Intelligence Education as a Competence Challenge: Applying the Intelligence Competence Framework to SOU 2025:78

by Gazmend Huskaj and Stefan Axelsson

Resumé

De underrättelseutbildningar som SOU 2025:78 hänvisar till uppvisar en strukturell asymmetri: formella och informella domäner dominerar medan den tekniska domänen är underartikulerad, särskilt på taktisk nivå. Mönstret framträder genom ett hybridramverk, Intelligence Competence Framework (ICF), som kombinerar tre analysnivåer (strategisk, operativ och taktisk) med tre domäner från Yngströms systemholistiska ansats: teknisk, formell och informell. Ramverket tillämpades genom riktad kvalitativ innehållsanalys på SOU 2025:78 och på elva internationella utbildningsprogram. Samtliga elva program kodas som stark i den formella domänen på strategisk nivå, medan endast ett program kodas som stark i den taktisk-tekniska cellen. En svensk underrättelseakademi byggd på befintliga modeller kan ärva denna asymmetri om inte teknisk domänkompetens behandlas som ett strukturellt krav i akademins utbildningsstruktur.

INTELLIGENCE EDUCATION OPERATES in an environment that is being reshaped by technological transformation.[1] Artificial intelligence, machine learning, cloud-based data processing, and advanced sensor systems are altering how intelligence services collect, process, analyse, and disseminate information.[2] The U.S. National Security Commission on Artificial Intelligence (NSCAI) concluded in 2021 that AI-enabled capabilities will improve every stage of the intelligence cycle, from tasking through collection, processing, exploitation, analysis, and dissemination.[3] The Commission recommended that intelligence professionals be enabled with baseline digital literacy and access to the digital infrastructure required for ubiquitous AI integration.[4]

Recent experimental evidence confirms this trajectory. In war-gaming exercises using the Snow Globe multi-player AI system, the Central Intelligence Agency's (CIA's) Directorate of Digital Innovation (DDI) and In-Q-Tel found that participants with greater prior digital experience used AI assistants more systematically and critically than those without such experience.[5] A parallel DDI research programme on Emergent Intelligence proposed that intelligence officers must develop not only technical skills but also advanced reasoning, ethical decision-making, and strategic communication skills. Effective collaboration with AI systems requires combining data science, machine learning, and advanced analytics with human judgement.[6]

These developments are not confined to the United States. In Sweden, the government inquiry *En reformerad underrättelseverksamhet* (SOU 2025:78) addresses the

country's intelligence and security services: the Military Intelligence and Security Service (Must), the National Defence Radio Establishment (FRA), and the Swedish Security Service (Säkerhetspolisen).[7] The inquiry characterises personnel as a strategic resource and frames education and competence development as prerequisites for a reformed intelligence system capable of meeting an increasingly complex and rapidly shifting threat landscape. SOU 2025:78 proposes that the Swedish Defence University (Försvarshögskolan, FHS) develop a joint education platform for intelligence and security services, with a long-term objective of establishing a Nordic intelligence academy in cooperation with partner nations.[8]

The proposal operates within an existing Swedish institutional landscape. Campus totalförsvar links FHS with Örebro University and Luleå University of Technology as a strategic platform for total-defence research and education.[9] Cybercampus Sweden, founded by KTH, RISE, and the Swedish Armed Forces, pursues research, innovation, and education for cyber security and defence.[10] Lund University's Department of Political Science offers intelligence-analysis teaching across first, second, and third cycles.[11] However, SOU 2025:78 does not systematically reference these institutions when specifying the proposed academy's scope.

The inquiry identifies cloud-based data processing, AI, and cross-domain integration as priority capability areas that require substantial investment. It further observes that the transition to cloud-based processing will deliver significant improvements for integrated processes between the different services, which in turn should lead to increased resource efficiency and increased attractiveness for new competencies.[12] SOU 2025:78 references a set of international intelligence education programmes as benchmarks for the proposed Swedish platform.[13] These include the National Intelligence University in the United States, the Intelligence College in Europe, and national programmes in Norway, Denmark, Germany, the Netherlands, and the United Kingdom.

Sweden's position within NATO, its total defence concept, and the demands of its intelligence services for personnel with cross-domain competence create a concrete policy context for the question of how intelligence education should be structured. The declining number of graduates with language competence in Russian and Chinese — identified by SOU 2025:78 as a constraint on recruitment — shows the broader human capital challenge facing Swedish intelligence services.[14] The inquiry also proposes reinstating the specialist officer training in intelligence and security at FHS, which was discontinued in the mid-1990s. It further proposes expanding the interpreter school at the Armed Forces' Intelligence and Security Centre (FMUndSäkC) into a national resource for the total defence.[15] These proposals address specific capability gaps. However, they do not articulate a systematic approach to the structural question of how competence should be distributed across levels and domains within the intelligence education system as a whole.

The structural case for a new education platform rests on three drivers that SOU 2025:78 identifies. The inquiry proposes a new foreign intelligence agency separated from the Swedish Armed Forces. The agency will operate under restructured oversight, strengthened democratic control, and its own governance arrangements.[16] Personnel entering this agency will require competence that is built for its specific mandate from the start. A joint education platform can deliver this competence at the point of recruitment.

The military intelligence service continues to operate within the Armed Forces. It needs a more coordinated and developed training pipeline at the operational and tactical levels, in line with how comparable services are supported in partner nations.[17] A joint platform can provide this pipeline as a shared national resource. SOU 2025:78 names cloud-based data processing, AI, and cross-domain integration as priority capability areas.[18] These capabilities must be reflected in what the education system teaches at every level.

Therefore, a joint platform provides one institutional answer to all three drivers. It supplies the new agency with purpose-built education, it gives the military intelligence service a shared operational-tactical training structure, and it places technical competence inside the curriculum as a core requirement.

Existing research has examined intelligence education from several perspectives. Coulthart and Crosston mapped American intelligence curricula thematically and identified three knowledge pillars — procedural, core, and domain — but found that technical expertise and engagement/collaboration were the least addressed competencies.[19] Petersen and Rønn analysed eleven Scandinavian intelligence programmes and concluded that teaching is dominated by Anglo-American methods and historical cases of intelligence failures, with limited adaptation to Nordic societal and cultural contexts.[20] Dylan, Goodman, Jackson, Jansen, Maiolo, and Pedersen documented how the Norwegian Defence Intelligence School resolved the tension between professional intelligence practice and academic accreditation through a dedicated bachelor programme.[21]

Berger, Borghoff, Conrad, and Pickl argued from the German experience with the Intelligence College in Europe that IT and data-science integration is essential for producing intelligence professionals capable of providing accurate and timely decision-making knowledge.[22] Ramsay and Macpherson assessed the degree to which U.S. graduate intelligence programmes have integrated quantitative analysis courses and found that intelligence education has not kept pace with the demand for data-literate analysts.[23] Gruszczak analysed the Intelligence College in Europe through the lens of cultural diffusion. He concluded that top-down institutional incentives are effective when embraced by stakeholders committed to shared values, but that bottom-up motivations driven by national assets have limited impact on shaping shared educational frameworks.[24]

These studies describe content, institutional design, or pedagogical orientation.

However, none applies a multi-level, multi-domain analytical framework that diagnoses where competence is structurally concentrated and where it is absent across the intelligence education landscape. Existing research provides limited systematic analysis of the interaction between technical, formal, and informal competence requirements at different levels of intelligence activity. This article addresses the following question:

> What structural patterns characterise the distribution of competence across intelligence education programmes referenced by SOU 2025:78, and where do asymmetries exist between what the inquiry requires and what existing programmes articulate?

The Swedish policy conversation on this question has a longer history than SOU 2025:78. At the FHS/Center for Asymmetric Threat Studies (CATS) workshop in October 2018, Yngström identified the structural tension between open academic institutions and Swedish national-interest competence supply. She argued that a new organisational form,

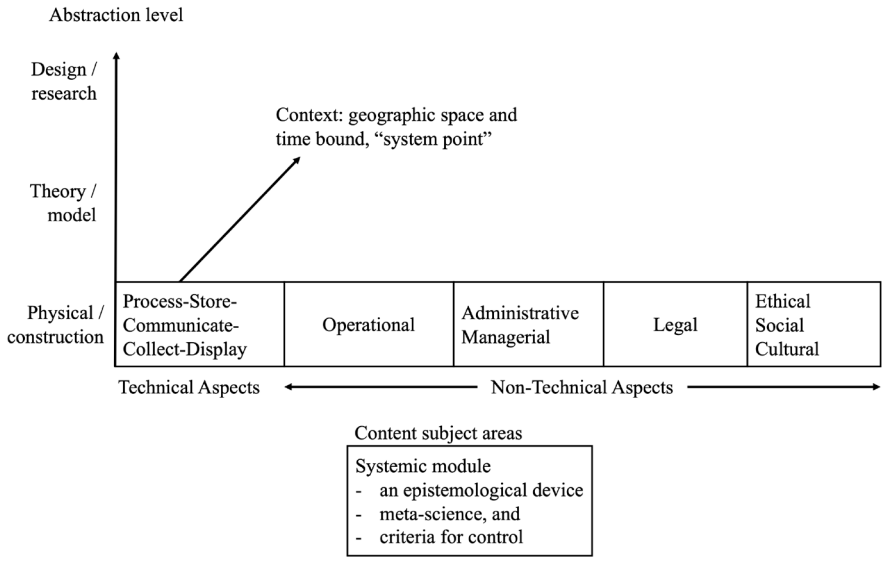

Figure 1. The Systemic-Holistic Model for Security Informatics (adapted from Yngström, 1996). Content subject areas range from technical aspects (process, store, communicate, collect, display) through operational and administrative-managerial to legal and ethical aspects, situated within a context of time, space, and geographical constraints.

operating in collaboration with existing Swedish research and education institutions, would be required to resolve it.[25] CATS itself has run intelligence education for more than twenty years. A 1999 government investigation of the Swedish intelligence community identified the need for educational development, and CATS ran the first Senior National Intelligence Course from 2003 and the National Executive Intelligence Course from 2004.[26]

The article is structured as follows. Section 2 presents the analytical framework. Section 3 describes the method, data, and analytical procedure. Section 4 presents the findings. Section 5 discusses the implications of the findings. Section 6 concludes.

Analytical Framework

Intelligence education serves functions that range from strategic policy support to operational collection and tactical analysis. An analytical framework for this domain should analyse where competence is concentrated and where it is absent across interacting system components, without reducing the problem to any single specialisation. Two traditions provide the conceptual vocabulary for such an instrument: the systemic-holistic tradition in information security research and the multi-level tradition in national security analysis.

The systemic-holistic tradition was developed by Yngström at the Department of Computer and Systems Sciences at Stockholm University.[27] Yngström's Systemic-Holistic Approach (SHA) — *systemic* in the sense of integrating interacting system components, not *systematic* in the sense of procedural regularity — relies on three building blocks: General Systems Theory including Cybernetics, Soft System Methodology, and

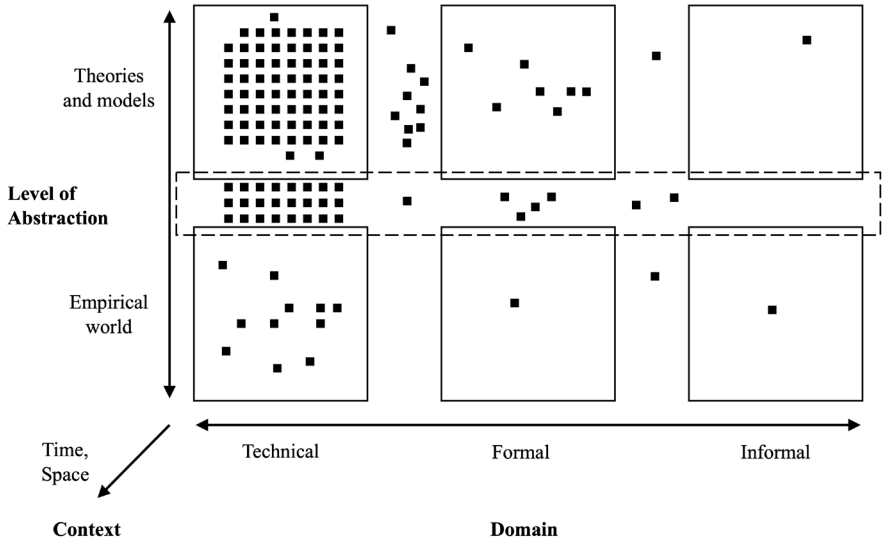

Figure 2. Applying the classification model to the 125 papers from the SEC 2000 proceedings (Björck and Yngström, 2000). Each dot represents one paper, placed within the domain (Technical, Formal, Informal) and level of abstraction where it belongs. The density in the technical domain is immediately visible.

General Living Systems Theory. Yngström also describes the approach as a multidisciplinary one, reflecting its design to draw research and description methods from several disciplines for a single application domain.[28] It organises security phenomena across three interacting domains: technical, formal, and informal.[29] The technical domain encompasses infrastructures, analytic tools, hardware, software, and communication systems. The formal domain encompasses laws, policies, governance structures, classification regimes, and explicit organisational rules. The informal domain encompasses professional norms, organisational culture, trust, judgement under uncertainty, and social relations. Figure 1 reproduces the SHA model.

The analytic power of this classification has been demonstrated empirically. Björck and Yngström applied the domain model to 125 papers presented at the IFIP World Computer Congress SEC 2000 conference. They found that 83 per cent concentrated in the technical domain, while only 14 per cent addressed the formal domain and 3 per cent the informal domain.[30] However, industry surveys indicated that employee awareness — located in the informal domain — constituted the primary obstacle to organisational security.[31] The value of the SHA lies in making such distributional asymmetries visible. Figure 2 reproduces the classification applied to the SEC 2000 proceedings.

This article applies the same analytic reasoning to intelligence education, where the asymmetry may run in the opposite direction. The analytical expectation is that intelligence education concentrates in the formal and informal domains with underarticulation of the technical domain as a system-level competence. If this holds, the distributional pattern in intelligence education would be the structural inverse of the

pattern that Björck and Yngström identified in information security research — a finding with direct implications for how states design and evaluate intelligence education systems.

The SHA is also an implementable curriculum model. DSV/SU built its *Säkerhetsinformatik* programme on the same systems-science foundation and taught technical and non-technical material from the programme's founding. The non-technical content included organisational science, business administration, and legal informatics. Between 2003 and 2012/13, DSV/SU delivered the international master's programme *Information and Communication Systems Security* (ICSS) at KTH.[32] Therefore, the SHA is not only an analytic instrument but a curriculum structure that has been operated inside a national university system for a decade. The ICF inherits this implementability.

The vertical axis of the framework is drawn from the Multi-Level, Multi-Dimensional (MLMD) framework developed by Huskaj for analysing how states organise national security capabilities.[33] The MLMD framework operates across three levels, each anchored in established theory. The theoretical foundations are drawn from deterrence theory at the strategic level, intelligence theory at the operational level, and the theory of offensive cyberspace operations at the tactical level. These three bodies of theory are not domain-specific to cyber; they address how states develop credible postures, how intelligence processes support decision-making, and how strategy is translated into executable action through technical means.

At the strategic level, deterrence theory provides the analytical base. Snyder's formulation addresses how states develop credible postures through the interaction of capability, intent, and signalling.[34] Dahl's concept of power clarifies the relational character of deterrence: credibility depends not only on what a state possesses but on what an adversary believes a state can and will do. For intelligence education, the strategic level addresses the competence required to understand how intelligence capabilities contribute to national signalling, strategic assessment, and the credibility of the state's deterrence posture.

At the operational level, intelligence theory directs the analysis. Gill and Phythian's framework addresses the processes of collection, analysis, and dissemination that support planning and decision-making.[35] Johnson's work on strategic intelligence clarifies how the intelligence cycle translates policy requirements into actionable products. The operational level addresses the competence required to manage the intelligence process across disciplines — coordinating tasking, integrating collection, producing analysis, and disseminating products to decision-makers.

At the tactical level, strategy translates into executable action through the application of technical tools, procedures, and tradecraft.[36] This rationale is articulated in offensive cyberspace operations doctrine but applies structurally across intelligence disciplines — whether the operating environment involves signals intelligence, human intelligence, or cyberspace operations. The tactical level addresses the competence required to operate technical systems, interpret data, and apply tradecraft norms in specific operational contexts. Tactical competence is where the formal rules of handling and dissemination meet the informal norms of professional judgement — and where the technical infrastructure either enables or constrains what an analyst can accomplish within the available decision window.

The MLMD's original dimensions — political, ethical, and technical — were tailored for the specific problem of offensive cyberspace

operations as a state capability.[37] However, the object of analysis in this article is intelligence education across the full range of intelligence disciplines within the state. This requires a broader vocabulary that captures governance structures and legal mandates, professional norms and judgement, and technical systems and infrastructure simultaneously. Yngström's domains — technical, formal, informal — provide this breadth because they were designed to classify security phenomena across the full socio-technical spectrum, and not within a single operational domain.[38] Therefore, this article retains the MLMD's three levels and replaces its original dimensions with Yngström's three domains. The result is a MLMD-SHA framework, herein called the Intelligence Competence Framework (ICF).

The ICF produces a 3×3 matrix (*Table 1*). Each cell represents the intersection of one level with one domain. The framework does not prescribe curriculum content. It functions as a diagnostic instrument that identifies distributional patterns and structural asymmetries in how intelligence competence is articulated and institutionalised. Competence requirements are structurally interdependent: strategic credibility depends on operational integration, operational performance depends on tactical literacy, and tactical activity is conditioned by strategic mandates.

Designing the Research

The article applies the ICF through directed qualitative content analysis to two corpora. Corpus A is SOU 2025:78, the Swedish Government's inquiry into reformed intelligence activities.[39] Corpus B consists of eleven intelligence education programmes that SOU 2025:78 references as benchmarks,[40] listed by country in *Table 2*.

Every passage in SOU 2025:78 that addresses competence, education, training, technology, or professionalisation was coded into one of the nine cells of the ICF matrix. Each passage was assessed for its dominant level (strategic, operational, or tactical) and

Level / Domain	Technical Domain	Formal Domain	Informal Domain
Strategic	National analytic infrastructures; system reliability and timeliness; performance constraints shaping strategic feasibility.	Mandates, oversight, classification, disclosure rules; authority conditions shaping signalling and deterrence posture.	Leadership risk posture; escalation norms; credibility expectations influencing strategic judgement.
Operational	Data integration, analytic tooling, secure workflows; feedback loops linking tasking, collection, analysis, and dissemination.	Tasking structures, governance routines, resource prioritisation; institutional coupling between intelligence output and planning.	Coordination routines, incentives, trust, organisational friction; communication norms shaping analytic consistency.
Tactical	System mapping, data provenance, tool limitations, error modes; time-sensitive interpretation of technical artefacts.	Handling constraints, dissemination boundaries, authorisation rules; operational compliance under time pressure.	Tradecraft norms; bias mitigation; judgement under uncertainty and temporal constraint.

Table 1. The Intelligence Competence Framework.

#	Country / Region	Host institution	Programme / platform	Type
1	Denmark	Danish Defence University / University of Southern Denmark	Master of Intelligence and Cyber Studies (MICS)	Professional-military
2	Europe	Intelligence College in Europe (ICE)	Transnational platform for professional exchange	Inter-governmental
3	France	Sciences Po Saint-Germain-en-Laye	*Diplôme inter-universitaire Renseignement et Menaces* (DIReM)	Academic
4	Germany	Bundesnachrichtendienst (BND)	*Nachrichtendienstliche Ausbildung;* SIGINT apprenticeship; dual-study programmes	Professional-military
5	Netherlands	Leiden University with NISA	MSc track in Intelligence and National Security	Academic
6	Norway	Norwegian Intelligence School (Etteretningsskolen)	Bachelor in Intelligence; master-level collaboration with King's College London	Professional-military
7	United Kingdom	Brunel University	MA in Intelligence and Security Studies	Academic
8	United Kingdom	Cambridge Security Initiative	International Security and Intelligence programme	Academic
9	United Kingdom	King's College London	MA in Intelligence and International Security (KCSI)	Academic
10	United Kingdom	University of Glasgow	Erasmus Mundus IMSISS	Academic
11	United States	National Intelligence University (NIU)	MSTI / MSSI / BSI	Academic

Table 2: Corpus B: the eleven benchmark intelligence education programmes referenced by SOU 2025:78.

its dominant domain (technical, formal, or informal). The nine cells provided the categories, so the coding was deductive.

Each of the eleven programmes in Corpus B was coded against the same nine cells using a three-level indicator. *Strong (❶)* indicates explicit and detailed coverage of the cell's competence content. *Partial (❷)* indicates implicit or limited reference without specificity. *Limited (❸)* indicates absence or invisibility in the available material. When a description addressed more than one domain or level, the dominant analytical focus determined the placement. The coding protocol was applied iteratively until the categories became analytically distinct.

The Corpus B programmes were identified through ten Boolean search strings in Elsevier Scopus,[41] returning 532 documents. The lead author then executed Mortenson and Vidgen,[42] computer-assisted literature review (CLR) process inside Claude Opus 4.6, using Python instead of R as the execution environment. Four filtering stages reduced the set to 29 papers on state or security intelligence education.

The analytical contribution arises from the comparison between the two matrices. The

Corpus A matrix shows what SOU 2025:78 requires. The Corpus B matrix shows what the benchmark programmes currently articulate. The gap analysis identifies where the inquiry states a requirement that existing programmes do not systematically address at the tactical and operational levels. However, limitations exist because the study relies on publicly available information.

In accordance with the principles of transparent and reproducible science, the lead author used Anthropic's Claude Opus 4.6 as a research assistant at four defined stages: literature screening, coding verification, figure generation, and drafting. All analytical judgements were made by the lead author, who assumes full responsibility for the text.

Findings

This section presents the findings from the application of the Intelligence Competence Framework to the two corpora. Section 4.1 reports the policy matrix derived from SOU 2025:78 (Corpus A). Section 4.2 reports the programme matrix derived from the eleven benchmark institutions (Corpus B). Section 4.3 reports the aggregate distributional pattern and its relationship to the Björck and Yngström finding.

The Policy Matrix: SOU 2025:78

SOU 2025:78 addresses competence and education across all nine cells of the framework's matrix, but with uneven depth and specificity.[43] *Table* 2 presents the Corpus A matrix with representative content coded into each cell. The inquiry concentrates its most detailed articulation in the formal domain. It provides substantial but less operationalised content in the informal domain. The technical domain is identified at a strategic level of abstraction without being translated into education requirements at the operational or tactical levels.

At the strategic level, the formal domain receives the most detailed treatment in the inquiry. SOU 2025:78 proposes a new foreign intelligence agency separated from the Swedish Armed Forces, restructured oversight mechanisms, and strengthened democratic

Level / Domain	Technical	Formal	Informal
Strategic	❷ Cloud, AI, cross-domain integration identified as priorities. Not operationalised as education requirements.	❶ New foreign intel agency, restructured oversight, democratic control. Legislative reform detailed.	❶ Personnel as strategic resource. Professional culture, loyalty, Nordic academy vision.
Operational	❷ Modernisation of technical systems referenced. Analytic tooling and workflows not specified.	❶ Joint education platform at FHS. Council for Intelligence Research. Cross-agency coordination.	❶ Cross-agency rotation, trust-building, personnel mobility between secret and open activities.
Tactical	❷ Specialist officers, interpreter training, language competence. Data provenance and tool limitations not articulated.	❷ Specialist officer programme reinstated. Norwegian model referenced. Handling drills not specified.	❷ Norwegian model for intelligence recipients. Structured tradecraft and bias mitigation not articulated.

Table 3. Corpus A Matrix: SOU 2025:78 coded against the Intelligence Competence Framework. ❶ *= strong explicit coverage,* ❷ *= partial or implied,* ❸ *= limited or absent.*

control through parliamentary and judicial review.[44] The inquiry further proposes a Council for Intelligence Research and Education to coordinate research priorities across the intelligence community. Legislative and organisational reform constitutes the inquiry's primary vehicle for change, with detailed descriptions of governance structures, reporting lines, and institutional mandates. The strategic-formal cell is the strongest cell in the Corpus A matrix.

The strategic-informal domain is also well articulated. The inquiry frames personnel as a "strategic resource" and emphasises loyalty, competence, and professional culture as prerequisites for a capable intelligence service.[45] The long-term vision of a Nordic intelligence academy implies a shared professional identity that extends beyond national boundaries. The inquiry explicitly addresses the need for cross-agency mobility, arguing that experience from multiple agencies should be a merit criterion for senior appointments within the intelligence system.

The strategic-technical domain is present but formulated at a high level of abstraction. The inquiry identifies cloud-based data processing, AI, and cross-domain integration as priority capability areas.[46] It states that the transition to cloud-based processing will deliver significant improvements for integrated processes between the services and should lead to increased resource efficiency. However, these references describe what technology should achieve for the intelligence system at a strategic level. They do not specify what competence intelligence professionals need in order to work effectively within such systems. The strategic-technical cell is coded ❷ *(partial)*: the domain is acknowledged but not operationalised.

At the operational level, the formal domain is again the strongest. The inquiry proposes that FHS develop a joint education platform offering both basic and specialised training for the intelligence and security services.[47] The platform is to be developed in cooperation with relevant Swedish universities, FMUndSäkC, and the intelligence services themselves. Active participation from the relevant agencies is described as a precondition for the development of and trust in the education. The operational-informal domain is articulated through the inquiry's emphasis on cross-agency rotation, shared experience, and the value of personnel mobility between classified and open activities.[48] Trust-building between services is explicitly addressed as a condition for the education platform's success.

The operational-technical domain receives partial treatment. The inquiry references the need to modernise technical systems for coordinating work and sharing information. It acknowledges that existing systems are outdated and require substantial investment. However, it does not specify analytic tooling, data integration architectures, or processing workflows as components of the education requirement.

At the tactical level, all three domains receive partial treatment. The inquiry identifies specific tactical needs: reinstating the specialist officer training in intelligence and security at FHS, expanding the interpreter school at FMUndSäkC into a national resource for the total defence, and developing language competence in Russian and Chinese.[49] It references the Norwegian model where the *Etteretningsskolen* trains intelligence recipients from state agencies in handling and use of intelligence products.[50] However, the inquiry does not articulate data provenance, tool limitations, or system-level error modes as tactical competence requirements.

The tactical level is where SOU 2025:78 is least specific about what intelligence professionals need to know and be able to

do. The inquiry's references to technology at this level address institutional resources — the interpreter school, the specialist officer programme, language training — rather than the technical competence that individual analysts require in their daily interaction with collection systems, processing tools, and dissemination platforms. This absence is notable because the inquiry's strategic-level identification of cloud-based processing, AI, and cross-domain integration implies a substantial shift in the technical environment in which tactical-level professionals will operate.

The Programme Matrix: Eleven Benchmark Institutions

Each of the eleven programmes referenced by SOU 2025:78 was coded against the nine cells of the framework's matrix. *Table 4* presents the aggregate coding matrix, reporting how many programmes scored ❶ *(Strong)*, ❷ *(Partial)*, and ❸ *(Limited)* in each cell.

The typology organises the findings by how closely each programme is connected to an intelligence service in practice. Academic programmes teach intelligence as a university subject. Students are admitted through normal university admission, the teaching is open and unclassified, and the link to operational services is limited. Professional-military programmes are built together with intelligence services and combine classroom teaching with practice inside those services. Intergovernmental platforms, such as the Intelligence College in Europe (ICE), operate above the national level and bring professionals from member states together for shared training and professional exchange. The three categories describe progressively closer ties between where a programme sits and where its graduates work. The tactical-technical cell is the point in the matrix where these ties matter most.

Among the academic programmes, the National Intelligence University (NIU) in the

Domain	❶	❷	❸	Description
Strategic				
Technical	2	6	3	Weak. Only DK (MICS) and DE (BND) score ❶ *(strong)*.
Formal	11	0	0	Universal strong coverage.
Informal	9	2	0	Near-universal strong coverage.
Operational				
Technical	3	7	1	Predominantly partial. FR, DK, and DE score ❶ *(strong)*.
Formal	11	0	0	Universal strong coverage.
Informal	10	1	0	Near-universal strong coverage.
Tactical				
Technical	1	5	5	Weakest cell. Only DE (BND SIGINT) scores ❶ *(strong)*.
Formal	3	8	0	Predominantly partial. NO, DE, and FR score ❶ *(strong)*.
Informal	5	6	0	Mixed. NO, DK, King's, NL, and FR score ❶ *(strong)*.

Table 4. Corpus B Aggregate Matrix: distribution of ❶ (Strong) / ❷ (Partial) /❸ (Limited) ratings across eleven programmes for each cell of the Intelligence Competence Framework.

United States offers the broadest coverage across the matrix.[51] NIU operates directly under the Office of the Director of National Intelligence and serves the entire U.S. Intelligence Community. Its Master of Science and Technology Intelligence (MSTI) programme includes concentrations in cyber intelligence, data science in intelligence, emerging technologies, and counterproliferation. These concentrations populate the strategic-technical and operational-technical cells with programme-level content.

However, the MSTI describes these areas as thesis research domains and programme objectives, not as hands-on tool-based training with specific systems. The tactical-technical rating is ❷ *(partial)*. NIU's Master of Science of Strategic Intelligence (MSSI) brings together students from across the entire Intelligence Community, including its military elements. The MSSI includes concentrations in collection and analysis, counterintelligence, strategic intelligence in special operations, and IC leadership and management. The cross-agency student body is itself an operational-informal design feature: trust and coordination norms are embedded in the learning environment, not taught as abstract principles. NIU also offers a Bachelor of Science in Intelligence and a Certificate in Intelligence Studies.[52]

The Cambridge Security Initiative and King's College London represent the UK academic model focused on strategic-level engagement between practitioners and scholars. Both are strong in the strategic-formal and strategic-informal cells. Cambridge's International Security and Intelligence programme is chaired by the former Chief of the Secret Intelligence Service and addresses democratic oversight, state secrecy, the intelligence-policy interface, and ethical considerations.[53] King's MA in Intelligence and International Security covers intelligence collection, assessment, and the producer-consumer relationship. The King's Centre for the Study of Intelligence (KCSI) maintains research priorities in regional approaches to intelligence, perceptions of intelligence, and state-based threats and information manipulation. KCSI brings together scholars, doctoral researchers, practitioners, and visiting fellows from four continents.[54] However, neither programme describes technical tool-based training, simulation exercises, or system-level competence development. The tactical-technical cell scores ❸ *(limited)* for both institutions.

Brunel University's MA in Intelligence and Security Studies follows a similar strategic-informal orientation and adds a practitioner engagement layer. Staff have contributed to UK Joint Intelligence Doctrine, provided evidence to parliamentary committees, and advised on the Integrated Review of Security, Defence, Development and Foreign Policy. The Centre's Deputy Director has delivered professional development courses to the EU Intelligence Centre and the governments of Norway, Latvia, France, and the United Arab Emirates.[55] The tactical-technical cell scores ❷ *(partial)*, based on explicit references to structured analytical tools and their practical application.

The University of Glasgow's Erasmus Mundus International Master in Security, Intelligence and Strategic Studies (IMSISS) spans four European universities and is structured around mobility periods across two years.[56] The multi-university mobility design populates the operational-informal cell through cross-cultural professional networking and exposure to different national perspectives on intelligence. However, the programme does not describe technical systems training at any level. The tactical-technical cell scores ❸ *(limited)*.

Among the professional-military programmes, the Danish Master of Intelligence and Cyber Studies (MICS) is the strongest Nordic programme in the technical domain. MICS is a joint programme between the Danish Defence University (Forsvarsakademiet) and the University of Southern Denmark, and addresses the cyber domain in a security-political context.[57] The programme includes twin specialisation tracks: intelligence and cyber. It builds competence through practice-oriented expertise combined with an analytical track, with focus on intelligence and cyber analysis, including hybrid warfare.[58] MICS populates the strategic-technical, operational-technical, and tactical-informal cells with explicit content. However, specific technical exercises or tool-based training are not described in the publicly available material. The tactical-technical rating is ❷ *(partial)*.

The Norwegian Intelligence School (*Etteretningsskolen*) is distinctive for its professional authority (*fagmyndighet*) function: the school exercises professional authority for intelligence on behalf of the Chief of the Norwegian Intelligence Service.[59] It sets unified competence requirements for intelligence across the entire Norwegian Defence. It issues and revises intelligence doctrine, including the Norwegian Intelligence Doctrine and the *Bestemmelse for Etterretning* (BEF). It advises on capability projects related to intelligence. This institutional function populates the tactical-formal cell with ❶ *(strong)* — the school does not only teach handling constraints, it defines them for the entire defence sector.

The Centre for Intelligence Studies at the school pursues five prioritised research areas: intelligence as decision support, intelligence and warning, use of academic theory and methods in intelligence analysis, hard intelligence targets, and intelligence and digital transformation.[60] The school collaborates with King's College London for master-level education. It also offers training for intelligence recipients within state agencies, a function that SOU 2025:78 explicitly references as a model for Sweden.[61]

The German BND programme is the only programme scoring ❶ *(strong)* in the tactical-technical cell. The BND offers three distinct training pathways: a general intelligence apprenticeship (*nachrichtendienstliche Ausbildung*), a SIGINT apprenticeship in electronic reconnaissance (*Fernmelde- und Elektronische Aufklärung*), and a physical security apprenticeship (*Fachkraft für Schutz und Sicherheit*).[62] The two-year general apprenticeship consists of 14 months of practical placements and 10 months of theoretical instruction. Trainees rotate through multiple BND departments, gaining exposure to both operational and analytical functions.

The SIGINT pathway includes hands-on training in electronic reconnaissance with practical placements in technical departments. It is supported by dual-study programmes in IT security, informatics, and data science at the bachelor level, producing graduates with both academic qualifications and operational competence.[63] The joint training with the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV) at the Centre for Intelligence Training and Professional Development (*Zentrum für Nachrichtendienstliche Aus- und Fortbildung*, ZNAF) includes constitutional law, administrative law, and public law modules. The BND programme's breadth across the matrix reflects its institutional character as a service-internal training system.

The Netherlands programme (NISA and Leiden) covers the formal domain comprehensively. Leiden's MSc track in Intelligence and National Security situates intelligence

in its political, societal, and bureaucratic contexts.[64] The track introduces students to intelligence and security services, their modus operandi, their interaction with the surrounding world, and the challenges they face. Students learn to weigh hypotheses, detect patterns, and derive logical conclusions from incomplete information.

NISA's membership comprises approximately 90 members including academics, media representatives, and current or former employees of the AIVD, MIVD, police, and private organisations.[65] NISA conducts quarterly meetings and organises international conferences. The tactical-informal cell scores ❶ *(strong)* due to Leiden's emphasis on analytical reasoning under uncertainty. The technical domain scores ❷ *(partial)* across all levels.

Among intergovernmental platforms, the Intelligence College in Europe (ICE) operates as a platform for professional and academic exchange, not as a degree-granting programme. ICE was launched in Paris on 5 March 2019 and has evolved to include 28 member countries and 3 partner countries.[66] Its primary function is cultural diffusion at the strategic-informal level: building a common strategic intelligence culture across European member states. The strategic-formal cell scores ❶ *(strong)* based on ICE's engagement with national intelligence strategies, intelligence oversight, and intelligence policy in democratic contexts. ICE's 2026 academic conference, hosted under the German presidency at the University of the Bundeswehr in Munich, addresses the theme "Science and Intelligence in Europe."[67] The conference programme lists computational OSINT, data-driven decision support systems, visual intelligence analysis, and complex system analysis as indicative topics. However, ICE does not deliver structured technical training through its own programmes.

The French DIReM at Sciences Po Saint-Germain-en-Laye is the only programme offering explicit OSINT tool training within a broader intelligence education context.[68] The *intelligence monitoring and data analysis* module (*veille et analyse des données*) teaches geolocation, reverse image search, and structured analysis techniques alongside political and sociological perspectives. The programme includes dedicated modules on intelligence law (droit du renseignement), islamist radicalisation, political radicalism, organised crime economics, and operational intelligence practice. Practitioner lecturers from the DGSI, DGSE, and armed forces contribute to instruction in the security-cleared environment of the French Intelligence Academy (*Académie du renseignement*).[69]

The Distributional Pattern

The aggregate finding reveals a structural asymmetry across the nine cells of the framework's matrix (Figure 3). The formal domain is the most densely populated: all eleven programmes score *Strong* in both the strategic-formal and operational-formal cells. The informal domain is similarly strong at the strategic and operational levels, with 9 and 10 programmes scoring *Strong* respectively. The concentration shifts at the technical domain.

At the strategic-technical cell, only two of 11 programmes score *Strong* (MICS and BND). Six score *Partial* and three score *Limited*. At the operational-technical cell, three programmes score *Strong* (DIReM, MICS, and BND), seven score *Partial*, and one scores *Limited*. At the tactical-technical cell — the intersection of technical systems and tactical execution — only one programme scores *Strong* (BND SIGINT training). Five

score *Partial* and five score *Limited*. This is the weakest cell in the entire matrix.

The tactical level as a whole is weaker than the strategic and operational levels. The tactical-formal cell is predominantly partial, with three programmes scoring *Strong* (Etteretningsskolen, BND, DIReM) and eight scoring *Partial*. The tactical-informal cell is mixed, with five programmes scoring *Strong* (Etteretningsskolen, MICS, King's, Leiden, DIReM) and six scoring *Partial*. The pattern is consistent across programme types but manifests differently in each.

Academic programmes — NIU, Cambridge, King's, Glasgow, Brunel, and Leiden — concentrate in the formal and informal domains at the strategic and operational levels. Their institutional purpose is to produce strategic thinkers, policy-literate analysts, and scholars who understand the intelligence enterprise. The technical domain appears in these programmes primarily as a topic of study rather than as a competence to be developed through hands-on training.

Professional-military programmes — MICS, Etteretningsskolen, and BND — extend further into the technical domain but with significant variation. The BND is the only programme that scores *Strong* in the tactical-technical cell, reflecting its apprenticeship model with practical placements in technical departments. MICS addresses the cyber domain explicitly but does not describe tool-specific training in public material. Etteretningsskolen's strength is in the formal domain through its professional authority function rather than in technical system training.

Intergovernmental platforms — ICE and Cambridge — operate primarily at the strategic-informal and operational-informal levels. Their institutional function is networking, cultural exchange, and shared professional development. They do not deliver structured technical or formal training at the tactical level.

Figure 3 presents the aggregate distributional pattern across the framework's matrix. The aggregate pattern is the structural inverse of the Björck and Yngström finding in information security research. In the SEC 2000 proceedings, 83 per cent of papers concentrated in the technical domain while formal and informal domains were underrepresented. In the intelligence education programmes analysed here, the pattern is reversed. Aggregated across all three levels, the technical domain receives *Strong* ratings in 6 of 33 possible cells (18 per cent). The formal domain receives *Strong* ratings in 25 of 33 cells (76 per cent) and the informal domain in 24 of 33 cells (73 per cent). The ratio between the technical domain and the formal/informal domains — approximately 1:4 — quantifies the structural asymmetry that the framework was designed to detect. The asymmetry deepens progressively from strategic (2 of 11 *Strong*) through operational (3 of 11 *Strong*) to tactical (1 of 11 *Strong*). Five of eleven programmes score *Limited* in the tactical-technical cell.

The three programmes that score most broadly across the technical column — BND, MICS, and DIReM — share a common characteristic: each integrates technical content with professional practice rather than treating technology as a separate academic subject. The BND achieves this through service-internal apprenticeship with practical placements. MICS achieves it through twin specialisation tracks that link cyber and intelligence within the same programme. DIReM achieves it through practitioner-led OSINT instruction within a broader sociological and legal framework.

The tactical-technical absence in public programme descriptions has three possible explanations. The first is that the content is

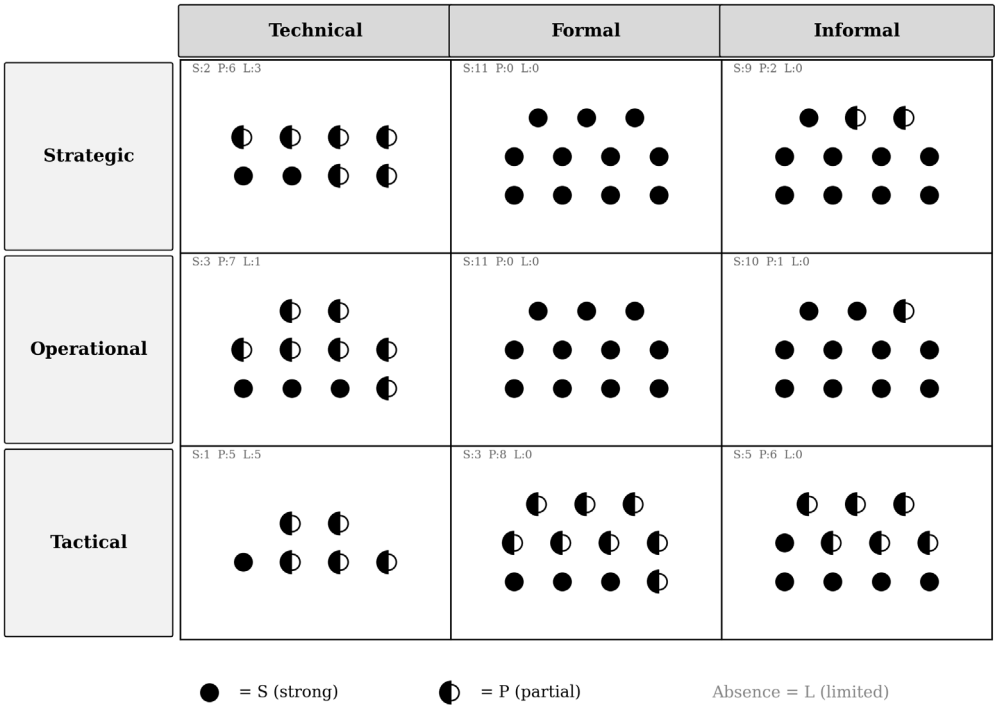

Figure 3: Intelligence Competence Framework dot-plot: distributional concentration of eleven intelligence education programmes across the 3×3 matrix. Filled circles (●) indicate S-rated programmes; half-filled circles (◐) indicate P-rated programmes. The density contrast between the formal/informal columns and the technical column — particularly at the tactical row — is the central finding.

protected as tradecraft: the tactics, techniques, and procedures exist, but intelligence services keep them out of public descriptions. The second is that officers learn this content on the job: services develop tactical-technical competence after graduation through their own internal training, and academic and professional-military programmes therefore need only give students the basics. The third is that the competence is not developed anywhere at sufficient scale — neither taught publicly, nor delivered through classified training in enough places, nor clearly located inside the education-training pipeline.

The three explanations lead to different decisions for the proposed academy. Under the first, the academy needs to align its classified track with the internal training of Must, FRA, and Säkerhetspolisen. Under the second, the academy needs to define what the basics of tactical-technical competence look like and leave the advanced content to the services. Under the third, the academy has a real supply gap to close. Furthermore, the three explanations are not mutually exclusive: classified training may cover one level, on-the-job practice another, and a gap may still remain. The framework does not resolve which explanation applies. However, it makes the question visible and directs the analysis toward the way Swedish intelligence services and education institutions would need to work together to answer it.

Analysis and Implications

The answer to the research question — *what structural patterns characterise the distribution of competence across intelligence education programmes referenced by SOU 2025:78, and where do asymmetries exist between what the inquiry requires and what existing programmes articulate?* — is a structural asymmetry in which the technical domain is systematically underarticulated relative to the formal and informal domains. The asymmetry deepens progressively from strategic through operational to tactical levels. The following analysis addresses the implications of this finding for the technical-domain deficit as a structural pattern (Section 5.1), for the proposed Swedish intelligence academy (Section 5.2), for the Nordic cooperation ambition articulated in SOU 2025:78 (Section 5.3), and for the limits of the framework itself (Section 5.4).

The Technical-Domain Deficit as a Structural Pattern

The finding that formal and informal domains dominate intelligence education is not an accident of programme selection. The pattern is consistent across programme types — academic, professional-military, and intergovernmental — and across national contexts spanning the United States, the United Kingdom, Scandinavia, Germany, the Netherlands, France, and the European intergovernmental level. The consistency of the pattern across such diverse institutional settings suggests that the asymmetry reflects something structural about how intelligence education has developed as a field, rather than an incidental feature of individual programme design.

Several factors may contribute to this structural pattern. Intelligence studies as an academic discipline grew out of history and political science departments, which are methodologically oriented toward the formal and informal domains. The study of intelligence organisations, oversight mechanisms, legal frameworks, intelligence failures, and the intelligence-policy interface constitutes the intellectual core of the discipline. These are formal-domain and informal-domain topics. Technical systems — how signals are intercepted, how data is processed, how AI models generate outputs — are typically treated as operational details rather than as objects of academic inquiry. The consequence is that academic programmes reproduce the disciplinary orientation of intelligence studies rather than the competence requirements of intelligence practice.

Professional-military programmes go part of the way to correcting this gap because they are designed together with intelligence services. The BND's apprenticeship model, the MICS twin-track design, and the Etteretningsskolen's role as the professional authority for intelligence across the Norwegian Defence all reflect close links between the classroom and the intelligence service that academic programmes typically do not have. However, the professional-military programmes differ from each other in how deeply they cover the technical domain. The MICS treats cyber as a subject of study but does not describe training in specific technical tools. The Etteretningsskolen is strong in the formal domain because it sets doctrine, not because it trains officers on technical systems. Only the BND, with its SIGINT apprenticeship and dual-study programmes in IT security and informatics, systematically covers the tactical-technical cell.

The overall pattern across the three categories tells its own story. The tactical-technical gap remains even where the connection between the classroom and the intelligence service is strongest, as in the profession-

al-military category. The gap widens in the academic category, where this connection is weakest. The closest link in the matrix — the BND's own internal apprenticeship — covers the cell only partially at the level of the programme as a whole. Therefore, the teaching methods available to an academic programme cannot close the cell on their own; the proposed Swedish academy also needs a formal agreement with the intelligence services.

> *The consequence is that academic programmes reproduce the disciplinary orientation of intelligence studies rather than the competence requirements of intelligence practice.*

The German case needs a separate explanation. The BND is the only programme in the matrix that scores ❶ *(strong)* in the tactical-technical cell. Three institutional factors may contribute. Germany's *duale Ausbildung* tradition combines classroom teaching with structured work placements across many skilled trades and professions, and the BND's apprenticeship programmes follow this established pattern. German federalism requires a clear division of responsibilities between federal and state-level security services, which is why the BND explicitly maps which competences sit at which level. The BND's own internal training system gives it direct control over the tactical-technical cell that a university-hosted programme does not have. The implication is not that Sweden should adopt the German model in full. However, the implication is that the tactical-technical cell is shaped by which institution controls the training, not by how the teaching is designed: where the service controls the training, the cell is populated; where the university controls the teaching, it is not.

The Coulthart and Crosston mapping of 17 American intelligence programmes reached a parallel finding: technical expertise and engagement/collaboration were the least addressed of the six ODNI core competencies. The Ramsay and Macpherson assessment confirmed that even US graduate programmes have not systematically integrated quantitative analysis courses. The Berger, Borghoff, Conrad, and Pickl argument from the German ICE module experience stated explicitly that the supply of intelligence practitioners with data science knowledge is of utmost importance — a recommendation that implies the supply is currently insufficient. The ICF reveals that this insufficiency is not randomly distributed across the competence landscape. It concentrates in the technical domain and deepens at the tactical level, where analysts interact with tools, data, and systems under operational conditions.

The inverse relationship to the Björck and Yngström finding is analytically significant. In information security research, the technical domain dominated at the expense of the formal and informal domains. In intelligence education, the formal and informal domains dominate at the expense of the technical domain. Both asymmetries represent structural imbalances in how a field distributes its attention across the socio-technical spectrum. The SHA's diagnostic value lies in making such imbalances visible regardless of the direction in which they run.

The framework does not prescribe what the correct distribution should be. Different intelligence functions may require different distributions. A strategic intelligence adviser may need stronger coverage in the formal and informal domains than in the technical

domain. A tactical SIGINT operator may need the reverse. The framework makes the actual distribution visible so that decision-makers and education designers can assess whether it matches the demands of the operational environment they are preparing professionals for.

The tactical-technical cell merits particular attention. This is the competence intersection where intelligence professionals interact with technical systems under time pressure. It encompasses interpreting sensor data, evaluating data provenance, understanding tool limitations, identifying error modes, and making time-sensitive judgements about technical artefacts. Five of eleven programmes score ❸ *(limited)* in this cell. Only the BND's SIGINT apprenticeship scores ❶ *(strong)*.

The implication is that for most programmes, tactical-technical competence is handled in one of three ways. Officers are expected to learn it on the job. Or it is delivered through classified training that this study cannot see. Or it is not taught anywhere in the education system in an organised way. Each of these three possibilities leads to different outcomes. If officers learn it on the job, then intelligence services pay the full cost of developing it themselves — which can work for services with large internal training, but is too expensive for smaller services. If it is delivered through classified channels, then the education system and the training system are not connected at the tactical-technical level. If it is not taught anywhere in an organised way, then the competence gap is real and may widen as technical systems become more complex.

The gap is likely to remain for as long as intelligence services and education institutions do not agree on how to develop the competence together. The services own the tactical-technical problem. The universities carry the formal tools to solve it. Both sides invest their time, curriculum, staff, and classified access only when the side that owns the problem and the side that can solve it work together.[70]

In an environment where AI-enabled systems are expected to be integrated into every stage of the intelligence cycle, this gap may have operational consequences. The CIA's Snow Globe experiment demonstrated that participants who lacked prior digital experience became frustrated and disengaged when AI tools failed to meet expectations. The participants could not articulate what they wanted from an AI assistant before they experienced what the tool could offer. This suggests that digital competence is not merely a skill set that can be listed in a curriculum. It is a mode of engagement with technology that must be developed through structured, repeated exposure.

The Emergent Intelligence framework from the DDI specifies that intelligence officers must develop technical skills alongside advanced reasoning, ethical decision-making, and strategic communication to collaborate with AI systems. This is a multi-domain competence requirement. Technical skills fall in the technical domain. Ethical decision-making falls in the formal domain. Strategic communication falls in the informal domain. All three must be integrated within the same individual and the same team. The ICF reveals that existing programmes develop the formal and informal components of this requirement but may not systematically develop the technical component — particularly at the level where the integration actually occurs.

Implications for a Swedish Intelligence Academy

SOU 2025:78 proposes that FHS develop a joint education platform with a long-term

objective of a Nordic intelligence academy. Swedish intelligence services — Must, FRA, and Säkerhetspolisen — are likely to engage and work with NATO allies and Five Eyes partners, which means the proposed academy may continue to teach Anglo-American methods, doctrine, and vocabulary as the operational standard for partner interoperability. How SOU 2025:78 describes competence, coded in the Corpus A matrix, is strongest in the formal domain. The inquiry describes governance, organisational design, and legislative reform in detail. The inquiry also covers the informal domain well, emphasising professional culture, trust, and cross-agency rotation. The inquiry names the technical domain at the strategic level — cloud, AI, and cross-domain integration. However, it does not turn this into a concrete teaching requirement at the operational or tactical levels.

The inquiry acknowledges the technological imperative but does not specify how it translates into competence. What does an analyst need to know about data provenance in order to assess the reliability of a cloud-based collection stream? What does a planner need to understand about system limitations to avoid building operational designs on capabilities that do not yet function as advertised? What does a tactical operator need to understand about tool error modes to avoid misinterpreting outputs under time pressure? These questions are not addressed in SOU 2025:78. They are the questions that populate the technical column of the ICF matrix at the operational and tactical levels.

The gap analysis — overlaying the Corpus A matrix on the Corpus B aggregate matrix — reveals that existing benchmark programmes do not systematically address this gap either. If the proposed Swedish academy draws its curriculum design from these programmes, it may reproduce the structural asymmetry rather than resolve it. The formal and informal domains are well served by existing models. Cambridge, King's, and Brunel offer education in the strategic-formal and strategic-informal domains that is among the strongest in the world. Glasgow and Leiden provide strong operational-informal and tactical-informal coverage through multi-institutional mobility and analytical reasoning training. The Norwegian Intelligence School demonstrates how a professional authority function can structure the formal domain across an entire defence sector.

> *The practical consequence for the proposed Swedish academy is that curriculum design should explicitly populate the technical column of the ICF matrix at all three levels.*

However, the tactical-technical cell — where the proposed Swedish academy would need to prepare analysts for AI-enabled operations — remains the weakest point across all benchmark programmes. The NSCAI report's recommendation that intelligence professionals be enabled with baseline digital literacy addresses this gap at the strategic level but not at the operational or tactical levels where education design determines what professionals actually learn to do.

The Snow Globe experiment showed, at the operational level of the framework, that prior digital experience shapes how well intelligence officers use AI assistants. The Emergent Intelligence framework states, as a matter of principle, that officers need to develop competence in data science, machine learning, and advanced analytics, as well as in ethical decision-making and strategic communication. Both sources point to the same conclusion: technical-domain compe-

tence is not an extra subject only for staff who already work in technical roles. It is a basic requirement for doing intelligence work in times dominated by AI.

The practical consequence for the proposed Swedish academy is that curriculum design should explicitly populate the technical column of the ICF matrix at all three levels. At the strategic level, this means developing understanding of how national analytic infrastructure shapes strategic options. What does cloud-based processing enable and constrain? How does system reliability affect the timeliness of decision support? At the operational level, this means integrating analytic tooling, data processing workflows, and secure communication systems into the education of intelligence planners and analysts — not only of technical specialists. At the tactical level, this means developing competence in data provenance, tool limitations, system mapping, and time-sensitive technical interpretation.

The three programmes that score most broadly across the technical column — BND, MICS, and DIReM — offer instructive models. Each integrates technical content with professional practice rather than treating technology as a separate academic subject. The BND achieves this through service-internal apprenticeship with practical placements in technical departments. MICS achieves it through twin specialisation tracks that link cyber and intelligence within the same programme. DIReM achieves it through practitioner-led OSINT instruction within a broader sociological and legal framework. A Swedish academy that draws on these integrated models rather than on the purely academic model may achieve better coverage of the technical domain while maintaining the formal and informal strengths that existing European programmes already provide.

Who is admitted to a programme is part of what that programme teaches. Most Swedish advanced-level information-security programmes require 180 credits in computer and systems science to apply. Only DSV/SU admits students from other academic backgrounds to advanced information-security studies.[71] A Swedish intelligence academy that keeps this narrow technical entry requirement will recruit only students who already work in the technical domain. Therefore, the integrated model this article recommends will fail because of who it selects, not because of how it teaches. The design question is not only what to teach but who is admitted to learn it. DSV/SU's SHA-based model offers one workable template for the academy. It combined open admission with technical, organisational, legal, and management content from the start.

Evidence of unmet demand is concrete. CATS' last master's course received over 550 applicants for 30 places, a ratio that indicates strong student interest in intelligence education within the existing Swedish higher education system.[72]

The proposed academy also operates inside an active Swedish network of institutions that SOU 2025:78 does not discuss in a systematic way. Campus totalförsvar links FHS with Örebro University and Luleå University of Technology. Cybercampus Sweden has the stated mission of research, innovation, and education for cyber security and defence. Lund University runs courses in security-relevant areas. These structures can be seen as partial versions of the new kind of organisation that Yngström proposed at FHS/CATS in 2018 — collaboration between a purpose-built body and existing research and education institutions. Therefore, the design question for the academy is how it can fit inside these structures, not how to build something in parallel. An academy that

duplicates what Campus totalförsvar and Cybercampus Sweden already do will use up scarce Swedish higher-education resources without closing the technical-domain deficit that the ICF identifies.

The Nordic Cooperation Question

SOU 2025:78 sets out a long-term vision of a Nordic intelligence academy. The Petersen and Rønn analysis found that Scandinavian intelligence education is heavily shaped by Anglo-American methods and historical cases, with limited adaptation to Nordic society. This observation suggests that a Nordic academy would need to deliberately work on adapting its teaching to the Nordic context. Teaching about Nordic democratic norms, oversight traditions, and societal institutions — rather than relying on Anglo-American frameworks as universal templates — would be a prerequisite for a genuinely Nordic institution.

The problem of adapting teaching to the Nordic context has two sides: one in the formal domain, and one in the informal domain. In the formal domain, Nordic countries share the same broad traditions of oversight and governance — parliamentary control, judicial review, and ombudsman institutions — but their specific intelligence laws are different. Swedish intelligence law is not identical to Norwegian intelligence law. Danish oversight arrangements differ from Finnish ones. A Nordic academy operating in the formal domain would need either to handle these differences or to focus on the shared principles that all Nordic systems use. Therefore, this is a design problem for institutions that can be solved, but it requires explicit attention.

In the informal domain, the Nordic countries share a society built on high levels of trust between citizens and the state. This shared model shapes what citizens expect from government transparency, from civic participation, and from the relationship between intelligence services and the public. These shared informal norms could be the foundation of a distinctively Nordic intelligence culture, built on top of the Anglo-American tradition that currently provides the operational standard for intelligence education. The Petersen and Rønn finding is that Scandinavian programmes currently copy Anglo-American teaching material and have not yet developed material adapted to the Nordic context. This suggests that the additional Nordic foundation has not yet been developed.

The Gruszczak analysis of the Intelligence College in Europe is relevant here. The ICE experience shows that shared educational frameworks only work when incentives from institutions at the top align with commitment from the people involved. Motivations that come from below, driven only by national interests, have limited impact on shaping cooperation across countries. A Nordic intelligence academy that operates without incentives from institutions at the Nordic level may remain a Swedish platform with Nordic participation, and not a genuinely integrated Nordic institution. A mandate from the Nordic Council, or a multilateral agreement among the Nordic states, could provide the institutional framework that the ICE experience suggests is necessary.

The Dylan, Goodman, Jackson, Jansen, Maiolo, and Pedersen analysis documented how the Norwegian Intelligence School solved the problem of integrating professional intelligence practice with academic teaching at the national level. The Norwegian model demonstrates that it is possible to design professional intelligence education that meets national standards for academic accreditation. However, it does not demonstrate that the same solution works across

national borders without careful institutional design that takes account of differences in legal frameworks, oversight traditions, and professional cultures.

These differences sit in the formal and informal domains — exactly where the ICF analysis shows existing programmes are already strong. The technical domain, by contrast, may be more transferable across national boundaries. Technical systems, data standards, and analytic tools operate across jurisdictions. Shared NATO systems, common intelligence-sharing platforms, and interoperable technical infrastructure already create a degree of technical standardisation that has no equivalent in the formal and informal domains.

The claim that cooperation in the technical domain is possible has a working example inside the Nordic region. The University of Agder proposed a two-year master's programme in cyber security in response to NOU 2015:3. The programme offers two tracks after a common first year — security management and cyber security — and draws staff from the faculty of mathematics and natural science and the faculty of social science. It carries export-control classification and is taught primarily in Norwegian. Students are security-cleared during the programme and supported by specialised laboratories and approximately 8.5 full-time academic positions.

A Nordic precedent also exists for the pracademic model. CATS developed a doctoral programme in collaboration with Åbo Akademi University in Finland, designed for civilian intelligence professionals pursuing second careers in research, and drew on support from military intelligence and the security service.[73]

Therefore, technical education that runs across faculties, is security-classified, and is export-controlled can be delivered inside a single Nordic university, without a new transnational organisation. However, SOU 2025:78 does not mention Agder in its list of benchmark programmes. The fact that SOU 2025:78 does not mention Agder is itself informative: the Nordic programme closest in how it is structured to what the inquiry proposes to build sits outside its frame of benchmark programmes.

A Nordic intelligence academy may therefore find that cooperation in the technical domain is easier to achieve than harmonisation of the formal domain. Joint technical training — shared cyber ranges, common instruction in analytic tools, and coordinated courses on OSINT methodology — could serve as a practical starting point for deeper institutional integration. Furthermore, this approach would also address the structural weakness identified by the ICF analysis: if the technical domain is the weakest point in existing European intelligence education, then making it the entry point for Nordic cooperation serves both goals at once — cooperation between the Nordic states, and development of the competence that the ICF identifies as weakest.

Limitations of the Framework

The ICF identifies distributional patterns. It does not measure educational outcomes, assess pedagogical quality, or prescribe curriculum content. The ❶ *(strong)* / ❷ *(partial)* / ❸ *(limited)* coding is based on publicly available descriptions. Classified curricula may contain technical content not visible to this analysis. The BND's SIGINT apprenticeship is the only programme scoring ❶ *(strong)* in the tactical-technical cell — but this may partly reflect the BND's greater transparency about the content of its technical training, and not necessarily an absolute difference in pedagogical coverage.

The analysis is also bounded by the selection of programmes. The eleven institutions coded are those that SOU 2025:78 references as benchmarks. Other intelligence education programmes exist — including classified training programmes that services run internally in Sweden, Finland, and elsewhere — that are not captured by this analysis. Therefore, the framework's diagnostic value is strongest when applied to a defined and bounded set of institutions, and not as an instrument for universal survey use.

The anchoring of the search strategy on the term *intelligence* is itself a source of bounded coverage. Education that develops relevant technical competence under labels such as cyber security, data science, and signals engineering sits outside the corpus. The framework may therefore understate the competence available to Swedish intelligence services when viewed across the full socio-technical domain. The framework could also produce different results if applied by different coders. The distinction between S and P depends on a judgement about whether programme descriptions are explicit and detailed or implicit and general. This judgement is informed by the cell definitions in *Table 1* but involves room for interpretation.

Future research could assess how consistently different coders reach the same result by having multiple analysts apply the framework to the same programme descriptions independently. Such an assessment would strengthen the methodological foundation for using the ICF in comparative studies. Future research could apply the framework to classified programme descriptions where access is granted. Graduate surveys could assess whether the distributional pattern correlates with competence gaps that practitioners themselves report. Applying the framework over time — coding the same programmes at two or more time points — would reveal whether the distributional pattern is static or whether programmes are converging toward greater technical-domain coverage. The current analysis captures a single cross-section. Whether the Björck-Yngström asymmetry will correct itself over time or will remain in place in intelligence education is an open question.

Conclusions

This article addressed the following question: *what structural patterns characterise the distribution of competence across intelligence education programmes referenced by SOU 2025:78, and where do asymmetries exist between what the inquiry requires and what existing programmes articulate?* The ICF — combining the MLMD's three levels with Yngström's three domains — revealed a structural asymmetry. The formal and informal domains are universally covered across the eleven programmes analysed. The technical domain is underarticulated, with the asymmetry deepening from strategic through operational to tactical levels. The tactical-technical cell — where analysts interact with systems under time pressure — is the weakest point in the entire matrix. Only one of eleven programmes scores ❶ *(strong)* in this cell. Five score ❷ *(partial)*, and five score ❸ *(limited)*. The distribution shows that the technical domain is addressed at the tactical level in about half the programmes, but in strong detail in only one.

SOU 2025:78 identifies the technological imperative at the strategic level but does not operationalise it as an education requirement at the operational or tactical levels. A Swedish intelligence academy modelled on existing European and American programmes may inherit this asymmetry unless technical-domain competence is treated as a structural

requirement at all three levels — not as a specialist supplement for technically oriented personnel.

The ICF provides the diagnostic instrument for monitoring whether future curriculum design addresses this imbalance. The framework does not prescribe what to teach. It identifies where attention is concentrated and where it is absent — allowing education designers, policy-makers, and intelligence professionals to make informed decisions about competence distribution across the intelligence education system.

Acknowledgements

Professor emerita Louise Yngström at the Department of Computer and Systems Sciences, Stockholm University, reviewed the manuscript and contributed substantive input on the Systemic-Holistic Approach, on Nordic institutional precedents, and on the relationship between open academic structures and national-interest competence supply. The authors are grateful for her engagement with the text.

Dr Gazmend Huskaj is Head of Global Cyber and Security Policy at the Geneva Centre for Security Policy (GCSP). His research addresses intelligence, offensive cyberspace operations, and the design of national cyber capabilities. He previously served as Director of Intelligence on cyber-related matters at the Swedish Armed Forces, with more than five years of field experience in conflict and post-conflict environments.

Stefan Axelsson was Sweden's first professor of digital forensics. He is Professor of Digital Forensics and Cybersecurity at the Department of Computer and Systems Sciences, Stockholm University. He researches and teaches in cyber security, digital traces, and cybercrime. His work focuses on how technical methods support law enforcement investigations and how individuals, organisations, and public institutions can defend themselves against digital threats.

Notes

1. *En reformerad underrättelseverksamhet*, SOU 2025:78, Statens offentliga utredningar, Stockholm 2025.
2. Ibid.
3. National Security Commission on Artificial Intelligence: *Final Report*, Washington D.C. 2021.
4. Ibid.
5. Brennan, Andrea; Grunspan, Rachel; Hogan, Daniel; Smith, Jessica D. and VanderVeen, Elizabeth: "Snow Globe Multi-Player AI System: Lessons from Human-AI Teaming in War Games", *Studies in Intelligence*, vol. 69, no 4, December 2025, p. 15–21.
6. "Emergent Intelligence: Spycraft and Intelligence in the AI Era", *Studies in Intelligence*, vol. 69, no 4, December 2025, p. 7-13.
7. SOU 2025:78.
8. Ibid.
9. Försvarshögskolan, "Campus totalförsvar," accessed 18 April 2026, *https://www.fhs.se/samverkan/campus-totalforsvar.html*; Luleå tekniska universitet, "Campus Total Defence," accessed 18 April 2026, *https://www.ltu.se/en/collaboration/campus-total-defence*. The initiative is led by Försvarshögskolan, Örebro universitet, and Luleå tekniska universitet, with a Government investment of SEK 30 million announced in Budgetpropositionen 2025.
10. Cybercampus Sverige, "About us," accessed 18 April 2026, *https://www.cybercampus.se/en/about*; KTH, "Inauguration of Sweden's first cyber campus," accessed 18 April 2026, *https://www.kth.se/en/om/nyheter/centrala-nyheter/sveriges-nya-cybercampus-invigt-1.1314934*. Cybercampus Sweden is a national initiative founded by KTH, RISE, and the Swedish Armed Forces, with a Government investment of SEK 100 million; its stated mission is research, innovation, and education for cybersecurity and defence.
11. Lund University, Department of Political Science, "Programmes and courses," accessed 18 April 2026, *https://www.svet.lu.se/en/education/programmes-and-courses*. The Department explicitly offers teaching in intelligence analysis at first-, second-, and third-cycle (research) levels.
12. SOU 2025:78.
13. Ibid.
14. Ibid.
15. Ibid.
16. SOU 2025:78.
17. Ibid.
18. Ibid.
19. Coulthart, Stephen and Crosston, Matthew: "Terra Incognita: Mapping American Intelligence Education Curriculum", *Journal of Strategic Security*, vol. 8, no 3, 2015, p. 46-68.
20. Petersen, Karen Lund and Rønn, Kira Vrist: "Intelligence Education for the Future: What Kind of Future is the Scandinavian Intelligence Community Prepared For?" in Rønn, K.V. et al. (eds.): *Intelligence Practices in High-Trust Societies: Scandinavian Exceptionalism?*, Routledge, London 2025, p. 121-135.
21. Dylan, Huw; Goodman, Michael S.; Jackson, Peter; Jansen, Pia Therese; Maiolo, Joe and Pedersen, Tore: "The way of the Norse Ravens: merging profession and academe in Norwegian national intelligence higher education", *Intelligence and National Security*, vol. 32, no 7, 2017, p. 944-960.
22. Berger, Lars; Borghoff, Uwe M.; Conrad, Gerhard and Pickl, Stefan: "Intelligence Education Made in Europe: Critical Reflections on the German Experience", *International Journal of Intelligence and CounterIntelligence*, vol. 38, no 3, 2025, p. 802-821.
23. Ramsay, James and Macpherson, Andrew: "The integration of statistical learning in intelligence education: is the academy equipping tomorrow's intelligence professionals to analyze data-centric threats?", *Journal of Policing, Intelligence and Counter Terrorism*, vol. 19, no 1, 2024, p. 3-21.
24. Gruszczak, Artur: "Intelligence College in Europe: Fostering Education and Culture", *International Journal of Intelligence and CounterIntelligence*, vol. 38, no 3, 2025, p. 767-784.
25. Yngström, Louise: *Kompetensförsörjning inom informationssäkerhetsområdet för svenska nationella intressen: Ett diskussionsunderlag* [keynote intervention], FHS/CATS Workshop, Försvarshögskolan, Stockholm, 16 October 2018.
26. Nicander, Lars: "The Developmental History of the Center for Asymmetric Threat Studies

(CATS)", *Journal of Information Warfare*, vol. 20, no. 4, 2021, p. 66.
27. Yngström, Louise: *A Systemic-Holistic Approach to Academic Programmes in IT Security*, PhD thesis, Department of Computer and Systems Sciences, Stockholm University, DSV report series 96:21, 1996.
28. Yngström, FHS/CATS 2018 intervention.
29. Yngström, Louise: "A Holistic Approach to IT Security" in Eloff, Jan H. P. et al. (eds.): *Information Security — the Next Decade*, IFIP, Springer, 1995, p. 98-109.
30. Björck, Fredrik and Yngström, Louise: "IFIP World Computer Congress / SEC 2000 Revisited", Stockholm university, 2000, retrieved from: *https://people.dsv.su.se/~bjorck/files/wcc2000-revisited.pdf*.
31. Ibid.
32. Yngström, FHS/CATS 2018 intervention.
33. Huskaj, Gazmend: *Organizing for Cyber Power: Offensive Cyberspace Operations and National Security*, Taylor & Francis, London 2026 (forthcoming).
34. Snyder, Glenn H.: *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press, Princeton 1961; Dahl, Robert A.: "The Concept of Power", *Behavioral Science*, vol. 2, no 3, 1957, p. 201-215.
35. Gill, Peter and Phythian, Mark: *Intelligence in an Insecure World*, 3rd ed., Polity Press, Cambridge 2018; Johnson, Loch K.: "Preface to a Theory of Strategic Intelligence", *International Journal of Intelligence and CounterIntelligence*, vol. 16, no 4, 2003, p. 638-663.
36. Joint Chiefs of Staff: *Joint Publication 2-0: Joint Intelligence*, U.S. Department of Defense, Washington D.C. 2018; Huskaj, *Organizing for Cyber Power*.
37. Huskaj, *Organizing for Cyber Power*.
38. Yngström, *A Systemic-Holistic Approach*; Björck and Yngström, "SEC 2000 Revisited."
39. SOU 2025:78.
40. Ibid.
41. Webster, Jane and Watson, Richard T.: "Analyzing the Past to Prepare for the Future: Writing a Literature Review", *MIS Quarterly*, vol. 26, no 2, 2002, p. xiii-xxiii.
42. Mortenson, Michael J. and Vidgen, Richard: "A computational literature review of the technology acceptance model", *International Journal of Information Management*, vol. 36, 2016, p. 1248-1259.
43. SOU 2025:78.
44. Ibid.
45. Ibid.
46. Ibid.
47. Ibid.
48. Ibid.
49. Ibid.
50. Ibid.
51. National Intelligence University: "Master of Science and Technology Intelligence (MSTI)" and "Master of Science of Strategic Intelligence (MSSI)", programme descriptions, *https://ni-u.edu*, (2025-12-15).
52. Ibid.
53. Cambridge Security Initiative: "International Security and Intelligence", programme description, *https://thecsi.org.uk/isi-acadmic-programme/*, (2025-12-15).
54. King's College London, King's Centre for the Study of Intelligence: "Intelligence and International Security MA", programme description, *https://www.kcl.ac.uk/study/postgraduate-taught/courses/intelligence-and-international-security-ma*, (2025-12-15).
55. Brunel University, Centre for Intelligence and Security Studies: "Intelligence and Security Studies MA", programme description, *https://www.brunel.ac.uk/study/courses/intelligence-and-security-studies-ma*, (2025-12-15).
56. University of Glasgow: "International Master in Security, Intelligence and Strategic Studies (IMSISS)", Erasmus Mundus programme description, *https://www.securityintelligence-erasmusmundus.eu*, (2025-12-15).
57. Danish Defence University (Forsvarsakademiet) and University of Southern Denmark: "Master of Intelligence and Cyber Studies (MICS)", programme description, *https://www.fak.dk/da/uddannelse/uddannelser/mics/*, (2025-12-15).
58. Ibid.
59. Norwegian Intelligence School (Etteretningsskolen), *https://www.etterretningstjenesten.no/etterretningsskolen*, (2025-12-15).
60. Ibid.
61. Ibid.; SOU 2025:78, p. 209.
62. Bundesnachrichtendienst: "Karriere: Ausbildung & Studium", career and training descriptions, *https://www.bnd.bund.de*, (2025-12-15).
63. Ibid.
64. Leiden University: "MSc Intelligence and National Security", programme description,

https://www.universiteitleiden.nl; Netherlands Intelligence Studies Association (NISA), *https://www.nisa-intelligence.nl*, (2025-12-15).
65. Ibid.
66. Intelligence College in Europe: institutional description, *https://www.intelligence-college-europe.org*, (2025-12-15).
67. Intelligence College in Europe: "Call for Papers: Science and Intelligence in Europe", 2026 Academic Conference, University of the Bundeswehr Munich, *https://www.intelligence-college-europe.org/call-for-papers*, (2025-12-15).
68. Sciences Po Saint-Germain-en-Laye: "Diplôme inter-universitaire Renseignement et Menaces (DIReM)", programme description, *https://www.sciencespo-saintgermainenlaye.fr*, (2025-12-15).
69. Ibid.
70. Yngström, FHS/CATS 2018 intervention.
71. Yngström, FHS/CATS 2018 intervention.
72. Nicander, Lars: "The Developmental History of the Center for Asymmetric Threat Studies (CATS)", *Journal of Information Warfare*, vol. 20, no. 4, 2021, p. 66.
73. Ibid, p. 66.