SCANDINAVIAN JOURNAL OF
MILITARY STUDIES

Lohse, M. (2020). The Intelligence Process in Finland.
Scandinavian Journal of Military Studies, 3(1),
pp. 68–79. DOI: https://doi.org/10.31374/sjms.55

PRACTICE-ORIENTED ARTICLE

The Intelligence Process in Finland

Mikael Lohse
Ministry of the Interior, FI
mikael.lohse@icloud.com

Civilian and Military Intelligence Acts entered into force in Finland on 1 June 2019. With the Finnish Security and Intelligence Service and the Finnish Defence Intelligence Agency securing new statutory powers to collect and use information on both domestic and international threats to Finland's national defence and security, these authorities have been transformed into combined domestic security and foreign intelligence services. The intelligence reform represents the most profound change ever made in the Finnish security sector, and it will have a major impact on the work of Finnish intelligence authorities in the years to come. How then is the Finnish intelligence organised as a process? This article aims to distinguish norms regulating the intelligence process from the vast intelligence legislation, and to organise this legal substance into four stages: (1) steering, (2) collection, (3) processing and analysis, and (4) sharing. The second objective is to identify areas of development in the intelligence process and suggest law and policy recommendations for the future.

Keywords: Military intelligence; Civilian intelligence; National security; National defence; Foreign and security policy

Introduction

Civilian and Military Intelligence Acts entered into force in Finland on 1 June 2019, at a time when a century had passed since the emergence of independent Finnish military intelligence and 70 years after the establishment of the Finnish Security Police, nowadays known as the Finnish Security and Intelligence Service (FSIS). With the FSIS and Finnish Defence Intelligence Agency (FDIA) securing new statutory powers to collect and use information on both domestic and international threats to Finland's national defence and security, these authorities have been transformed into combined domestic security and foreign intelligence services. The intelligence reform represents the most profound change ever made in the Finnish security sector, and it will have a major impact on the work of Finnish intelligence authorities in the years to come.

Intelligence may be understood as information, as the organisation that processes it, as the practices of such an organisation, as a set of missions, as risk shifting, or as a process (Kent 1949: 7–23; Warner 2008: 16–32; Johnson 2010: 7–27; Lowenthal 2017: 73–90). The understanding chosen here is intelligence as a process where intelligence is considered to be some type of product or activity for the purpose of supporting the decisions by civilian and military leaders (Bang 2017: 7). The intelligence process is a continuum of stages that begins by specifying the client's – such as the Prime Minister's or the military commander's – information needs and ends when the intelligence authority reports to the client. This means that any description of the intelligence process will be rooted in the interaction between the two parties to intelligence: the intelligence client and the intelligence authority.

There is an abundance of different 'intelligence cycles'. Most of them include four stages: steering/direction, collection, processing/analysis, and dissemination. This is in accordance with the general view of the stages involved in the intelligence process as established in Denmark, Norway, Sweden, and Finland (PET 2017: 25; NOU 2016: 75; SÄPO 2018; FSIS 2018: 13). This view also has its detractors. For example, it has been argued that in practice, the client hardly ever provides steering with respect to the focus of collection, that the collection and analysis of information are best managed in tandem, and that numerous successive processes may be required in order to discharge intelligence tasking. In other words, the view has been criticised for failing to reflect the practicalities of real intelligence operations. It has also been argued that

clients are not even expecting intelligence that supports any genuine decision-making process, but are just seeking justification for pursuing the policies that have already been decided (Hulnick 2006: 959– 979). The criticism is, however, not a reason for abandoning the view presented here. As with all models, it should be understood as a simplification and a general guideline as to how to proceed.

Hence, *the first objective* of this article is to distinguish norms regulating the intelligence process from the vast intelligence legislation, and to organise this legal substance into four stages:

1. Steering
2. Collection
3. Processing and analysis
4. Sharing (see **Figure 1**).

The intelligence authority is responsible for the intelligence implementation stages (2–4), while the intelligence client must provide active steering and feedback (1) to ensure that the collection focuses on the principal information requirements, and that the end product is fit for purpose (Lohse & Viitanen 2019: 96). Albeit this macro look of the stages of the intelligence process is shared by all Nordic countries, the details within each of these stages vary from country to country. The aim of this article is, among other things, to shed light on some of these particulars, i.e. the Finnish model on intelligence process. *The second objective* is to identify areas of development in the intelligence process and suggest law and policy recommendations for the future.

The body of the article follows the four stages of the intelligence process: steering, collection, processing and analysis, and sharing. The article ends with law and policy recommendations for improvements of the legal set-up and practices regarding the intelligence process in Finland.

Steering

Every state has interests of national security and international relations to defend. The most pressing of these interests – sovereignty of the state and indivisibility of its territory, a democratic form of government, social order and inviolability of legislative, governmental, and judicial powers – are subject to threats of a military or similarly serious nature, such as:

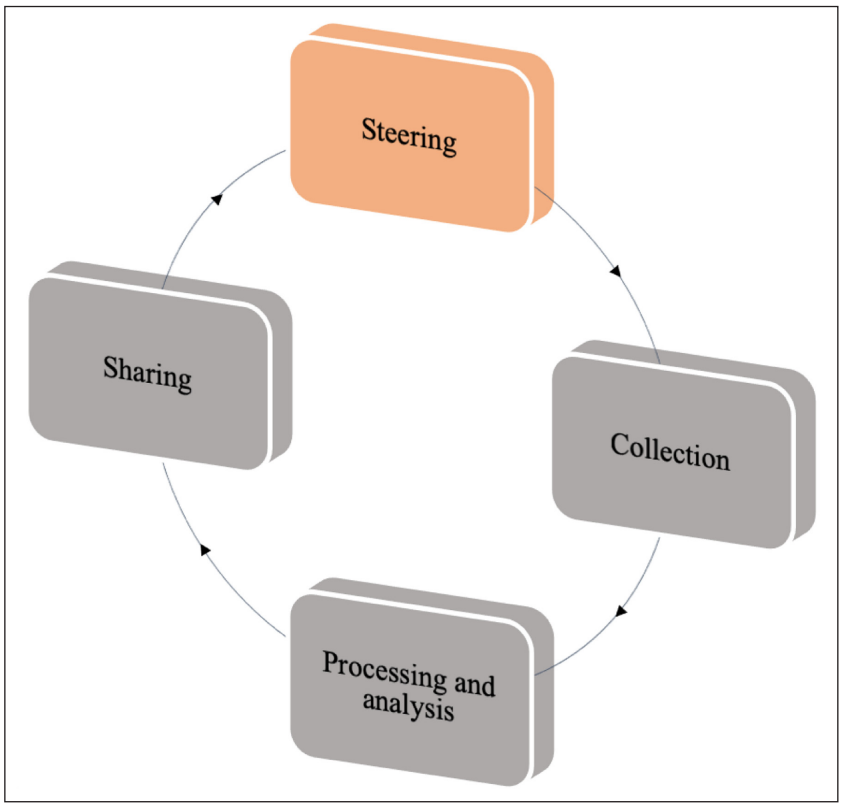

Figure 1: The four stages of the intelligence process.

- The operation and operational preparation of foreign armed forces and equivalent organised forces
- Terrorism
- Intelligence operations of foreign powers
- The design, manufacture, distribution and use of weapons of mass destruction
- A crisis that seriously jeopardises international peace and security
- Activities that seriously compromise the security of international crisis management operations
- Activities that seriously threaten the national defence of Finland
- Activities that seriously jeopardise the vital functions of society

Threats nevertheless evolve over time and therefore, regular reassessment is required concerning which national security interests are considered most vital at any time, which threats are believed to target those interests, and the order of gravity that should be assigned to these threats. Steering of intelligence is essentially about preparing for and evaluating these issues and about the associated political decision-making process.

Intelligence priorities

Finland's key security interests and the threats affecting them are assessed and evaluated as part of the national foreign and security policy, meaning that deliberation and policymaking in this area fall within the purview of the President of the Republic and of the government under sections 93.1 and 67 of the Constitution of Finland.[1] A special forum already exists for meetings of this kind: the joint meeting of the Foreign and Security Policy Committee and the President of the Republic (TP- UTVA). Section 13.1 of the Military Intelligence Act[2] specifically provides that TP-UTVA preliminarily prepares priorities with respect to military intelligence targets. The intelligence priorities of the FSIS must be prepared at the same meeting. In contrast to military intelligence, no further provisions governing this procedure under section 10.1 of the Police Administration Act[3] were considered necessary (Prop 346/2014: 9).

Either the President of the Republic or the Prime Minister may convene a joint meeting of TP- UTVA, as provided in section 24 of the Government Act.[4] TP-UTVA seeks to hold one meeting annually in order to formulate the priorities for civilian and military intelligence. The Ministry of the Interior and the Ministry of Defence prepare these priorities in advance, for consideration by TP- UTVA. The FSIS and FDIA in turn collate and submit inputs on intelligence priorities to serve as the basis for this preparatory work at the said ministries, meaning that these ministries form a key link in the preparatory chain between TP-UTVA and the intelligence authorities. This status assigns a gatekeeper role to the Ministry of the Interior and the Ministry of Defence, enabling them to decide which intelligence authority priority inputs are selected for the TP-UTVA agenda.

Intelligence priorities refer to significant medium term (1–3 year) development policies of foreign and security policy importance to Finland, for which more detailed information is required to substantiate top-level government decisions. The intelligence priorities may naturally be revised at TP-UTVA more frequently than once a year if unexpected new events or trends are observed in the national security environment (Prop 1/2018: 33). The priorities may concern such aspects as a certain area or theme or some overall threat scenario that combines them. On the other hand, concrete and precisely specified activity that seriously threatens national security will not give cause for recording as priorities, as it is the job of the intelligence authorities. The same applies to the choice of intelligence gathering methods used for collecting information on some phenomenon, event or trend. These and other operational issues are also solely for the intelligence authority to decide. The administrative culture of Finland generally abhors any interference by political policymakers in the process of making operational decisions (Prop 203/2017: 120).

While TP-UTVA and the Ministry of Defence steer military intelligence, the Defence Command manages military intelligence in compliance with the assigned priorities for military intelligence (section 13.3 of the Military Intelligence Act). The Director of the FSIS in turn manages civilian intelligence within the constraints of the authority's assigned intelligence priorities. In practice, the Defence Command is responsible for managing military intelligence by issuing tasks to the intelligence authorities on the basis of requests for information.

Information requests

Only military intelligence involves a statutory guidance format based on information requests. Section 14 of the Military Intelligence Act provides that the President of the Republic, the Prime Minister's Office, the Ministry for Foreign Affairs and the Ministry of Defence may submit information requests to the Defence

Command, complying with the priorities concerning targets of military intelligence. This means that information requests must be tied to the targets of military intelligence referred to in section 4 of the Military Intelligence Act which have been selected as current military intelligence priorities. The party requesting information must accordingly specify with optimal precision not just the information requirement, but also how this requirement relates to the military intelligence priorities that have been prepared at TP-UTVA and issued by the Ministry of Defence.

Only the designated principal clients of military intelligence, meaning the leadership of Finland's foreign and security policy, are eligible to submit requests for information. These provisions seek to ensure that the administration subordinate to the President of the Republic and the government will not employ information requests as *ultra vires* ('beyond the powers') means of obtaining intelligence information, and that information requests will be adequately important.

Based on a request for information, the Chief of Intelligence of the Defence Command issues an intelligence assignment to the military intelligence authority, which in turn decides the most expedient way of discharging the task. After collecting, processing, and analysing the information, the military intelligence authority prepares a report pursuant to the request for information which the Defence Command then shares with the party that submitted the request (Prop 203/2017: 209).

Coordinating intelligence gathering

Section 58 of chapter 5 a of the Police Act[5] and section 15 of the Military Intelligence Act contain congruent provisions governing the coordination of intelligence gathering. These provisions stipulate that matters of civilian and military intelligence – insofar as they are considered to have an impact on foreign and security policy – will be preliminarily prepared and coordinated between the President of the Republic, the Prime Minister's Office, the Ministry for Foreign Affairs, the Ministry of Defence, the Ministry of the Interior, and, if necessary, between other ministries and authorities (Rep 9/2018: 36).

The procedural purpose of coordination is to give the representatives of various administrative sectors linked to intelligence gathering a basis for submitting foreign and security policy views and sharing a jointly formulated vision with policymakers, parties working in foreign intelligence, and others whose work is affected by the policies concerned (Prop 202/2017: 230; Prop 203/2017: 210; Rep 6/2018: 4). The coordination policies for intelligence gathering are one of the most important forms of client steering issued to the intelligence authorities. Their substantive content covers intelligence priorities and information requests with foreign and security policy implications.

The key reason for dividing responsibilities on the basis of coordination is to ensure that the resources of civilian and military intelligence are allocated expediently, and that intelligence gathering, particularly when conducted abroad, do not give rise to duplication of collection by civilian and military intelligence authorities with the attendant inadvertent risks. The arguments concerning division of responsibilities will not always be altruistic in this procedure. Questions of priorities and the division of responsibilities in intelligence work also have underlying implications for the resource allocation and the justification of additional operating expenses (Lowenthal 2017: 77). An observation by the Parliamentary Committee for Administration, for example, that 'the threat priority has shifted to the domain of internal security in the conventional foreign and security policy sector', might be taken as a hint that the importance of civilian intelligence targets would somehow essentially outweigh that of military intelligence targets where the tendency is to focus on external threats (Rep 36/2018: 89).

In addition to intelligence priorities, the coordination procedure handles information requests with foreign and security policy implications. This procedure focuses on assessing whether acting on an information request could damage Finland's international relations or cause other foreign policy problems. Circumstances involving foreign and security policy sensitivities are precisely what has been stressed when insisting that the threshold for submitting intelligence gathering to the coordination process must remain low (Rep 6/2018: 4). The government proposal on the Military Intelligence Act maintains that coordination could also involve a review of the competencies applied when implementing requests for information in each situation (Prop 203/2017: 210). While such reviews are justified from the perspective of risk management, it should also be stressed that both the decision to use a particular intelligence gathering method and other operational decisions must remain the sole responsibility of the intelligence authority.

Figure 2 shows the steering and management of intelligence in the form of assigning intelligence priorities and presenting requests for information in accordance with those priorities, and also shows it as a process that reconciles these contributing factors.

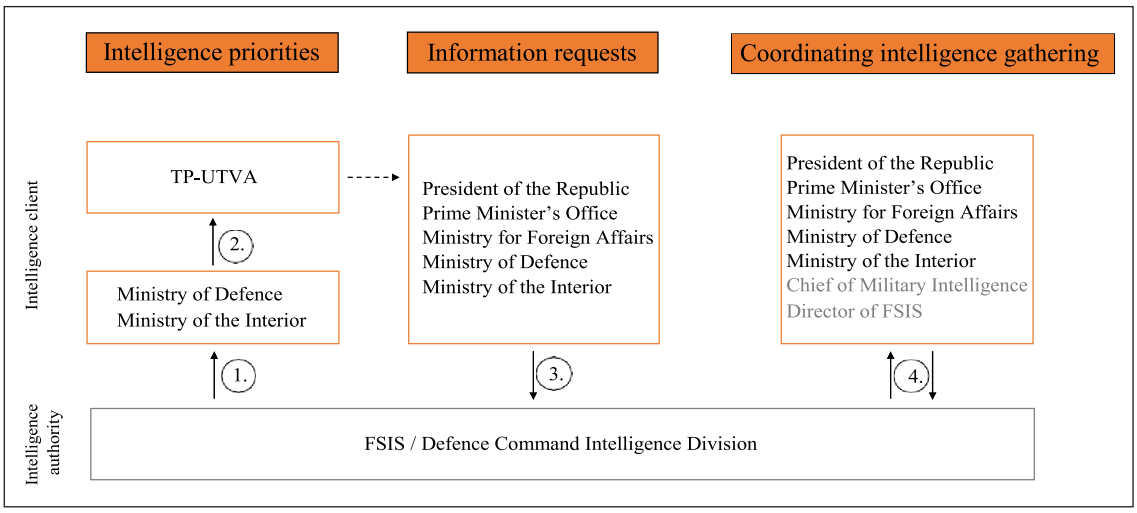

Figure 2: The steering and management of intelligence.

Collection

Information gathering by the intelligence authorities may be understood in general as a process of collecting data that targets both open sources and non-public information. The gathering seeks to produce early stage information that will enable contingency planning and influencing in relation to various threats and opportunities (MoD 2015: 15). The threat determines defensive intelligence, referring to gathering information about threats to national security interests. The logic of offensive intelligence is in turn based on taking opportunities. This proactive intelligence may, for example, help to promote the political status of a country internationally or the prospects of its business community in relation to foreign competitors (Rep 36/2018: 24). Civilian and military intelligence in Finland are based on threats. Information gathering by the FSIS and FDIA is accordingly already defensive within its own normative terms of reference.

Assessed from the perspective of the intelligence process, information collection is the stage following the political steering of intelligence. The intelligence authorities obtain information in response to a request for information in accordance with the assigned priorities. This is a directed and systematic activity that the intelligence authorities remain solely responsible for discharging in practice (Lohse, Meriniemi & Honkanen 2019: 16).

Intelligence tasking

The Defence Command is responsible for managing military intelligence by issuing detailed tasks to the FDIA on the basis of requests for information. While there is an established format for issuing military intelligence tasks, no practice arising from civilian intelligence assignments has emerged to date (Rep 16/2018: 8). It would appear that managing of civilian intelligence will continue operating without concrete intelligence tasks issued by the leadership of the FSIS, given that the entire concept of intelligence tasking is absent from the statutes governing civilian intelligence. The difference in statutory solutions nevertheless does not necessarily reflect any fundamental disparity between civilian and military intelligence with respect to the manner in which they convert the client's information requirements into a task, but rather a difference in the organisational level at which this occurs. Even FSIS procedures are naturally subject to practicalities structured at operating unit level in terms of objectives and means, i.e. by intelligence questions and intelligence gathering methods.

Point 9 of section 10 of the Military Intelligence Act defines intelligence tasking as an assignment given by the Chief of Intelligence of the Defence Command – based either on intelligence priorities prepared by TP-UTVA or on a request for information – to the FDIA to obtain information on a target of military intelligence. The intelligence tasking will specify the intelligence priorities, for example, the information requirements and the thematic or regional target of the intelligence. More detailed specifications relating to such aspects as individuals, groups or particular spaces or places will by contrast remain the business of the FDIA that discharges the intelligence task. The Defence Command will plan and design the intelligence tasking and will also be involved in analysing the information obtained by the FDIA and reporting it to the client (Prop 203/2017: 198–99).

The provision governing intelligence tasking is important in many respects. In the first place, referring to a task highlights the result-oriented character of intelligence. This means that some outcome, such as situation awareness, will follow the concluded process, and that reports of interim findings are also expected from any sustained, but not yet completed task. It is also important that intelligence tasking ties the use of intelligence gathering methods to the task concerned. Finally, the definition of intelligence tasking relates to supervision of intelligence. The Parliamentary Committee for Defence notes that a more precise specification of intelligence tasking could assist evaluations of the conditions for using intelligence gathering methods in civilian intelligence and thereby streamline oversight of intelligence (Rep 16/2018: 8).

Use of intelligence gathering methods

The manner of implementing intelligence gathering and the methods used will vary according to the type of foreign military activities or other threats to national security that are targeted. For example, we cannot expect to gather useful intelligence on a cyber threat, meaning a threat to the security of an electronic operating environment, through imagery intelligence using electro-optics or radar. Network traffic intelligence is much better suited for uncovering this threat (Lowenthal 2017: 80). Civilian and military intelligence apply a wide range of intelligence gathering methods, so specialist expertise is required to decide the method or combination of methods that are most appropriate in each intelligence operation. This decision-making process will be guided by the general and special conditions for using intelligence gathering methods and by the general principles of intelligence, including the consequent requirement to comply with the principle of proportionality (Lohse & Viitanen 2019: 108).

The intelligence gathering methods can be divided into three groups according to the level on which a decision regarding their use is made. Deployment of the intelligence gathering methods (12 pcs) which represent the deepest infringement on the fundamental and human rights of an individual are authorised by district judges. The Director of the FSIS and the Chief of the Intelligence of the Defence Command are entitled to decide on the use of intelligence gathering methods (5 pcs) which typically involve safeguarding intelligence officials and covert human intelligence sources or foreign and security policy sensitivities. The use of the remaining methods (7 pcs) are decided by the brass of the FSIS and FDIA – a designated official who is specialised in the use of intelligence gathering methods and run intelligence operations (see **Figure 3**).

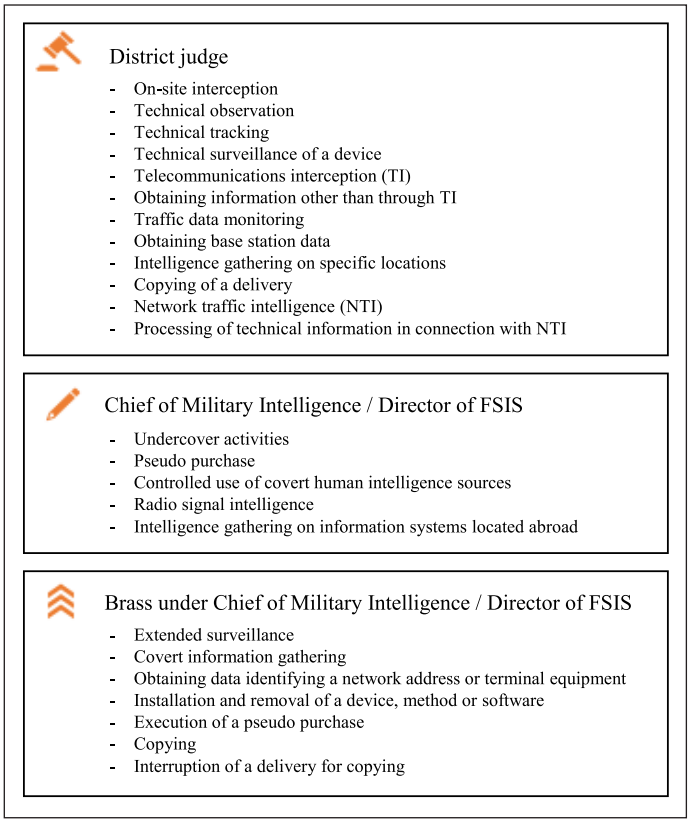

Figure 3: Grouping of competence-based methods according to decision-making level.

Decisions on foreign intelligence nevertheless form an exception to the foregoing decision-making level. Under section 39 of chapter 5 a of the Police Act, decisions on civilian intelligence operations and the use of intelligence gathering methods outside Finland are made by the Director of the FSIS. Accordingly, decisions on military intelligence overseas fall within the competence of the Chief of Intelligence of the Defence Command (section 64 of Military Intelligence Act). This means that in the context of foreign intelligence, the Director/Chief in question is empowered to decide on the use of intelligence gathering methods that would require a court warrant if used in Finland.

The methods of civilian and military intelligence gathering in Finland can be grouped into:

- Human Intelligence (HUMINT)
- Telecommunications Intelligence (t-COMINT)
- Signals Intelligence (SIGINT)
- Methods based on other competences
- Methods based on customary law

Human intelligence refers to information gathering based on personal interaction or on personal observations of an individual or other intelligence target. Information gathering in human intelligence consequently targets individuals and the documents and electronic records to which they have access (Prop 203/2017: 219). Human intelligence in Finland includes surveillance and extended surveillance, covert information gathering, undercover activities, pseudo purchase, use of covert human intelligence sources, and controlled use of covert human intelligence sources.

Telecommunications interception (wiretapping) largely occurs on public communications networks, but also refers to eavesdropping on communications transmitted over a satellite network. An example of how data may be obtained other than through telecommunications interception is when the message available under wiretapping powers has been lost, but can still be retrieved by technical means from a telecommunications operator or a corporate subscriber. Traffic data monitoring refers to acquiring identification data that indicates the parties to a communication. Obtaining access to base station data denotes the collection of data concerning those terminal end devices and network addresses (i.e. mobile phones) that are, were, or will be located within the range of a particular base station. These methods all relate to the notions of a communications network and a telecommunications operator, which justifies talking about intelligence in telecommunications networks or telecommunications intelligence, or (t-COMINT) for short.

Signals intelligence is information gathering that targets electronic signals (MoD 2015: 16). Network traffic intelligence refers in particular to technical information gathering targeted at network traffic in a communications network crossing the Finnish international border based on automated screening of network traffic and processing of the obtained information for the purpose of performing intelligence task (Lohse, Meriniemi & Honkanen 2019: 99). Radio signals intelligence is information gathering that targets radiofrequency electromagnetic transmissions, i.e. radio waves.

Examples of intelligence gathering methods based on other competencies are on-site interception, technical observation, technical tracking, technical surveillance of a device, intelligence gathering on information systems located abroad and on specific locations, copying, copying of a delivery, and interruption of a delivery for copying.

The intelligence methods based on customary law are short-term surveillance, open source intelligence (OSINT), imagery intelligence (IMINT), and geospatial intelligence (GEOINT). Surveillance is regarded as an ancillary concept for defining extended surveillance and as a method of information gathering that is permitted in customary law (Helminen et al. 2014: 1152). Open source intelligence refers to media monitoring and obtaining information from other public sources, including official records, television and radio broadcasts, social media, statistics and maps. Imagery intelligence is the compilation of a local status report, for example using radar imaging. Geospatial intelligence seeks to describe, evaluate, and present particular targets, areas, natural phenomena and conditions using geographic data and image materials, situational information, and statistical materials (Prop 203/2017: 218–19).

Processing and analysis

In the third stage of the intelligence process, the collected intelligence data must be processed – separating the signals from the noise – and converted into usable information (Johnson 2010: 19–20). Processing information is a core function of the FSIS and FDIA, supporting the intelligence analysis that in turn is the work stage generating the greatest added value in the final product of intelligence. Analysis is at the heart

and soul of the intelligence process. As analysis is based on human cognitive abilities, it is also one of the most difficult factors to replace in intelligence (Lowenthal 2017: 163 and 173).

Processing and information systems

Processing is about refining 'raw' intelligence, such as telephone intercepts and data obtained through technical tracking, into a readable format. Information processing includes filtering, classifying, encoding, visualising, or otherwise handling information to enable the combination and comparison of materials, for example with data held in the information systems of the intelligence authorities. Thus, encoding may use dichotomous (1/0) variables to evaluate a property or item of information appearing in the material, enabling procedures such as mining qualitative materials in spoken language using quantitative research methods.

Information processing is a largely automated activity centred on an information system. The FSIS relies on its own information system, whereas the FDIA uses the Military Intelligence Register. Section 48.1 of the Act on the Processing of Personal Data by the Police provides that FSIS in its information system may process personal data that is necessary for safeguarding national security. Such data includes, but is not limited to, the personal ID number and date of birth, sound and image recordings, details of citizenship and family relations, and identification data that may be associated with a legal or natural person. The said information will be collected by means of intelligence gathering methods and through information exchanges with domestic and foreign partners (Prop 202/2017: 264). Under section 14 of the Act on the Processing of Personal Data in the Defence Forces, various details and identification data that may be associated with a natural person or with a legal entity, such as IP addresses, telephone numbers, and communication transmission data may be recorded in the Military Intelligence Register (Prop 13/2018: 37).

Some general observations on analysis

The task of analysis is to bring meaning and insight to the intelligence data that has been collected and processed. The analysis of information is an activity that actively seeks to identify, parse, and express the threats and opportunities of the national security environment (MoD 2015: 15). The intelligence authorities use multi-source analysis in this work, relying on their own information collection, on open sources, and on information obtained from domestic and foreign partners. This analysis is basically a matter of quality assurance and improving the reliability of analysis – with the use of multiple sources reducing the risk of drawing conclusions that subsequently may prove incorrect. Whether relying on a single source (Single-Int), on multiple sources (Multi-Int), or on all sources (All-Source Analysis), the crucial point for the intelligence client is to understand the kind of source materials base on which the final intelligence report relies, and the kind of additional information that use of a richer source might have brought to the analysis.

The analysis of information can be divided into operational and strategic analysis. Operational analysis focuses on topical events and, under normal conditions, its end products are the primary focus of intelligence clients (Lowenthal 2017: 82). Operational intelligence attracts all the attention in conflict or crisis situations, where decision-makers are required to make tactical decisions. One of the principal functions of operational analysis in military intelligence is to issue indications and warnings (I&W), typically under circumstances where this is warranted by the activities of foreign armed forces. The operations of armed forces generally exhibit regularities, for example in monitoring directions pertaining to deployment and movements and to the volume of communications. If changes occur in these continually monitored aspects that suggest offensive measures or otherwise give cause for alarm, then the early warning will enable a decision to be made, such as heightening of readiness or mobilisation of forces. Admittedly, detecting such changes is easier said than done, as the communications of armed forces tend to be strongly encrypted and the true nature of their operations may have been disguised. Strategic analysis assesses foreign military activities and phenomena that threaten national security in the longer term and with a view to anticipating associated future trends.

The functions of analysis

Timeliness is important in sharing information (MoI 2017: 19). Particularly in acute situations and emergencies, it is more important to be able to ensure distribution to the intelligence client of analysed information – even though such information may stem from just a few sources – than it is to wait for missing data with the associated refinement measures such as type assignment, temporal rekeying, classification, cross-tabulation or calculation of various key figures. The hallmarks of good analysis also include added value in the final intelligence product and readability for the intelligence client. To achieve these objectives, an intelligence

report should respond to the individual need for information to the extent and to the degree of accuracy that the client is seeking or is believed to desire. Responding to the client's information requirements must nevertheless never result in compromising the objectivity of the analysis or politicising the analysis, meaning practices whereby opportunism supplants the pursuit of independence and impartiality with efforts to gratify the intelligence client by adapting the report according to the client's declared or presumed policy objectives.

The structure of a good report enables the reader to distinguish, where necessary, between what is known and what is not known. It should also indicate the reliability of sources, so that the intelligence client can assess the accuracy of the analysis and any factors that may challenge it. This corresponds to the provision in section 14.2 of the Act on the Processing of Personal Data in the Defence Forces concerning information in the Military Intelligence Register, applied at the stage of analysing and sharing information. This statute provides that an evaluation of the reliability of the information provider or source and of the accuracy of the information must be appended as necessary to personal data recorded in the register. Recording this kind of evaluation is particularly necessary if suspicions arise concerning the reliability of the information source or the accuracy of the information in an individual case (Prop 13/2018: 37–38).

It should also be stressed that intelligence information cannot be assumed to satisfy forensic standards of reliability in a court of law. Intelligence does not provide evidence, and it is hardly ever certain (Manget 2010: 190). Analysing information may be understood in terms of assembling a jigsaw puzzle or creating a pearl, indicating the fragmentary character of such information and the often tenacious and enduring nature of intelligence (Lowenthal 2017: 188). The outcome may be a conclusion shared by the intelligence community concerning a terrorist whose culpability is not substantiated by probable cause, and even less by grounds for a criminal conviction. This difference of outlook simply reflects the diverging ontological starting points of intelligence and law enforcement. There is no fundamental difficulty in such a disparity of concepts concerning reality, provided that:

1. Policies based on intelligence information do not address the issue of guilt, as this is solely a judicial matter, and
2. countermeasures initiated on the basis of intelligence information do not impinge on the personal liberty or other rights of those targeted by intelligence authorities without lawful grounds, for example based on the provisions of the Coercive Measures Act.[6]

Sharing

As part of the intelligence process, information sharing refers to transferring analysed information, often in the form of standardised output, from the intelligence authorities to their client. The international intelligence community commonly channels client reporting according to various product or release types, even organising reporting into specialised production lines (Lowenthal 2017: 84). The range of such products varies from daily topical reviews or digests to studies that may take up to a year to complete. Besides these standardised products, materials such as memoranda suited for unanticipated information requirements are also distributed to the client, especially if the intelligence authorities already have such material in a readily available form.

Regardless of the type of information release product chosen, certain common features may be discerned in reporting intelligence to clients. The first relates to the notion of time. The reporting deals with current affairs or future trends, as opposed to historical events. Another feature concerns quality assurance. Studies in particular, but also overviews, seek to include a peer review by colleagues working at the same level or in corresponding capacities as the author(s) of the product under evaluation. A third common feature concerns linking the range of products to processing of the same theme from varying perspectives and with varying degrees of precision. A multi-layered release strategy primarily responds to the various information requirements of clients and helps the intelligence authorities to distribute the product to those who need it.

With the exception of military intelligence monitoring, the parties involved in reporting are fairly free to negotiate the products that the intelligence authorities deliver to their client. Section 16.1 of the Military Intelligence Act requires the Ministry of Defence to submit a report of intelligence priorities to a joint meeting of the Foreign and Security Policy Committee and the President of the Republic on an annual basis, or more frequently if TP-UTVA so requests. The Ministry of Defence may also issue the said report on its own initiative before the annual reporting deadline when required on account of information obtained on targets of military intelligence, relating to such questions as foreign policy or Finland's relations with another state or international organisation (Prop 203/2017: 211). The report issued to TP-UTVA will contain the

results of an intelligence task issued pursuant to military intelligence priorities and to any specifying request for information. The report may evaluate such aspects as the security situation of Finland and factors having a bearing on it, and how circumstances that are relevant to national security seem to be evolving.

In the same manner, the Defence Command is required to issue an annual report to the Ministry of Defence concerning military intelligence, its quality and scope, and its targeting. The said report must also be submitted without delay whenever the Ministry of Defence so requests (section 16.2 of the Military Intelligence Act). This provision ensures that the Ministry of Defence is regularly informed of military intelligence to substantiate its decisions on steering and oversight, and for the purposes of monitoring performance.

Conclusions

The activity of the civilian intelligence services is commonly more transparent than that of military intelligence services. It is therefore somewhat surprising that the statutory steering of the FDIA is more comprehensive and detailed than the legal steering of the FSIS. In contrast to military intelligence legislation, laws governing civilian intelligence do not involve a specific provision on monitoring of intelligence. This difference has not gone unnoticed. The Parliamentary Audit Committee welcomed the introduction of an explicit statutory provision in the Military Intelligence Act concerning the procedure governing the monitoring of reports on intelligence priorities (Rep 4/2018: 3). Neither do the laws on civilian intelligence include the notion of intelligence tasking. The provision on intelligence tasking is important because referring to a task highlights the result-oriented character of intelligence and ties the use of intelligence gathering methods to the task at hand. This connection in turn is pivotal for the intelligence oversight because of its duty to scrutinise, among other things, that intelligence powers only be exercised for a purpose laid down in the law. To correct this inconsistency between civilian and military intelligence regulation, chapter 5 a of the Police Act should be amended to incorporate particular provisions on monitoring civilian intelligence and on civilian intelligence tasking.

Where necessary, the use of intelligence gathering methods must be coordinated to ensure the occupational safety of the officials working for the FSIS and FDIA and to prevent tactical and technical methods and plans used in covert intelligence gathering from being revealed (section 56.1 of chapter 5 a of the Police Act and section 19.1 of the Military Intelligence Act). Numerous public authorities, such as the National Bureau of Investigations (NBI) and the Customs and Finnish Border Guard, are entitled to deploy secret information gathering methods, so there is a risk of unintended duplication of information gathering by various operators. The drawbacks of triggering this risk under such circumstances may take the form of work-related accidents and information leakage of tactical and technical methods and plans. Therefore, it is important to ensure that security authorities engaged in covert intelligence gathering coordinate such operations in each case. It is thus strongly advisable that more detailed provisions on organising the coordination of covert intelligence gathering be issued by government decree, and that agreement on best practices regarding this coordination be made – at the very least – between the FSIS, FDIA, and NBI.

Notes

[1] The Constitution of Finland No. 731 of 1999, as amended by No. 817 of 2018.
[2] Act on Military Intelligence No. 590 of 2019.
[3] Police Administration Act No. 110 of 1992, as amended by No. 583 of 2019.
[4] Government Act No. 175 of 2003, as amended by No. 837 of 2017.
[5] Police Act No. 872 of 2011, as amended by No. 581 of 2019.
[6] Act on Coercive Measures No. 806 of 2011, as amended by No. 624/2019.

Competing Interests

The author has no competing interests to declare.

References

Bang, M. (2017). *Military Intelligence Analysis: Institutional Influence*. Helsinki: National Defence University Series 1: Research Publications No. 14.

FSIS. (2018). *Jubilee Year Book*. Retrieved from https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/77291_WWW_SUPO_Juhlakirja_70_2019_ENG.pdf?a10a73874125d788

Government. (2014). *Proposal No. 346 on amending the Police Administration Act and other associated acts*. Retrieved from https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_346+2014.pdf

Government. (2017). *Proposal No. 202 on Civilian Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_202+2017.pdf

Government. (2017). *Proposal No. 203 on Military Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_203+2017.pdf

Government. (2018). *Proposal No. 13 on Legislation on the Processing of Personal Data in the Defence Forces*. Retrieved from https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_13+2018.pdf

Helminen, K., Fredman, M., Kanerva, J., Tolvanen, M., & **Viitanen, M.** (2014). *Esitutkinta ja pakkokeinot*. Helsinki: Talentum.

Hulnick, A. S. (2006). What's wrong with the Intelligence Cycle. *Intelligence and National Security, 21*(6), 959–79. DOI: https://doi.org/10.1080/02684520601046291

Johnson, L. K. (2010). National Security Intelligence. In L. K. Johnson (Ed.), *The Oxford Handbook of National Security Intelligence* (pp. 3–32). Oxford: Oxford University Press. DOI: https://doi.org/10.1093/oxfordhb/9780195375886.003.0001

Kent, S. (1949). *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press.

Lohse, M., Meriniemi, M., & **Honkanen, K.** (2019). *Tiedustelumenetelmät*. Helsinki. Alma Talent.

Lohse, M., & **Viitanen, M.** (2019). *Johdatus tiedusteluun*. Helsinki: Alma Talent.

Lowenthal, M. M. (2017). *Intelligence: From Secrets to Policy. Seventh Edition*. Los Angeles: SAGE Publications.

Manget, F. F. (2010). Intelligence and Law Enforcement. In L. K. Johnson (Ed.), *The Oxford Handbook of National Security Intelligence* (pp. 189–211). Oxford: Oxford University Press. DOI: https://doi.org/10.1093/oxfordhb/9780195375886.003.0012

Ministry of Defence. (2015). *Guidelines for developing Finnish legislation on conducting intelligence* (Report of the Working Group). Retrieved from https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

Ministry of the Interior. (2017). *Development of guidance for civilian intelligence and the Finnish Security Intelligence Service in the administrative branch of the Ministry of the Interior* (Working group's report 16/2017). Retrieved from http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80032/Siviilitiedustelun%20ja%20suojelu poliisin%20ohjaus_NETTI.pdf?sequence=1&isAllowed=y

NOU. (2016). *Official Norwegian Reports No. 8. A Good Ally: Norway in Afghanistan 2001–2014*. Retrieved from https://www.regjeringen.no/contentassets/09faceca099c4b8bac85ca8495e12d2d/en-gb/pdfs/nou201620160008000engpdfs.pdf

Parliamentary Administration Committee. (2018). *Report No. 36 on Civilian Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_36+2018.pdf

Parliamentary Audit Committee. (2018). *Report No. 4 on Military Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/TrVL_4+2018.pdf

Parliamentary Defence Committee. (2018). *Report No. 9 on Military Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/PuVM_9+2018.pdf

Parliamentary Defence Committee. (2018). *Report No. 16 on Civilian Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PuVL_16+2018.pdf

Parliamentary Foreign Affairs Committee. (2018). *Report No. 6 on Military Intelligence Legislation*. Retrieved from https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/UaVL_6+2018.pdf

PET. (2017). Årlig redegørelse. Retrieved from https://www.pet.dk/~/media/Aarsberetninger/rligredegrelseforPET2017WEBpdf.ashx

SÄPO. (2018). *The Security Service's intelligence work in focus*. Retrieved from https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-11-26-the-security-services-intelligence-work-in-focus.html

Speaker's Council. (2018). *Proposal No. 1 on amending the work order of Parliament and provision 9 of the Act on Parliament Officials*. Retrieved from https://www.eduskunta.fi/FI/vaski/Lakialoite/Documents/PNE_1+2018.pdf

Warner, M. (2008). Intelligence as risk shifting. In P. Gill, S. Marrin, & M. Phythian, (Eds.), *Intelligence Theory. Key questions and debates* (pp. 16–32). London and New York: Routledge. DOI: https://doi.org/10.4324/9780203892992.ch2

How to cite this article: Lohse, M. (2020). The Intelligence Process in Finland. *Scandinavian Journal of Military Studies,* 3(1), pp. 68–79. DOI: https://doi.org/10.31374/sjms.55

Submitted: 29 October 2019 **Accepted:** 11 May 2020 **Published:** 19 June 2020

SCANDINAVIAN MILITARY STUDIES

Scandinavian Journal of Military Studies is a peer-reviewed open access journal published by Scandinavian Military Studies.

OPEN ACCESS