Intelligence Practices in High-Trust Societies

Scandinavian Exceptionalism?

Edited by Kira Vrist Rønn, Adam Diderichsen, Mia Hartmann, and Melanie Hartvigsen

First published 2025

ISBN: 978-1-032-61703-9 (hbk)
ISBN: 978-1-032-61639-1 (pbk)
ISBN: 978-1-032-61637-7 (ebk)

Chapter 9

Recruiting the Swedish Intelligence Professional

Sebastian Larsson

DOI: 10.4324/9781032616377-13

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

9 Recruiting the Swedish Intelligence Professional

Sebastian Larsson

Introduction

This chapter explores the transforming professional dispositions of signals intelligence agency workers. It does so by analysing recent recruitments to a Swedish intelligence agency which has been in a process of significant expansion in recent years. What can such recruitments reveal about contemporary signals intelligence practices in Sweden, Scandinavia, and beyond?

The public's perception of signals intelligence services changed drastically following whistle-blower Edward Snowden's revelations in 2013 of the extensive and intrusive surveillance practices of the NSA and its extended network of actors (MacAskill & Dance, 2013). These leaked documents revealed not only that the Scandinavian countries were part of this extended network but also that certain actors such as the Swedish signals intelligence agency – the National Defence Radio Establishment (*Försvarets Radioanstalt*; from hereon: FRA) – were deeply involved in its operations. For years, FRA had played a key part in enabling transatlantic digital surveillance, including data-sharing and joint hacking operations, pushing the limits of what was legally and technologically possible in this area (Larsson, 2022; Rensfeldt, 2013).

Despite the controversial nature of FRA's operations with the NSA, their mandate, capabilities, or authority did in fact not diminish after the Snowden revelations. Following the trend towards rearmament and increased defence spending in Sweden since around 2015, FRA has rather grown, and their practices become increasingly formalized. For instance, FRA's transnational surveillance and data-sharing activities have now been further inscribed into law, as has their capacity to cooperate with other domestic agencies on policing, counterterrorism, and cybersecurity issues.[1] This is not entirely surprising, however, as outcry over intelligence controversies often tends to lead to further legalization and formalization of intelligence work, rather than a blocking of the services' activities (Bigo et al., 2023). Sophie Duroy even argues that international law does less to restrict intelligence operations than to favour the national security interests of those states that comply with it (2023).

In recent years, FRA has also taken up a more visible and seemingly transparent position towards the public, e.g., by participating at trade shows and

DOI: 10.4324/9781032616377-13

university career events and by joining social media.[2] This suggests that the agency is aware of their still controversial status and are in a process of seeking to normalize themselves as “just another defence agency”, as a regular “9 to 5” in the security sector.[3] Of course, parallel with this normalization process, FRA also strives to maintain its status as an undeniably “special” place to work. Across their publications and social media posts, FRA makes it persistently clear that their job is also exceptional and “important”, that they deal with the most serious threats towards society and our way of life, and that they are ready to pre-empt them with the most advanced ways of listening in.[4] Hence, both normalcy and exceptionalism play a part in attracting people to the booming signals intelligence sector in Sweden, something which is directly necessary if they are to meet current and future recruitment demands. Indeed, in recent defence budgets, FRA is the third-largest defence agency (after the Swedish Armed Forces and the Swedish Defence Materiel Administration) with a share of SEK 1.9 billion in 2023, planned to increase to SEK 2.8 billion in 2025.[5] This makes it clear that signals intelligence is one of the most politically prioritized security practices in the country. In the following years, the agency will require not only new technologies and material acquisitions but also a large amount of new personnel.

This chapter focuses on the latter. Drawing on a rich collection of job advertisements as the main empirical material (detailed below), it analyses FRA’s ongoing recruitment process and finds that the agency targets not only future intelligence analysts with a security policy interest, but even more so the new generation of “tech talents” in areas like computer engineering, programming, data science, systems development, and information technology. Through the ad material, the different ideal types of professionals sought after for each agency branch can be mapped out, including candidates’ practical skills and experience as well as preferred personality types. This, I assume, will reveal key details about how FRA’s intelligence and surveillance practices are currently organized and carried out, something that is otherwise veiled by secrecy. At the same time, however, I acknowledge that job ads represent a constructed and to some extent curated story about the agency that its leadership wants to communicate to an external audience and niche part of the job market. Hence, the ad material will be treated simultaneously as a strategic narrative about the agency as well as a partial representation of the actual practices it partakes in and shapes. In the analysis, the following series of questions will be addressed: What professional skills, experience, and personalities are sought after for the various roles and branches within the agency? How does the agency frame itself and its practices through the advertisements? What do the recruitments say about the current organization of FRA and Swedish signals intelligence practices more generally?

In doing so, the chapter contributes, firstly, to the relatively slim literature on contemporary Swedish signals intelligence. Authors have covered the policy changes that expanded FRA’s mandate in the early 2000s (Nohrstedt, 2011), the legal framework for and potential transgressions of their operations

(Klamberg, 2009, 2010), and their transnational cooperation and data-sharing activities as well as "special" relationship with the US, the UK, and expanded Five Eyes network (Larsson, 2022; see also Bigo & Bonelli, 2019; Ördén, Chapter 3 in this volume).

The chapter also contributes to research on intelligence services' increasingly sophisticated methods of data collection as well as the dangers of such technologies (Bigo et al., 2019). Here, scholars have addressed services' use of Big Data (Wegge & Wetzling, 2020), bulk collection (Wetzling & Vieth, 2018), algorithms, and related means. Together, these trends enact a gradual shift of intelligence towards digital mass surveillance practices that impact societies broadly, not least from an ethical and privacy perspective (Macnish, 2018; see also European Union Agency for Fundamental Rights, 2017, pp. 15–18; Bauman et al., 2014). Félix Tréguer (2019) argues, moreover, that the expansion of intelligence services into digital surveillance should be seen as the state's response to a world increasingly determined by multinational technology companies like Apple, Amazon, Google, Microsoft, and Facebook. For states and intelligence actors "to make the digitized world legible and governable", they need to increasingly see and think like Big Tech, co-opting their infrastructures and data-processing techniques (Tréguer, 2019, p. 147; see also Zegart, 2023).

This chapter seeks to link the two literatures, analysing how Sweden's currently expanding and internationally regarded signals intelligence agency, FRA, is in a process of transformation. Recent recruitments suggest that FRA's professional disposition is growing distinctly "plural" (Lahire, 2011) in how its main expertise is focused not only on intelligence analysis but increasingly on acquiring intrusive digital means of data extraction and collection. As such, its core operation is driven as much (or even more) by technological development and technocratic logics as it is by "national security". FRA's profile has thus been redefined: it is not simply an intelligence agency, but it has come to see, think, and act increasingly like a major technology firm.[6]

Material and theoretical framework: the multiple professional dispositions of SIGINT

The material for this chapter consists of an archive of job advertisements downloaded from FRA's recruitment website between December 2022 and October 2023 (115 in total, see appendix). Job postings are for one or several positions at the agency's "signals intelligence section" (23 ads), "technology section" (63), or "cyber activities section" (29).[7] Some ads also specify which of the section's office, unit, or team the position concerns (e.g. the "crypto office", "access development office", "DevOps team", or "detection and warning unit").

Job postings contain both generic information about FRA's mission and what they offer as an employer as well as specific information about the advertised role and the qualifications, experience, skills, and personality traits that are sought after for each position. This ad-specific information is rather detailed and contains information about work organization, everyday tasks and responsibilities, which software, coding languages, or operating systems are used, and more. Personality descriptions are also usually lengthy and address everything from specific qualities like "loyalty" or "creativity" to how applicants should be able to work in groups or independently. It is unclear who exactly authors these ads but given the usually high level of technical detail in the job descriptions, it should be fair to assume that they were not originally written by HR/recruitment staff but by section heads or team leaders from the different agency branches, i.e., people with direct insight into daily operations. Ad texts are then presumably filtered through an HR department (or equivalent) and edited for coherence, before being posted online.

Job advertisements constitute a limited empirical material insofar as they cannot show what actually goes on in practice, as a direct observation or perhaps an interview could. They can only indicate what goes on in practical reality. They can also help construct a kind of "ideal type" (see e.g. Stapley et al., 2022) of the various professionals that are in fact sought after by the agency – both in terms of their practical skills and their personalities, of what they are supposed to "know" and "do" and how they are supposed to "be". This is valuable information, especially since it pertains to a secret intelligence organization that it is otherwise impossible to access.

The material could also be read as an expression of how the agency *wants* to be seen and talked about from an outside perspective. In this regard, the formulation of the ads can be said to constitute what Erving Goffman (1956) called "impression management", i.e., the social effort to influence others' expectations and views of oneself. Indeed, the fact that FRA publicly shares detailed job postings to this extent speaks not only to the current normalization they are undergoing but also to how they see the need to carefully manage their image as employers on a fiercely competitive security technology job market. The ad material should therefore be read partly as a "shadow play", as a carefully curated story and portrayal of intelligence work by the agency's senior officers and HR staff. At the same time, when creating this public image, FRA necessarily needs to reveal some actual details about their practices, work organization, and technical systems in order to attract the candidates they need. Both these dimensions of the material will be taken into account in the analysis.

In the ad material, I have drawn out and analysed common themes and recurring patterns in the ads for the respective agency sections, focusing on (a) the type of task/mission assigned to the advertised position, (b) the type of qualifications, skills, work experience, and/or educational background called for, and (c) the personality types outlined for each role. When read and analysed systematically, the archive of job ads demonstrates, at least to an extent, how FRA's day-to-day work is organized, how the agency is subdivided into departments/teams, and which socio-professional skills and qualities are attached to each unit. This then sheds some light on the relationships, differences, and potential tensions between the units of the organization.

The archive of job ads has been complemented with a number of publicly available employee interviews conducted by FRA themselves and posted on their website and in their annual reports since 2015 and onwards.[8] These contain responses from anonymized employees concerning their specific roles and tasks and include everything from intelligence analysts to system developers to production managers. It can be assumed that these texts, too, are carefully edited to depict the workplace in a particular (neutral or positive) manner and should therefore be read even more as public impression management efforts to attract future employees.

Theoretically, I approach the FRA agency not as a rational or homogenous entity, but more as a "social space" (see e.g. Ben Jaffel et al., 2020) in the sense that it is a diverse workplace and heterogeneous actor which itself consists of multiple agents doing different things. Firstly, from an institutional point of view, FRA can be seen as what Andrew Abbott (1988, pp. 171–177) called a "multi-professional workplace". Following the bureaucratization of professions in most societies, large workplaces have not only grown increasingly hierarchical, but many have also become organizations with multiple forms of professional authority. This includes security and defence institutions. A national intelligence agency, for example, does not consist only of threat analysts, but also engineers and innovators, programme developers and coders, hardware technicians, policy experts, lawyers, and administrators – just as how military organizations, arms manufacturers, police forces, etcetera are made up of an increasingly diverse workforce today. Indeed, as noted, HR departments have also come to play an increasingly key role in defence institutions, especially in times of rearmament when personnel recruitment and brand management become particularly crucial tasks.

Rather than being involved in the public competition over jurisdiction and expertise between professions, multi-professional organizations tend to subsume and integrate several different professional orientations into the workplace. For instance, rather than surrendering software development activities to a private technology firm, agencies like FRA have strived to keep such knowledge and expertise inside the organization by recruiting early-career computer experts and providing them with in-house training (ibid., p. 174). As will be discussed later, this has the potential of shifting loyalties, with some employees solidarizing more with the multi-professional organization itself rather than their broader occupation.

When subsuming multiple professional specializations into an agency, battles over jurisdiction and expertise are also moved in-house. Emerging multi-professional organizations are, therefore, almost by definition, sites of heterogeneity, competition, and internal struggle. This intra-institutional point of view can be taken further into account by drawing, secondly, on Bernard Lahire's (2011) notion of "plural actors". Lahire considers not merely the organizational diversity of professional institutions, but more fundamentally the plurality in terms of an actor's dispositions. Departing from Pierre Bourdieu (e.g. 1977), he insists that an actor's logic of action and disposition (or *habitus*) is far from straightforward and not necessarily organized around a single practice unfolding in a single field. Rather, by intersecting with multiple societal fields over time, an actor "can be the bearer of a plurality of dispositions and straddle a plurality of social contexts" (ibid., p. xii). This can instil a conflictual sense of self in the plural actor, as it is not immediately clear in in which field it "belongs", or what constitutes its main practice.

This goes for not only individuals but also professional bodies whose traditionally coherent role is "challenged by competing and heteronomous logics" when its practice interfaces with "outsiders who do not share the same values", or when its organization is increasingly made up of members with different backgrounds and dispositions (ibid., p. 22). Consider here, for instance, how military organizations have been traditionally seen as autonomous "total institutions" (Goffman, 1961), or how intelligence services have been assumed to function like enclosed "secret societies" (Simmel, 1906), but how such institutions today have become increasingly opened up and plural – interfacing more and more with surrounding society, carrying out expansive missions under broader mandates, and, indeed, recruiting people with diverse experiences who have not been brought up exclusively in the military or intelligence fields. Hence, an actor's dispositional plurality stems from both its internal conflicts and its surrounding societal context.

As Lahire summarizes, an actor "plunged into a plurality of social worlds is subjected to heterogeneous and sometimes contradictory principles of socialisation that they embody", eventually leaving them "with a stock of schemes of action or habits that are non-homogenous, non-unified, and with practices that are consequently heterogeneous (and even contradictory)" (2011, p. 26).

In the analysis below, I will study FRA's recent recruitments from the perspective that it is growing into an increasingly multi-professional organization. This may in turn be transforming the agency into a "dispositionally" plural actor since large parts of its everyday work are conducted by professionals whose core skills and expertise are sometimes far from conventional signals intelligence. What kind of professional dispositions, then, make up a "plural" intelligence actor? Indeed, who *is* the signals intelligence professional today?

Recruiting Swedish signals intelligence professionals

As mentioned, FRA is organized into different "sections", including the signals intelligence section, the technology section,[9] and the cyber activities section. These can be seen as representing "local enclaves" (Abbott, 1988) of the larger organization, all with their own specializations, consisting of individuals with more or less distinct professional dispositions. Indeed, sections are presented as having independent roles and functions, requiring specific kinds of practitioners and experts, yet are at the same time supposed to engage in regular cooperation and exchange amongst each other.

Below, I will begin by analysing the agency sections separately, discussing the role of each section and the competencies and personality types that are sought after in their job ads. In the section after that, I will analyse the agency sections jointly, reflecting on some larger patterns emerging from the material pertaining to the apparent organization of FRA's practices and division of labour among sections.

The signals intelligence section

This section is described as working largely according to the model of the "intelligence cycle", that is, collection of "raw material", followed by processing and analysis of data, followed by production of intelligence reports to state spokespersons. Intelligence analysis concerns the military capabilities of other countries as well as international terrorist activities. The section's electronic surveillance practices are described as "continuously developing" in order to be "one step ahead" and meet "tomorrow's challenges", signalling their close cooperation with the agency's technological development teams.

The section calls for applicants with a variety of educational backgrounds. Ads list high school or vocational college degrees in technical subjects (mentioning specializations like systems development, IT security, and software programming), and university degrees in political science, international relations, law, economics, mathematics, and data science. This agency section is the only one calling explicitly for social science academic degrees.

Ads for this section seek applicants with work experience from the security, defence, and foreign policy sectors. Specific mention is made of security and intelligence agencies like the Swedish Armed Forces, the Security Services, and FRA itself, but also other forms of employment where applicants have acquired knowledge of military platforms and training as well as "military relations" broadly or gained general experience of working with secret or sensitive material. Ads also mention experience of "investigative work", including investigative journalism. Some ads mention specific language skills beyond Swedish and English, as well as experience in translation work. Languages include Dari, Farsi, Arabic, Russian, and Mandarin. This agency section frequently lists tasks involving cooperation/interaction with "internal and external contacts" as well as engaging in "international cooperation".

In terms of professional skills, ads seek analysts with knowledge of processing and analysing large amounts of data (including Big Data, metadata, and traffic data). Specific tools and programmes for data analysis include TensorFlow, pyTorch, Hadoop, Spark, and Wireshark. Some ads also mention work experience related to mobile and fibreoptic networks, and web/application development. Analysts at the signals intelligence section only seem to need a rudimentary knowledge of how technological systems work, though, as tasks to a large extent seem to be about report writing – i.e., compiling and making sense of data and delivering text to executives.

Indeed, more important than technological knowledge is that analysts have the "right personality" and "interests". It is mentioned that applicants should have an interest in foreign policy and security policy. In terms of preferred personality types, ads make explicit use of descriptors such as cooperative, driven, motivated, analytical, orderly, persistent, loyal, "experts" in their area, and "curious about the outside world". The analyst "Petra", interviewed for the FRA website, mentions, for instance, that the most exciting thing about her job is that she can combine her language skills with her "interest in foreign and security policy", and that her team "has a mission that feels important and meaningful".

Interestingly, this section is the only one calling for broadly educated people, preferably with experience from elsewhere in the security sector or policy world, thus holding what Bourdieu would call "cultural capital" and "political capital". Taken together, the calls for a broad academic education and experience from security work along with a "curiosity" about the outside world go hand in hand with how analysts are mainly tasked with translating data patterns into a language understandable for state spokespersons. Analysts need to be able to reproduce established security and foreign policy discourse, in this regard, and perhaps more generally have a diplomatic "feel" for the sociopolitics of intelligence analysis in relation to the broader security policy field.

The technology section

This agency section supplies FRA with the technological systems required to carry out signals intelligence and electronic surveillance. This work includes developing, programming, administering, putting into operation, and providing maintenance to new and existing systems. Judging simply by the number of ads for this section compared to the others, it is, if not already the largest, then at least the section set to expand the most in the coming years.

As with the section above, the educational background among applicants ranges from high school to vocational college to university level. Here, however, specializations and degrees are limited to technical subjects such as IT and radio technology, computer science, civil engineering, and software development.

In terms of tasks and professional skills, ads mention not the *use* of technical systems as above but, again, their *development* and *maintenance*. This involves experience working with Windows and Linux operating systems and servers, radio and telecommunications systems development, system integration, software and application design, developing automation tools, data storage, cloud solutions, IT security, firewalls, and large-scale LAN/WAN systems. It also includes knowledge of specific coding languages (Java, Python, C++, C#/.Net, and PHP), databases (Oracle, MongoDB, PostgreSQL, HDFS, HBase, Cassandra), application packaging tools (VMware AppVolumes, Numecent Cloudpaging, Flexera, Admin Studio), and systems for monitoring online operations (Prometheus, Grafana, Ansible).[10] General knowledge of certain hardware is also mentioned, including radios, antennas, microwaves, signal amplifiers, routers, and electromagnetics. A number of ads mention the development and use of "high-performance computing" or so-called supercomputers and such associated skills (e.g. Linux programmes such as InfiniBand, Lustre, and BeeGFS). Supercomputers are able to process enormous amounts of data and have been used elsewhere for everything from climate modelling to tracking financial flows to teaching AI and machine learning systems.[11]

In terms of the personality descriptions for this section, applicants should be stable, realistic, responsive, helpful, accommodating, solution-oriented, able to "keep calm" and "anticipate problems", and focused on "customer satisfaction". Indeed, most personality descriptions involve tropes of service-mindedness and (technical) supportiveness. A common task description is that "all of our work is based on the team's [product] delivery, and we value a high customer focus".

The overall interpretation is that the technology section is to serve as the "helping hands" to the intelligence analysts, in terms of being their calm and collected support crew that makes sure everything technical runs smoothly. If the signals intelligence section contains broadly competent analysts, the technology section appears like the "nerve centre" that enables the very functioning of the agency. They are also supposed to be one step ahead of analysts regarding what kind of technologies they will need, now or in the future. Indeed, a generic task description for this section mentions the need to "predict developments in the signal environment". This means mapping new and emerging forms of sending data and communicating digitally, as well as understanding how intelligence analysts will require new tools to tap into and listen to such communications. Pushing the limits of what signals intelligence is or means in a technological and methodological sense thus seems to be at the heart of this section's mission. In this regard, they need to constantly think ahead of intelligence analysts.

The cyber activities section

The cyber activities section at FRA has two central tasks. First, it is supposed to "strengthen the protection against qualified IT attacks from abroad" on key societal infrastructure. Second, it is to "develop and deliver access and exploitation capabilities" to the signals intelligence teams. As such, the section can be seen as having both a "defensive" and an "offensive" orientation. They are to protect Sweden's own digital integrity as well as breach others' integrity by penetrating their IT systems. The latter activities – involving technologies of "access and exploitation", or simply put, hacking – are in some ads connected to a policing function at FRA. Some applicants to the cyber section are supposed to work with "IT forensics" and in the role of so-called threat-hunters. This entails mapping individual attackers and their methods as well as digitally tracing and identifying them.

In terms of professional skills, ads similarly focus on applicants' knowledge and experience of developing systems and applications. Here, however, descriptors are possibly even more technical and specific. A whole heap of languages, tools, and programmes are listed related to coding/programming (Python, Golang, Java, Scala, Rust, Elixir, C/C++, Powershell, Assembler, Swift, google-fu, Erlang, Bash), database maintenance (Neo4j, Elasticsearch, Hadoop, Spark, PostgreSQL, MongoDB, S3), data processing (Apache Iceberg, Apache Airflow, and Apache Spark), "reverse engineering" (IDA Pro, Ghidra, Binary Ninja, Radare), "container-based" software packaging (Kubernetes, Podman), software integration and delivery (Jenkins), embedded software architectures (ARM, MIPS), hardware description (VHDL, Verilog), debugging (x64dbg), network protocol analysis (Tshark), digital vulnerability mitigation (ASLR, DEP, CFG), and more.[12] General knowledge of other technologies are also mentioned, including encryption, machine learning/deep learning, malware analysis, binary code/source code, and "white and black box fuzzing".

In some ads, experience with specific "offensive IT security tools" such as BloodHound, Burp Suite, Kali, Metasploit, and Mimikatz are mentioned. Some of these have been designed and used elsewhere for exploiting IT vulnerabilities, extracting passwords, hacking into financial institutions, and illegally installing malware. With these ads, FRA is essentially calling for skillsets mirroring those of cybercriminals.

In terms of applicants' educational background, some degrees/specializations similar to those in the technology section's ads are listed. However, for the cyber activities section, it is far more common to read that "your knowledge and genuine interest for the area [is] more important than a formal education". This reflects a recent strategy at FRA to recruit "amateur" coders and hackers. They have probably realized that people with a strong interest in and knowledge of computer technologies, and especially hacking tools, will not necessarily have undertaken formal education but may have developed these skillsets by themselves. This can be seen as a recognition of the fact that technological development is currently so rapid that more informal ways of knowing are relevant or even necessary.

Therefore, FRA has also launched a website containing "technical challenges".[13] Here, FRA regularly posts new challenges related to coding, IT incidents, encryption, data traffic analysis, installing malware clients, and more. Challenges are typically posted with a short scenario description together with bits of Python code or PCAP files containing network traffic which anyone can download, analyse, and try to solve. If solutions are submitted to FRA, they technically count as job applications.[14] Some challenges have to do with potential real-life scenarios, like digital intrusions into key societal infrastructures, whereas a number of challenges are associated purely with gaming – for instance, recreating the code for classic games like PacMan. This is presumably not a random decision, but one based on the assumption that the best young self-taught programmers and hackers are also part of the gaming culture. Perhaps, it could even be seen as an effort from FRA's side to "gamify" intelligence work, suggesting that some digital forensics work or IT exploitation campaigns are not too dissimilar from computer games.

In terms of personality types for the cyber activities section, descriptors are quite similar to those used for the technology section's ads. However, they include a more frequent use of qualities like “creative”, “curious”, and “innovative”. They also look for personalities who are comfortable working far beyond established conventions. For instance, some ads say that the candidate should “enjoy seeking creative solutions where the manual ends”, where “few or perhaps no recipes or readymade solutions are available” and be “able to solve an upside-down 1000-piece puzzle”. The overall interpretation is that the cyber section seeks to attract the most niche and “nerdy” candidates. It is described as favourable if applicants are “passionate about” extremely detailed things, such as a particular computer software or coding language. The more near-sighted and myopic, the better, it would seem.

FRA as a multi-professional actor with conflicting dispositions

Analyzing the FRA agency’s overall practical organization and division of labour, several patterns emerge. Generally, FRA is presented as an organization in which professionals should be able to develop, grow, and climb the ranks. Advertisements in the technology and cyber sections particularly emphasize that positions include a significant amount of competence development and continuous education. If candidates lack formal training, it will be taken care of in-house since, again, in most cases one’s “interest” in particular technologies and “personality type” seems to trump, e.g. formal diploma and university degrees. For instance, the technology section has a “DevOps” team with an abundance of available positions. As one ad puts it, for the “right people” there are “very good development capabilities”, and “regardless of if you have knowledge or experience of Windows, Linux, networks, data storage, or virtualization, *we have a job for you*” (emphasis added). Applicants should therefore have a strong will to develop and learn from the organization and its teams. If applicants already are experts in their area – for instance, some positions relating to crypto technologies and quantum computing call for candidates with PhD degrees – they are expected to serve as “knowledge resources” for the rest of the agency. Everyone is generally expected to follow the “state of the art” in their specific area, e.g., by attending courses, conferences, and “lab experiments”, both in-house and externally.

Moreover, some applicants are offered junior positions that they can grow out of over time. Being able to climb the career ladder within the organization is indeed an explicit promise at FRA. Employee interviews at the FRA website reflect this as well, as many tell how they have been at FRA for numerous years and shifted roles over time, often to more qualified or senior positions. One job ad concerning an administrative role even suggests that the position, with sufficient competence development in technical systems, could evolve into a signals intelligence role. This suggests that skilled or dedicated individuals, even more or less uneducated ones, can successfully apply to an abundance of technical roles, and from there receive substantial in-house training and climb to positions directly involving threat analysis and intelligence collection.

This poses potential problems. What is the quality of in-house training? Does it address legal and ethical aspects of signals intelligence? Consider, for instance, an intrusive surveillance technology designed to collect communications data without user permission. An academically educated engineer would perhaps problematize the use of such technologies, whereas an internally trained programmer would consider the technology's function for the organization's larger mission. With a well-established system of in-house training of early-career practitioners in multi-professional organizations, recruits' association with the larger occupation and its professional standards indeed tend to break, and their loyalties shift instead to the organization itself (Abbott, 1988, p. 174). This may become particularly amplified in organizations whose work is secret, where practitioners are virtually unable to associate with others in their occupational field. Here, solidarity with the "mission" rather than adherence to broader societal values becomes a consequence as much as a necessity. Nor is allowing young professionals to climb ranks through internal training a new phenomenon but, rather, common in security and defence institutions. What can be regarded as new, though, is how FRA so publicly frames itself as a "career ladder", both in job advertisements and through participating in university career events. They also seem intent on fostering the image of strong internal loyalties, as several of the employee interviews make sure to mention how the agency is "like a family" and has a strong sense of collegial cohesion (e.g. FRA, 2022, p. 39).

In both task and personality descriptions, several advertisements talk of professional "freedom", creative "independence", and the importance of taking "initiative". These are notable terms. In the context of a modern tech firm or software development company, they would appear natural. In an intelligence organization, however, they become unusual, even paradoxical to some degree, since what these professionals deal with is sensitive information, generated through methods and tools of data collection that are equally secretive. Analysts and developers are rather the opposite of "free and independent": they are heavily restricted and regulated by secrecy laws. Similarly, "knowledge sharing", "cooperation", and "teamwork" are mentioned across virtually all ads, and most of the work is described as conducted in various units, teams, and working groups. This is also commonplace in most workplaces today *except*, perhaps, in intelligence and secret services which tend to be strictly divided and ordered through chains of command (see also Ingesson, this volume).

Why does FRA claim to organize itself in this "liberal" way, then, as a workplace of both individual freedom and collective cooperation? Firstly, one could argue that what is presented is a false, or at least only a *partial*, form of freedom and cooperation. Working groups are perhaps allowed to work freely and by their own initiative, but likely only with specific tasks, within clearly restricted boundaries, and under heavy supervision. They may cooperate amongst themselves and with other teams, but only around certain issues and within a strongly controlled socio-professional environment. As the ads make clear, FRA is to a large extent made up of highly specialized technological experts and data analysts, working in niched roles, teams, and "local enclaves". One could guess that these units all hold on tightly to their piece of the larger puzzle that makes up FRA's work, to their secret or sensitive parts of the larger intelligence picture, and only have limited insight into how their knowledge is used by other teams or contributes to the overall mission. As Bigo (2019) reminds us, "secrets" are never fully shared, nor ever fully closed down. Intelligence work should perhaps rather be seen as a spectrum between those who possess mainly technical knowledge (e.g. programmers), to do those who know a few secrets (analysts), to those who know more secrets (middle-managers), to those who possess more of the "full picture" (heads of agency).

Is the framing of FRA as a place of freedom and independence only a clever marketing technique, and a replication of the discourse of large tech firms? Given the kind of competencies and profiles FRA is currently targeting for their technology and cyber sections, candidates are in extremely high demand in today's digitized society, and FRA is in direct competition with everything from exciting new tech start-ups to megafirms like Google and Amazon, and their Swedish counterparts. Again, this speaks to how intelligence services are increasingly forced to see the world and think like "big tech" (Tréguer, 2019). The innovation discourse is not merely a façade, though, not simply a way for FRA to brand themselves. In order to, as they themselves put it, keep up in the ever-evolving "signals environment", they need to also *recruit* and *act* as big tech. Seemingly unorthodox work descriptions and personality types for a secret intelligence organization thus reflect the current transformation of FRA into an actor of plural dispositions. Some agency sections' ways of seeing, understanding, designing, and conducting intelligence require adjustment, even if this creates tensions and contradictions with other sections' ways of traditionally doing things. As Lahire (2011, pp. x–xiii) notes, plural actors are characterized by this kind of clash between historically embodied dispositions and currently lived realities in a multiplicity of social contexts, for instance as in how FRA's transformation into a high-tech multi-professional organization stands in some contrast to its original role of collecting military secrets through telegraphic cables.

A further illustration of the agency's big tech metamorphosis is how its technology section is described as organized and working in so-called agile development teams and around "agile working methods". The "agile" philosophy has become a common way of organizing modern workplaces, particularly in product and software development firms. It essentially means removing "bureaucratic" obstacles to efficient and innovative product development, such as unnecessary processes, guidelines, administration, and documentation. Instead, people should be organized in smaller and more flexible teams where they can communicate efficiently and do more hands-on work, with a strong product and customer focus. Agile methods have many names/orientations (with some of the more popular being Scrum, DevOps, and SAFe), and "agile coaches" can be hired, just as FRA has done, to teach and implement these methods at the workplace.

In the context of FRA, the agile philosophy seems to play out in a way that creates a kind of commodified market dynamic between the different sections. As noted above, the technology section becomes the leading innovator and product developer with a strong service- and customer-oriented mindset. The signals intelligence section, according to the same philosophy, then becomes the "product owner", and is in fact frequently referred to in the ads as the in-house "client" or "customer". In agile work, any obstacles to pure product development should be removed so that developers can supply the "perfect" product. Here, the product is deemed perfect not according to its broader societal value or contribution, but rather when the customer is satisfied with it and when it runs as it should without bugs. Imposing a supplier–customer relationship between developers and intelligence analysts hence effectively frees, or at least distances, the technology section's staff from any ethical issues surrounding their products and solutions. Coders and system developers need not worry if the signals intelligence section places an order on an outrageously intrusive surveillance tool. Their focus should be on perfecting the product – or better, thinking "one step ahead" on how it could be pushed even further.

This dominant product focus risks further imposing a technocratic logic behind the organization of FRA's practices. As a range of scholars in the field of critical security studies have shown (e.g. Guittet & Jeandesboz, 2010; Huysmans, 2006), such thinking around security issues is dangerous because it effectively depoliticizes responses to threats by assuming that key decisions should be taken by technical experts and that the "solution" is always more and better technologies. As noted, this is seemingly already unfolding at FRA where it appears that digital surveillance innovators and in-house hacking teams are drawing the maps for intelligence analysts and setting the agendas for the future.

Conclusion

An analysis of job advertisements for an intelligence service generates limited findings insofar as the material can only say very little about the organization's day-to-day operations. It can say more, however, about the professional skills *needed* for such operations, what practitioners are *supposed* to do and know, and roughly how they are to be *organized* in relation to each other. This is still meaningful information, especially given the classified nature of intelligence organizations. It has mattered less for the analysis if this information has been carefully edited and to some degree curated by the service itself. On the contrary, this too becomes valuable information since it illuminates how FRA publicly positions itself in the current security technology job market. This chapter has thus been about the professional make-up and apparent practical organization of FRA as much as it has been about its public image and "official story".

With these empirical caveats in mind, findings have nonetheless illustrated certain emerging characteristics of FRA and how it is gradually turning into (or at the very least, wants to be perceived as) a multi-professional intelligence organization. What makes up an ideal type signals intelligence professional in such an organization? While this question still requires further investigation, it can be concluded that FRA today consists of a range of people with different skills, merits, experience, expertise, educational backgrounds, interests, and, indeed, professional dispositions. The agency consists simultaneously of tech experts *and* threat analysts, data engineers *and* social scientists, manufacturers *and* customers – practitioners who operate in distinct enclaves of the organization yet are expected to "cooperate". Some groups focus their expertise on talking the language of governments, others on delivering the perfect surveillance product, and others still on imitating cybercriminals and hackers. Some wield political and bureaucratic capital; others draw on technological capital. Here, it would be fair to assume that the growing dispositional plurality within FRA has given rise to new hierarchies, tensions, and potential conflicts that did not exist within the service some decades ago.

This has arguably also shifted the profile of the agency as well as challenged the exceptionalism and "mystique" that tend to surround intelligence actors (Herman, 1996, p. 327). Among the individuals, teams, and sections constituting FRA, only a few are filling the conventional intelligence "function" of assessing threats to national security, whereas a large proportion, perhaps even a majority, are concerned with developing, delivering, and maintaining digital surveillance products. To many employees, everyday tasks and work philosophies likely do not differ much from those of a software development company. Hence, FRA is now increasingly required to balance its image as an extraordinary secret service against its image as an "ordinary job" in the tech sector. The agency cannot simply play the stereotypical role of being the state's secret informer, but it needs to position itself in a variety of social contexts in order to navigate a highly competitive niche job market. Has this also disturbed the agency's sense of field belonging? FRA may have more in common, and share more struggles with, private tech firms than other intelligence organizations, secret services, and defence agencies in Sweden. Indeed, as Lahire (2011, pp. 28–31) notes, plural actors should be considered as more than field actors: not everything in socio-professional life occurs in fields; nor is an actor contained only within one field.

I want to end by again underlining the risks with one of the world's most prolific signals intelligence services seemingly transforming into a big tech player. Judging by current recruitment priorities in FRA's job ads, the hunger for technological innovation (i.e. developing more "effective" surveillance tools) appears almost stronger than the hunger to achieve "national security". This would certainly be worrying. Even the most transgressive members of the international intelligence community already enjoy significant impunity (Bigo et al., 2023), and this tendency would only increase if services are allowed to continue down the path of technocracy where the answer is always *more* technical "solutions" and *less* political conversation on intelligence practices, on which "problems" they actually respond to, and with what social and ethical implications.

Notes

[1] Between 2018 and 2020, two public investigations were conducted to update the legal framework for Swedish signals intelligence practices. They focused on FRA's international cooperation and handling of personal data, respectively (SOU, 2020).

[2] FRA joined Twitter in 2018 and Instagram in 2022. They also participate in career events like the Swedish Defence University's "Cyber Challenge".

[3] Similar tendencies can also be seen in Denmark, where the Defence Intelligence Service (*Forsvarets Efterretningstjeneste*) have publicly commented on the need to wash off the "Bond myth" and start hiring "ordinary people"; see https://jyllands-posten.dk/indland/ECE14806247/fechef-vi-leder-efter-agenter-med-realkreditlaan-og-aulalogin/ (in Danish).

[4] See also Michael Herman's (1996, p. 327) discussion on how intelligence professionals tend to share the characteristics of secrecy, mystery, as well as a sense of being different.

[5] See https://www.regeringen.se/contentassets/def2026cac0b4ef7acf4afeb988326ed/utgiftsomrade-6-forsvar-och-samhallets-krisberedskap.pdf (in Swedish), p. 60.

[6] The author is grateful to the volume editors as well as Hager Ben Jaffel for their valuable comments on earlier versions of this chapter.

[7] Ads for the agency's administrative department have not been collected for analysis.

[8] Available at https://fra.se/nyheter/arsrapporter.4.55af049f184e92956c42a87.html (in Swedish).

[9] The branch responsible for technological development can be likened to what has previously been referred to as FRA's "auxiliary operations" (*utvecklingsverksamhet*) (Klamberg, 2010). These activities seem to have grown into a formal agency section since the 2000s.

[10] Additional technological terms whose meaning/context is not described further in this section's ads include Powershell scripting, WebAssembly, Node.js, D3.js, OpenLayers, MECM/SCCM, VDI/Horizon, Data Science Notebooks (Jupyter, Zeppelin), DOTNET, Typescript, REST/Microservices, KVM, React, Jira, and Confluence.

[11] See e.g. https://www.ibm.com/topics/hpc.

[12] Additional technological terms whose meaning/context is not described further in this section's ads include YARA, xxd, PostgresQL, Phoenix, RabbitMQ, and EventStoreDB.

[13] See https://challenge.fra.se.

[14] Here, it should be noted that technical challenges used as job applications is not a new phenomenon. FRA rolled out an advertisement campaign in the Stockholm subway trains some years ago where posters showed only a short bit of code. Solving the "puzzle" would lead you to their recruitment webpage. In fact, since the 1990s, the Swedish intelligence community has frequently used similar "tests" and cryptos in place of ordinary job interview questions, with candidates asked to, e.g., analyse signals data to recreate a fictional terrorist organization (see interview in Swedish with Jan-Olof Grahn in the *I Krig och Fred* podcast, ep. 66, May 2020).

References

Abbott, A. (1988). *The System of Professions: An Essay on the Division of Expert Labor*. University of Chicago Press.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R.B.J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144.

Ben Jaffel, H., Hoffmann, A., Kearns, O., & Larsson, S. (2020). Collective discussion: Toward critical approaches to intelligence as a social phenomenon. *International Political Sociology*, *14*(3), 323–344.

Bigo, D. (2019). Shared secrecy in a digital age and a transnational world. *Intelligence and National Security*, *34*(3), 379–395.

Bigo, D., & Bonelli, L. (2019). Digital data and the transnational intelligence space. In *Data Politics: Worlds, Subjects, Rights*. Routledge.

Bigo, D., Isin, E., & Ruppert, E. (Eds.). (2019). *Data Politics: Worlds, Subjects, Rights*. Routledge.

Bigo, D., McCluskey, E., & Tréguer, F. (Eds.). (2023). *Intelligence Oversight in Times of Transnational Impunity: Who Will Watch the Watchers?* Routledge.

Bourdieu, P. (1977). *Outline of a Theory of Practice*. Cambridge University Press.

Duroy, S. (2023). *The Regulation of Intelligence Activities under International Law*. Edward Elgar Publishing.

European Union Agency for Fundamental Rights. (2017). *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume 1: Member States' Legal Frameworks*. European Union Agency for Fundamental Rights.

FRA. (2022). *FRA Årsrapport 2022: Året då kriget kom till Europa*. Försvarets Radioanstalt.

Goffman, E. (1956). *The Presentation of Self in Everyday Life*. University of Edinburgh Social Sciences Research Centre Monographs.

Goffman, E. (1961). *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates* (1st ed). Anchor Books.

Guittet, E.-P., & Jeandesboz, J. (2010). Security technologies. In *The Routledge Handbook of New Security Studies*. Routledge.

Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge University Press.

Huysmans, J. (2006). *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. Routledge.

Klamberg, M. (2009). FRA:s signalspaning ur ett rättsligt perspektiv. *Svensk Juristtidning*, *4*, 519–541.

Klamberg, M. (2010). FRA and the European convention on human rights: A paradigm shift in Swedish electronic surveillance law. In *Overvåking i en rettstat* (pp. 96–134). Fagforlaget.

Lahire, B. (2011). *The Plural Actor*. Polity Press.

Larsson, S. (2022). The techno-legal boundaries of intelligence: NSA and FRA's collaborations in transatlantic mass surveillance. In *Problematising Intelligence Studies: Towards a New Research Agenda*. Routledge.

MacAskill, E., & Dance, G. (2013, November 1). NSA files: Decoded – What the revelations mean for you. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Macnish, K. (2018). Government surveillance and why defining privacy matters in a post-snowden world. *Journal of Applied Philosophy*, *35*(2), 417–432.

Nohrstedt, D. (2011). Shifting resources and venues producing policy change in contested subsystems: A case study of Swedish signals intelligence policy. *Policy Studies Journal*, *39*(3), 461–484.

Rensfeldt, G. (2013). Read the Snowden documents from the NSA. *Sveriges Television*. https://www.svt.se/nyheter/granskning/ug/read-the-snowden-documents-from-the-nsa

Simmel, G. (1906). The sociology of secrecy and of secret societies. *The American Journal of Sociology*, *11*(4), 58.

SOU. (2020). *Försvarets radioanstalts internationella samarbete—En översyn av regelverket: Betänkande av Utredningen om regleringen av Försvarets radioanstalts internationella samarbete* (2020:68). Government of Sweden.

Stapley, E., O'Keeffe, S., & Midgley, N. (2022). Developing typologies in qualitative research: The use of ideal-type analysis. *International Journal of Qualitative Methods*, *21*, 1–9.

Tréguer, F. (2019). Seeing like big tech: Security assemblages, technology, and the future of state bureaucracy. In *Data Politics: Worlds, Subjects, Rights*, 1st Edition. Routledge.

Wegge, N., & Wetzling, T. (2020). Countering hybrid threats through signals intelligence and big data analysis? In *Intelligence Relations in the 21st Century*. Springer International Publishing.

Wetzling, T., & Vieth, K. (2018). *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations*. Heinrich Böll Stiftung.

Zegart, A.B. (2023). *Spies, lies, and algorithms: The history and future of American Intelligence*. Princeton University Press.

A. Appendix

List of job advertisements (in Swedish, 115 unique ads in total), collected from FRA's recruitment website between December 2022 and October 2023 (https://fra.easycruit.com).

Signals intelligence section

- Analytiker Inom Farsi/Mandarin/Ryska/Dari
- Analytiker Med Inriktning Naturvetenskap Och Ryska
- Analytiker Med Inriktning Teknisk Analys
- Analytiker Med Teknikfokus
- Analytiker Med Teknisk Inriktning
- Analytiker till Nytt Spännande Verksamhetsområde
- Analytisk Signaldetektiv
- Data Scientist till Svensk Underrättelsetjänst
- Datastöd till FRA
- Enhetschef till Signalunderrättelseverksamheten
- FRA Söker Analytiker Med Fokus På Bearbetning till Vår Underrättelseproduktion
- FRA Söker Personal till Kabelinhämtningen
- Framtidens Underrättelseanalytiker
- Handläggare till Signalunderrättelseavdelningens Expedition
- Kreativ Signalspanare
- Kreativ Signalspanare (2)
- Kvalificerad Signalspanare till Svensk Underrättelsetjänst
- Senior Handläggare till Signalunderrättelseverksamheten
- Stabshandläggare
- Teknisk Enhetschef För Verksamhetsområdet Kontraterrorism
- Underrättelseanalytiker Med Teknikfokus
- Underrättelseanalytiker till Signalunderrättelseverksamheten
- Underrättelseanalytiker

Technology section

- Agil Projektledare
- Agil projektledare/Leveransledare
- Applikationspaketerare – Deployment Och Klientvirtualisering
- C++ Utvecklare

- Data Engineer
- DevOps Engineer
- DevOpsNet-Ingenjör TDV
- Elektronikkonstruktör
- Elektronik-/Mätteknik-Ingenjör
- Erfaren Nätverkstekniker
- FRA Söker En Driven Virtualiseringstekniker
- FRA Söker En Erfaren Applikationspaketerare
- FRA Söker IT-Tekniker
- FRA Söker Kreativ Mjukvaruutvecklare
- FRA Söker Systemutvecklare Inom JavaScript
- FRA Söker Systemutvecklare
- FRA Söker Teknisk Leveransledare
- Frontend-Utvecklare Inom Radiosystem
- Fullstackutvecklare
- Infrastructure System Engineer
- Infrastructure Developer Linux Engineer
- IT Portfolio Manager till FRA
- IT Portfolio Manager
- IT-Arkitekt Nätverk
- IT-Säkerhetsrådgivare För Compliance
- IT-Specialist till Svensk Underrättelsetjänst
- IT-Specialist till Svensk Underrättelsetjänst (2)
- IT-Talanger till Svensk Underrättelsetjänst
- Junior Systemtekniker Med Fokus På IT-Drift
- Junior Systemutvecklare till Göteborgsområdet
- Kreativ Systemintegratör till FRA
- Linux Systemadministratör i Superdatormiljö
- Linux Systemadministratör Inom Produktion Och Utveckling
- Matematisk Algoritmutvecklare
- Mätingenjör Inom EMC Och RÖS
- Nätverksingenjör
- Nätverkstekniker/IT-Tekniker
- Oracle DBA
- Platform Developer Linux Engineer
- Senior Nätverkstekniker
- Senior Nätverkstekniker (2)
- Senior Software Engineer
- Senior Software Engineer (2)
- Supporttekniker
- Systemintegratör Inom Nätverksteknik Och Utveckling
- Systemintegratör Inom Nätverksteknik
- Systemintegratör Med Erfarenhet Av Linux
- Systemintegratör till FRA
- Systemintegratör
- Systemutvecklare/Data Engineer

- Systemutvecklare Fullstack Java
- Systemutvecklare Inom Mjukvaruradio
- Systemutvecklare Inom Mjukvaruradio (2)
- Systemutvecklare Inom Radiosystem
- Systemutvecklare
- Teknisk Strateg Inom Svensk Underrättelsetjänst
- Vi Söker Alltid Duktiga IT-Specialister
- Vi Söker Fler IT-Specialister till Svensk Underrättelsetjänst
- Vi Söker Fler IT-Tekniker till FRA
- Windows/Linux-Specialist
- Windows/Linux-Specialist (2)
- Windowsspecialist till Svensk Underrättelsetjänst
- Windowsspecialist till Svensk Underrättelsetjänst (2)

Cyber activities section

- Analytiker Cyberhot
- Är Du TDV-Enhetens Nästa Koordinator?
- Elixirutvecklare till Svensk Underrättelsetjänst
- Enhetschef i Kärnan Av Svensk Signalspaning
- Enhetschef till Cyberavdelningen
- Exploitutvecklare
- Exploitutvecklare (2)
- Förmågeutvecklare Telekommunikation
- FRA Söker Cyberstrateg
- FRA Söker Hacker/Reverse-Engineer
- FRA Söker Threat Hunters Och Incidenthanterare
- Handläggare Med Inriktning Juridiska Och Policyrelaterade Frågor
- Handläggare Signalskyddsnycklar
- Hårdvarudekonstruktör Reverse Engineer for Embedded Systems
- IT-Säkerhetsspecialist Med Inriktning På Penetrationstestning
- Junior Analytiker Inom Cyberhot
- Junior DevOps till Svensk Underrättelsetjänst
- Kommunikatörer Med Inriktning Press Och Webb
- Kryptokontoret Söker Enhetschef
- Kryptolog Inom HPC
- Kryptolog Med Intresse För Reverse-Engineering
- Kryptolog till FRA
- Platform Engineer
- Senior Data Engineer/Scientist
- Systemutvecklare För Att Stärka Sveriges Cyberförmåga
- Teknisk Kryptoanalytiker/Utvecklare Med Intresse För Matematik
- Utvecklare/Problemlösare/Hackers
- Utvecklareproblemlösarehackers
- Windowsspecialist till Svensk Underrättelsetjänst