy process, as presented in article 1. The security risk assessment approach (labelled the three-factor approach or 3FA) is seen as a policy, and the study follows the 3FA's "journey" from one institutional context to the next, utilizing a within-case, longitudinal, comparative case study design. The process had three phases – it started within government agencies, moved to the jurisdiction of the SSO, and lastly consisted of the 3FA being debated by security and risk professionals.

The investigation of the standardization process utilises, but also develops, the multiple streams approach (MSA) originally developed by Kingdon. It contributes theoretically, by incorporating two sets of institutions – formal rules and knowledge – into the MSA. Both policy entrepreneurs and the institutional context are important for the institutionalization of the 3FA. Special attention is given to the characteristics of SSO standardization and its many ambiguities. The concept of "institutional deficit" is introduced, describing a potential mismatch between SSOs producing policy in a government-like institution, but where SSOs are not structured such that they manage to take responsibility for policies in a government-like way.

The second part investigates security professionals' sensemaking on risk assessment in a security context, utilizing methods from qualitative interpretive traditions. Article 2

investigates understandings of probability's role, and article 3 the role of risk assessment in protective security management.

This part of the thesis draws on Michael Power's risk governance theory as well as security theory. It builds on a little-utilized part of Power's theory, namely his development of three ideal models of risk management logics. The thesis develops these logics into four: risk management as anticipation, optimization, governance, and protection. The theorizing makes it possible to highlight three findings from the second part of the study.

First, there is a perceived tension between risk management's aim at optimization and the goal of protection. Probability plays a key role in the former but is a potential "threat" to the latter and vice versa; precautionary practices embedded in protection are at odds with optimizing resources.

Second, probability has two roles in the expression of risk, that is, anticipating the future and moderating the risk. Those arguing against expressing security risks through probability pay attention to the former (epistemic uncertainty). Those arguing against the 3FA pay attention to probability's moderating role, concerned that downplaying probability leads to overinvestment in low-probability risks.

Third, the thesis finds a perceived inconsistency across time between what is expected before and after an incident. Before, there is an expectation of analytical conduct and optimization, whereas afterwards, they expect a judgement of failure to protect, with blame as a potential outcome.

In summary, both the characteristics of the policy process and security professionals' sensemaking must be taken into account. Conceived of exclusively as a policy process, ideas and sensemaking play a modest role. However, investigating sensemaking by security professionals provides nuance to this conclusion. The 3FA reflects security professionals' sensemaking, where the tension between protection and risk optimization becomes evident. Probability makes risk "risky," and downplaying probability moves risk assessment in the direction of precaution and security. Hence, although the policy process was pivotal for the development of the standard, the 3FA also reflects struggles to combine contradictory risk logics in protective security management.