# Strengthening Analytical Competence in (Cyber) Intelligence

**Gazmend Huskaj[1,2] and Stefan Axelsson[2]**
[1]Geneva Centre for Security Policy, Geneva, Switzerland
[2]Department of Computer and Systems Sciences, Stockholm University, Kista, Sweden

g.huskaj@gcsp.ch
stefan.axelsson@dsv.su.se

**Abstract:** Sweden's intelligence education system lacks the technical-domain competence required to meet the analytical demands of contemporary cyber intelligence. This finding emerges from a diagnostic analysis of eleven international intelligence education programmes using the Intelligence Competence Framework (ICF), which combines a multi-level analytical structure (strategic, operational, tactical) with the domain classification (technical, formal, informal) of the Systemic-Holistic Approach. When applied to the programmes referenced by Sweden's government inquiry on intelligence reform (SOU 2025:78), the framework reveals that formal and informal domains receive strong coverage across all programmes while the technical domain is systematically underarticulated — particularly at the tactical level, where only one of eleven programmes achieves strong coverage. Three interdependent capability requirements emerge from an analysis of SOU 2025:78, five international programme models (the German BND, the Danish MICS, the French DIReM, the ICE CIADM module, and the Norwegian Etteretningsskolen), consultations with Swedish intelligence practitioners, and contemporary analyses of AI-supported intelligence (NSCAI, Snow Globe, Emergent Intelligence). Organisationally, the proposed intelligence academy requires a professional authority function that sets competence standards across the intelligence community rather than delivering education alone. Educationally, programmes that integrate technical content with professional practice through apprenticeship models, twin-track specialisations, and practitioner-led instruction produce broader competence coverage than purely academic programmes. Technologically, baseline digital literacy encompassing data provenance, tool limitations, and AI-assisted analytical workflows must be treated as a structural requirement in curriculum design rather than as an optional specialisation. The practitioner consultations identified three specific capability gaps in the current Swedish system: OSINT training that moves beyond keyword searching, exposure to AI-assisted analytical workflows before operational deployment, and secure technical environments for realistic practice. A Swedish intelligence academy built on existing European models will inherit the same technical-domain deficit unless technical competence is embedded as a design principle from the outset.

**Keywords: (**Cyber) intelligence, Competence development, Intelligence education, Offensive cyberspace operations, Open-source intelligence, Systemic-holistic approach

## 1. Introduction

Sweden's security environment is marked by persistent cyber intrusions, foreign intelligence activity, and organised influence operations. The deteriorating threat environment — including the limitations revealed by the intelligence assessment of Russia's political intent prior to the 2022 invasion of Ukraine — created the policy impetus for a comprehensive review of Sweden's intelligence system. The resulting government inquiry, *En reformerad underrättelseverksamhet* (SOU 2025:78), proposes the establishment of a new civilian foreign intelligence agency, restructured oversight mechanisms, and a joint education platform with the long-term objective of an intelligence academy developed in Nordic cooperation.

The inquiry identifies competence development as a strategic priority. It proposes that the Swedish Defence University (FHS) develop a research-based training platform for the intelligence and security services. However, while the inquiry articulates what the intelligence system should achieve at a strategic level, it does not specify what competence intelligence professionals need in order to work effectively within the technical systems through which intelligence is collected, processed, and disseminated. The gap between strategic ambition and tactical competence specification is the problem this article addresses.

A diagnostic analysis using the Intelligence Competence Framework (ICF) — which combines the Multi-Level, Multi-Dimensional (MLMD) framework with Yngström's (1996) Systemic-Holistic Approach (SHA) — reveals an asymmetry in the technical domain of European intelligence education programmes (Huskaj and Axelsson, 2026). This distributional pattern mirrors, in reverse, the finding of Björck and Yngström (2000) that information security research concentrated 83 per cent of its output in the technical domain while neglecting the formal and informal domains.

The question this article addresses is: *what organisational, educational, and technological capabilities are required to build national competence in (cyber) intelligence for Sweden?* The article draws on SOU 2025:78, international intelligence education models, consultations with practitioners in the Swedish intelligence community conducted during the development of the intelligence academy concept, and contemporary

analyses of AI-supported intelligence. The article is structured as follows. Section 2 provides the theoretical framework, and Section 3 describes the method and sources. Section 4 presents the results, organised around three capability domains. Section 5 discusses the implications for Sweden's emerging reform agenda. Section 6 concludes.

## 2. Theoretical Framework

Intelligence education operates across multiple disciplines and institutional contexts. Mapping this landscape requires an analytical framework that can identify where competence is concentrated and where it is absent. Two prior efforts provide the foundation. Coulthart and Crosston (2015) mapped 17 American intelligence programmes and identified significant curricular variation in the absence of accreditation standards. Ramsay and Macpherson (2024) examined 28 U.S. graduate programmes and found that only 25 per cent offered classes across all seven educational categories defined by the International Association for Intelligence Education. Both studies demonstrate that intelligence education develops unevenly — but neither provides a multi-dimensional framework that distinguishes between technical, formal, and informal competence domains.

The Intelligence Competence Framework (ICF) addresses this gap. The ICF combines two analytical traditions. The first is the Multi-Level, Multi-Dimensional (MLMD) framework, developed in the author's doctoral research and formalised in the forthcoming monograph *Organizing for Cyber Power* (Huskaj, forthcoming). The MLMD framework structures analysis across three levels — strategic, operational, and tactical — and integrates deterrence theory, intelligence theory, and the theory of offensive cyberspace operations. The second tradition is the Systemic-Holistic Approach (SHA), developed by Yngström (1996) for information security education. The SHA classifies competence into three domains: technical, formal, and informal. Björck and Yngström (2000) applied this classification to 125 papers from the IFIP SEC 2000 conference and 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.

The ICF combines the MLMD's three levels with the SHA's three domains to produce a 3×3 diagnostic matrix (Table 1).

**Table 1: The Intelligence Competence Framework (adapted from Huskaj and Axelsson, 2026).**

| 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. |

Each cell represents a specific competence intersection — for example, the tactical-technical cell represents the competence required when intelligence professionals interact with technical systems under operational conditions. When applied to eleven international intelligence education programmes referenced by SOU 2025:78, the ICF reveals a structural asymmetry that is the inverse of the Björck and Yngström finding. The formal domain receives strong coverage in 76 per cent of possible cells across the matrix. The informal domain receives strong coverage in 73 per cent. The technical domain receives strong coverage in only 18 per cent. Technical-domain coverage weakens at each successive level, from 2 of 11 programmes at the strategic level to 1 of 11 at the tactical level (Huskaj and Axelsson, 2026). This diagnostic finding establishes the empirical starting point for the prescriptive analysis that follows.

Recent European intelligence education scholarship describes the same landscape from different analytical perspectives. Dylan et al. (2017) document how the Norwegian Intelligence School merged professional training with academic standards through four academic modules on the historical, functional, structural, and decision-maker dimensions of intelligence. Berger et al. (2025) present the ICE Cyber Intelligence and Data-Driven Decision Support module as the German effort to integrate IT capability into European intelligence education, arguing that data science and digitisation must become integral to curriculum design. Gruszczak (2025) analyses ICE through institutional isomorphism and concludes that its contribution operates through cultural diffusion at the strategic-informal level. These perspectives align with the ICF finding: European intelligence education is well-developed in the formal and informal domains, and technical-domain competence is the area where scholarly and institutional attention is most actively being requested.

## 3. Method

The article employs a structured-focused comparison (George and Bennett, 2005) of international intelligence education models to extract transferable design principles for a Swedish intelligence academy. The comparison is structured by a consistent analytical framework — the Intelligence Competence Framework (ICF) — and focused on a specific research question: what capabilities are required to build national competence in (cyber) intelligence.

The analysis draws on four source categories. The first source is Sweden's government inquiry on intelligence reform (SOU 2025:78), which provides the policy context, the institutional proposals, and the competence requirements articulated by the inquiry. The second source is the programme descriptions of five international intelligence education programmes that score most broadly in the technical domain of the ICF: the German Bundesnachrichtendienst (BND) training pathways, the Danish Master of Intelligence and Cyber Studies (MICS), the French Diplôme inter-universitaire Renseignement et Menaces (DIReM) at Sciences Po Saint-Germain-en-Laye, the Intelligence College in Europe (ICE) Cyber Intelligence module (CIADM), and the Norwegian Intelligence School (Etteretningsskolen). These programmes were selected because they address the technical domain more extensively than the academic programmes in the dataset.

The third source is consultations with practitioners in the Swedish intelligence community, conducted during the development of a concept note for the proposed intelligence academy in 2025–2026. These consultations involved professionals from the Swedish Armed Forces, the Swedish Defence University, Stockholm University, and affiliated research institutions. The consultations were informal and unstructured, conducted under conditions of professional confidentiality. They do not constitute formal interviews and no individual statements are attributed. However, the patterns that emerged from these consultations inform the identification of capability requirements in Section 4. No ethical clearance was required because the consultations did not constitute formal interviews and no individual statements were attributed.

The fourth source comprises contemporary analyses of AI-supported intelligence, including the final report of the U.S. National Security Commission on Artificial Intelligence (NSCAI, 2021), the CIA's Snow Globe experiment in human-AI teaming (Brennan et al., 2025), and the "Emergent Intelligence" assessment of intelligence work in the AI era (Studies in Intelligence, 2025). These sources identify the technological transformation that shapes the competence requirements the article examines.

In accordance with the principles of transparent and reproducible science, the author used Anthropic's Claude Opus 4.6 as a research assistant during the preparation of this article. The tool was used to support structured literature screening, to verify coding consistency, and to assist with formatting during drafting. All analytical judgements were made by the author. The author assumes full responsibility for the accuracy of all claims and any errors that remain.

## 4. Results

The results are organised around three interdependent capability domains: organisational, educational, and technological. Each domain addresses a dimension of the research question and draws on the international models and practitioner consultations described in Section 2.

### 4.1 Organisational Capabilities

The Norwegian Intelligence School (Etteretningsskolen) provides the clearest model for the organisational function that a Swedish intelligence academy would need to perform. The school exercises *fagmyndighet* — professional authority — for intelligence on behalf of the Chief of the Norwegian Intelligence Service (Dylan et

al., 2017). This institutional function means that the school does not merely teach intelligence; it defines what intelligence competence means for the entire Norwegian Defence. It sets unified competence requirements, issues and revises intelligence doctrine, and advises on capability projects related to intelligence.

This distinction between teaching and standard-setting is the central organisational insight from the international comparison. SOU 2025:78 proposes that FHS develop a joint education platform. However, the inquiry does not assign the platform a professional authority function equivalent to the Norwegian model. Without such a function, the platform risks becoming a course catalogue rather than a competence architecture. The consultations with Swedish practitioners confirmed this concern: multiple interlocutors identified the absence of a single institution with the authority to define competence requirements across the intelligence community as a structural gap in the current system.

The Intelligence College in Europe (ICE) demonstrates a different organisational model. ICE operates as a platform for professional and academic exchange rather than a degree-granting institution (Gruszczak, 2025). Its contribution is cultural diffusion at the strategic-informal level: building a common strategic intelligence culture across European member states. ICE's 28-country membership, 89 affiliated intelligence agencies, and 33-institution academic network provide a horizontal cooperation structure. However, ICE does not deliver structured technical training and does not exercise professional authority over competence standards. For Sweden, ICE's model is relevant as a networking and cultural exchange mechanism but insufficient as the primary vehicle for technical competence development.

The BND's organisational model reflects a third approach: service-internal training that integrates education with operational practice. The BND offers three distinct training pathways — a general intelligence apprenticeship, a SIGINT apprenticeship, and a physical security apprenticeship — each combining theoretical instruction with practical placements across departments. This model ensures that competence development is directly governed by the operational requirements of the service. The BND's breadth across the ICF matrix reflects its institutional character as a system that trains for the full range of intelligence functions. The trade-off is that service-internal models are not designed to serve a broader national intelligence community.

The organisational capability requirement for Sweden is therefore a hybrid: a professional authority function that sets competence standards for the entire intelligence community (the Norwegian model), combined with structured cooperation with operational services that grounds education in professional practice (the BND principle), and connected to international networks for strategic culture development (the ICE function). SOU 2025:78's proposal for a Council for Intelligence Research and Education could serve as the governance mechanism for this hybrid model, provided it is given the authority to define competence requirements and not only to coordinate existing offerings.

The consultations with Swedish practitioners reinforced the need for a multi-institutional collaboration model. No single institution possesses the full range of capabilities required. The Swedish Defence University holds the defence education mandate and proximity to the intelligence community but lacks depth in AI and data science. Stockholm University's Department of Computer and Systems Sciences leads in data science, AI, and decision support but operates outside the security-cleared environment. The Swedish Defence Research Agency (FOI) conducts applied research in intelligence-relevant domains but does not deliver degree programmes. Lund University has cultivated Sweden's most sustained tradition in intelligence analysis but its institutional capacity in this area is concentrated in a small number of senior scholars.

Thus, the discussions revealed that an inclusive model — one that draws on each institution's specific strengths under a coordinating governance structure — is the only architecture that can meet the breadth of competence requirements. As one respondent observed, the priority must be to ensure that no existing knowledge or competence is lost in the transition to a new institutional structure. This observation carries particular urgency given that several of Sweden's most experienced intelligence scholars are approaching or have passed retirement. The intelligence academy is therefore not only a forward-looking construction project but also a preservation mechanism for competence that currently exists in individuals rather than in institutions.

### 4.2 Educational Capabilities

The diagnostic analysis using the ICF confirms that the technical domain is the weakest across the eleven programmes, with the formal and informal domains receiving strong coverage in the majority of cells (Huskaj and Axelsson, 2026). The three programmes that score most broadly across the technical column — BND,

MICS, and DIReM — share a common design principle: each integrates technical content with professional practice rather than treating technology as a separate academic subject.

The Danish MICS programme provides the most relevant Nordic model for educational design. MICS is a joint programme between the Danish Defence University and the University of Southern Denmark, explicitly addressing the cyber domain in a security-political context. The programme includes twin specialisation tracks — intelligence and cyber — and builds competence through practice-oriented expertise combined with an analytical track. MICS is designed for personnel with experience from the intelligence or cyber domain. This twin-track model ensures that technical competence is developed alongside strategic and analytical competence rather than in isolation.

The French DIReM at Sciences Po Saint-Germain-en-Laye offers a different educational model: practitioner-led instruction within a broader analytical framework. The *veille et analyse des données* module develops practitioner competence in geolocation, imagery verification, and structured open-source techniques alongside political and sociological perspectives. Practitioner lecturers from the DGSI, DGSE, and armed forces contribute to instruction in the security-cleared environment of the Académie du renseignement. DIReM's strength is the integration of technical methods with legal and sociological analysis.

The ICE CIADM module, developed by Berger et al. (2025) for the German Master of Intelligence and Security Studies (MISS) and adapted for ICE delivery, provides a five-day curriculum model addressing cyber intelligence and data-driven decision support. The module covers cyber intelligence concepts, threat assessment, AI-based analytical tools, operational analysis, and horizon scanning. It combines critical reflection with a problem-solving focus, targeting intelligence practitioners at an earlier career stage. The module demonstrates that structured technical content can be delivered in a compact format within an international, multi-agency setting.

The educational capability requirement is a structured progression from strategic understanding through operational application to tactical proficiency. SOU 2025:78 proposes a joint education platform but does not articulate what this progression should contain. The international models suggest that the progression should include: strategic-level courses on how technology reshapes the intelligence enterprise (following the MICS model); operational-level modules on AI-supported analytical workflows, OSINT tool proficiency, and data-fusion methods (following the DIReM and CIADM models); and tactical-level training through practical placements in technical departments where analysts interact with collection systems under operational conditions (following the BND model).

The practitioner consultations also identified a governance dimension to educational design. Multiple respondents noted that Sweden currently lacks a mechanism for coordinating intelligence education across institutions. Courses are developed and delivered by individual departments — at FHS, at DSV, at Lund, at FOI — without a shared framework for ensuring that the aggregate output meets the intelligence community's competence requirements. The proposed Council for Intelligence Research and Education (SOU 2025:78) could address this gap if it is empowered to commission education based on identified competence needs rather than to merely catalogue existing offerings. The consultations suggested that a steering function — analogous to a curriculum board with representation from the intelligence services, academia, and the research institutes — would be necessary to translate the competence requirements identified through the ICF into specific course designs, practicum placements, and assessment criteria.

### 4.3 Technological Capabilities

The NSCAI (2021) report identifies AI competence as a national security requirement and argues that the United States must prepare the intelligence workforce for a future in which AI augments human analytical capacity. The Snow Globe experiment demonstrated that participants with greater prior digital experience used AI assistants more systematically and critically, suggesting that baseline digital literacy shapes the quality of human-AI interaction in intelligence settings (Brennan et al., 2025). The "Emergent Intelligence" assessment identifies the competence intersection where intelligence professionals interact with AI tools as the baseline requirement for the next generation of intelligence work (Studies in Intelligence, 2025).

The MI6 chief's first public address emphasised that in a "faster, more dangerous and technology-mediated world," the rediscovery of human agency alongside technological capability will determine how the future unfolds (Metreweli, 2025). This framing positions technical competence not as a replacement for human judgement but as a precondition for its effective exercise. Intelligence professionals who do not understand how AI tools generate their outputs cannot exercise meaningful judgement over those outputs.

The consultations with Swedish practitioners identified three specific technological capability gaps. First, the absence of structured OSINT training that moves beyond keyword searching to encompass geolocation, reverse image search, social media pattern analysis, and data provenance verification. Second, the lack of exposure to AI-assisted analytical workflows — including the limitations and failure modes of machine learning systems — before analysts encounter these tools in operational settings. Third, the absence of secure technical environments where analysts can practise with realistic data without compromising operational security.

SOU 2025:78 identifies cloud-based data processing, AI, and cross-domain integration as priority capability areas. However, the inquiry describes what technology should achieve for the intelligence system at a strategic level. It does not specify what competence intelligence professionals need in order to work effectively within such systems. The technological capability requirement is therefore not about acquiring specific tools but about developing the analytical competence to evaluate, use, and critically assess the outputs of technical systems. This competence includes understanding data provenance, recognising tool limitations, identifying system error modes, and making time-sensitive judgements about technical artefacts.

The Geneva Centre for Security Policy's (GCSP) Global Cyber and Security Policy Programme demonstrates that a holistic, systems-based, and comprehensive approach to cyber and security policy challenges is already in operation internationally (GCSP, 2024). The programme integrates training and executive education, dialogue and outreach, and security policy-relevant research into a systemic architecture. This model provides evidence that the prescriptive framework proposed here — integrating organisational, educational, and technological capabilities — is operationally viable.

## 5. Discussion

The answer to the research question — what organisational, educational, and technological capabilities are required to build national competence in (cyber) intelligence for Sweden? — is that the three capability domains are interdependent and must be developed in parallel. Organisational authority without educational content produces empty mandates. Educational programmes without organisational authority produce competent individuals who return to institutions that do not recognise their competence. Technical training without organisational integration produces specialists who cannot connect their skills to the intelligence mission.

### 5.1 The Technical-domain Deficit as a Design Problem

The diagnostic analysis (Huskaj and Axelsson, 2026) reveals that the technical domain receives strong coverage in 18 per cent of possible cells across eleven European programmes, compared to 76 per cent for the formal domain and 73 per cent for the informal domain. The ratio — approximately 1:4 — quantifies the structural asymmetry. This is not a failure of individual programmes. It is a systemic pattern that reflects how intelligence education has historically been structured: around policy, law, governance, and professional culture rather than around technical systems and their analytical exploitation.

For Sweden, this pattern has a specific policy implication. SOU 2025:78 references the eleven programmes analysed in the diagnostic study as benchmarks for the proposed intelligence academy. If the academy is designed by replicating the educational patterns of these benchmarks, it will inherit the same distributional asymmetry. The technical domain will remain the weakest area of competence — precisely the domain that the NSCAI, Snow Globe, and Emergent Intelligence assessments identify as the most urgent requirement.

The Swedish public debate on SOU 2025:78 has focused on organisational structure rather than competence. Critics have warned that the proposed reform risks defence capability, is badly timed, and centralises too much (Wiktorin, 2025). The Must chief has responded that the intelligence services have sufficient work for all agencies and that broadening the intelligence service is necessary (Nilsson, 2026). Both sides of the debate accept that analytical competence must be strengthened. The disagreement is about how to organise the institutional architecture, not about the competence requirement itself. This article contributes to the uncontested ground: specifying what competence is needed and how it should be structured.

### 5.2 Design Principles for the Intelligence Academy

Five design principles emerge from the analysis. First, the academy should exercise a professional authority function that defines competence requirements for the entire intelligence community, following the Norwegian fagmyndighet model. This function should include the authority to issue intelligence education doctrine and to certify that competence requirements are met.

Second, the academy should integrate technical content with professional practice through structured practical placements in operational services. The BND model demonstrates that this integration produces graduates with both academic qualifications and operational competence. For Sweden, this implies formal cooperation agreements between the academy and the intelligence services that provide placements in technical departments.

Third, the academy should offer twin-track specialisations that link cyber intelligence with strategic analysis, following the MICS model. This design ensures that technical specialists understand the strategic context of their work and that strategic analysts understand the capabilities and limitations of the technical systems that produce the intelligence they assess.

Fourth, OSINT tool training should be embedded within a broader analytical framework that includes legal, ethical, and sociological perspectives, following the DIReM model. The consultations with Swedish practitioners identified OSINT as the area where the gap between existing competence and operational requirement is widest. The DIReM model demonstrates that OSINT proficiency can be developed alongside policy and legal analysis rather than as a standalone technical course.

Fifth, the academy should establish a secure technical environment — a laboratory or testbed — where analysts can practise with realistic data and AI-assisted tools without compromising operational security. This requirement emerged consistently in the practitioner consultations and is consistent with the broader NSCAI emphasis on preparing the intelligence workforce for AI-augmented analytical work.

### 5.3 Nordic Cooperation and NATO Integration

SOU 2025:78 articulates a long-term vision of an intelligence academy developed in Nordic cooperation. The Norwegian Etteretningsskolen already collaborates with King's College London for master-level education. The Danish MICS is a joint programme between a military and a civilian university. ICE provides a European platform. Sweden's NATO membership, effective since 2024, generates new requirements for the interoperability of intelligence cooperation. An intelligence academy that meets NATO's competence standards while maintaining the Nordic tradition of combining profession and academe (Dylan et al., 2017) would position Sweden as a contributor to collective intelligence capability rather than a consumer.

The Berger et al. (2025) analysis of the ICE experience demonstrates that European intelligence education benefits from combining the critical reflection of academic programmes with the problem-solving focus of practitioner training. The German MISS and the ICE CIADM module exemplify this combination. For Sweden, the implication is that the proposed academy should be designed to both receive and contribute modules to the ICE network, ensuring that Swedish intelligence education is integrated into the European landscape from the outset.

### 5.4 The Governance gap Between Mandate and Capacity

The practitioner consultations identified a structural tension that SOU 2025:78 does not fully resolve. FHS has been assigned the mandate to develop the joint education platform. However, the technical capacity required to deliver AI-enabled analytical training, data science instruction, and secure laboratory environments does not reside at FHS. It resides at DSV/SU, at FOI, at RISE, and within the intelligence services themselves. The mandate and the capacity are located in different institutions. Without a governance mechanism that bridges this gap, the mandate risks remaining unfulfilled — or fulfilled in a manner that replicates the formal-domain concentration of existing programmes because FHS's institutional strengths lie in precisely that domain.

The Norwegian model resolves this tension through the fagmyndighet function: the Etteretningsskolen both defines competence requirements and delivers education, with external academic partners contributing to specific programmes. The Danish model resolves it through joint institutional design: MICS is formally a programme of two universities, one military and one civilian. For Sweden, neither model can be directly transplanted. The Swedish intelligence community is larger and more institutionally fragmented than Norway's, and the proposed academy must serve multiple agencies rather than a single service.

A fuller picture of the governance gap requires acknowledging the Swedish institutional structures that already operate in the adjacent space. Campus Totalförsvar is a strategic collaboration led by FHS, Örebro University, and Luleå University of Technology, launched in 2024 with thirty million SEK in government funding to strengthen Sweden's total defence through coordinated education and research across more than thirty participating higher education institutions (Campus Totalförsvar, 2024). Cybercampus Sweden, inaugurated at KTH in 2024 with over one hundred million SEK in government funding, is a national initiative led by KTH, RISE,

the Swedish Armed Forces, Karlstad University, Saab, Ericsson, and MCF (formerly MSB) to deliver research, innovation, and education for cybersecurity and defence beyond what individual organisations can achieve alone (Cybercampus Sweden, 2024). Both initiatives address parts of the competence terrain that a Swedish intelligence academy would also need to cover.

Campus Totalförsvar organises research and educational activities across the civil-military spectrum of total defence. Cybercampus Sweden builds national capacity in cyber security and cyber defence, including through the CDIS collaboration between KTH, the Swedish Armed Forces, FOI, FRA, FHS, and MCF. The proposed intelligence academy cannot be designed in isolation from these structures. Two governance implications follow. First, the academy's technical-domain competence requirements should be specified in coordination with Cybercampus Sweden rather than developed in parallel — the technical capacity for cyber intelligence training already exists in the Cybercampus network, and duplication would be institutionally wasteful. Second, Campus Totalförsvar provides an existing coordination architecture that the intelligence academy could integrate with rather than replicate. The technical-domain deficit identified in European intelligence education programmes is not a gap in Swedish technical capacity as such — it is a gap in the institutional connection between Swedish technical capacity and the intelligence application domain.

The governance requirement is therefore a coordinating authority that can commission research and education from multiple institutions, ensure that the aggregate output covers all cells of the ICF matrix, articulate the intelligence academy's relationship with Campus Totalförsvar and Cybercampus Sweden, and monitor whether the technical-domain deficit is being addressed over time.

## 6. Conclusion

The answer to the research question — what organisational, educational, and technological capabilities are required to build national competence in (cyber) intelligence for Sweden? — is that the three capability domains are interdependent and must be developed in parallel. A professional authority function is required to set competence standards across the intelligence community. An educational progression from strategic understanding through operational application to tactical proficiency is required to populate the technical domain that existing programmes underarticulate. Baseline digital literacy — encompassing data provenance, tool limitations, and AI-assisted analytical workflows — must be treated as a structural requirement in curriculum design.

The five design principles identified in this article — professional authority, practice-integrated education, twin-track specialisation, embedded OSINT training, and secure technical environments — provide a framework for translating the diagnostic finding into institutional design. Without structured attention to the technical domain, a Swedish intelligence academy built on existing European models will inherit the same distributional asymmetry that characterises the field. The Intelligence Competence Framework provides the diagnostic instrument for monitoring whether future curriculum design addresses this challenge.

## Acknowledgements

The author gratefully acknowledges the foundational work of Prof Emerita Louise Yngström and Dr Fredrik Blix (formerly Björck) on the Systemic-Holistic Approach and the SEC 2000 classification, which this article adapts for intelligence education.

**AI Declaration**: The first author used Anthropic's Claude Opus 4.6 as a research assistant during the preparation of this article. The tool was used to support structured literature screening, to verify coding consistency across programme descriptions, and to assist with formatting and style calibration during drafting. All analytical judgements — including the design of the framework, the interpretation of findings, and the formulation of design principles — were made by the author. The author assumes full responsibility for the accuracy of all claims and any errors that remain in the published text.

**Ethics Declaration**: The research did not require ethical clearance under the Swedish Ethical Review Act (2003:460). No personal data were processed and no statements in the paper are attributed to identifiable individuals.

**Disclaimer:** The views expressed in this paper are solely those of the authors and do not necessarily reflect the official policies or positions of the Geneva Centre for Security Policy, or Stockholm University. The analysis and conclusions are presented for academic and policy discussion purposes only.

## References


Berger, L., Borghoff, U. M., Conrad, G. and Pickl, S. (2025) “Intelligence Education Made in Europe: Critical Reflections on the German Experience”, *International Journal of Intelligence and CounterIntelligence*, 38(3), pp. 802–821.

Björck, F. and Yngström, L. (2000) “IFIP World Computer Congress / SEC 2000 Revisited”, Stockholm University. Available at: https://people.dsv.su.se/~bjorck/files/wcc2000-revisited.pdf.

Brennan, A., Grunspan, R., Hogan, D., Smith, J. D. and VanderVeen, E. (2025) “Snow Globe Multi-Player AI System: Lessons from Human-AI Teaming in War Games”, *Studies in Intelligence*, 69(4), pp. 15–21.

Campus Totalförsvar (2024) *Campus totalförsvar*. Available at: https://www.fhs.se/samverkan/campus-totalforsvar.html (Accessed: 18 April 2026).

Coulthart, S. and Crosston, M. (2015) "Terra Incognita: Mapping American Intelligence Education Curriculum", *Journal of Strategic Security*, 8(3), pp. 46–68.

Cybercampus Sweden (2024) About us. Available at: https://www.cybercampus.se/en/about (Accessed: 18 April 2026).

Dylan, H., Goodman, M. S., Jackson, P., Jansen, P. T., Maiolo, J. and Pedersen, T. (2017) “The way of the Norse Ravens: merging profession and academe in Norwegian national intelligence higher education”, *Intelligence and National Security*, 32(7), pp. 944–960.

“Emergent Intelligence: Spycraft and Intelligence in the AI Era” (2025) *Studies in Intelligence*, 69(4), pp. 7–13.

Geneva Centre for Security Policy (2024) *Global Cyber and Security Policy Programme*. Available at: https://www.gcsp.ch/topics/global-cyber-and-security-policy (Accessed: 15 December 2025).

George, A. L. and Bennett, A. (2005) *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Gruszczak, A. (2025) “Intelligence College in Europe: Fostering Education and Culture”, *International Journal of Intelligence and CounterIntelligence*, 38(3), pp. 767–784.

Huskaj, G. (forthcoming) *Organizing for Cyber Power: Offensive Cyberspace Operations and National Security*. London: Taylor & Francis.

Huskaj, G. and Axelsson, S. (2023) “A Whole-of-Society Approach to Organise for Offensive Cyberspace Operations: The Case of the Smart State Sweden”, *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, pp. 1188–1196.

Huskaj, G. and Axelsson, S. (2026) “Intelligence Education as a Competence Challenge: Applying the Intelligence Competence Framework to SOU 2025:78”, *Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift* (forthcoming).

Metreweli, B. (2025) *Speech by the Chief of the Secret Intelligence Service*, 15 December 2025. London: SIS.

National Security Commission on Artificial Intelligence (2021) *Final Report*. Washington, D.C.: NSCAI.

Nilsson, T. (2026) Interview with *Dagens Nyheter*, 24 January 2026.

Ramsay, J. and Macpherson, A. (2024) "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*, 19(1), pp. 3–21.

SOU 2025:78 (2025) *En reformerad underrättelseverksamhet*. Stockholm: Statens offentliga utredningar.

Wiktorin, J. (2025) “Ett farligt förslag för svensk säkerhet”, *Svenska Dagbladet*, 6 October 2025.

Yngström, L. (1996) *A Systemic-Holistic Approach to Academic Programmes in IT Security*. PhD thesis, Stockholm University.