ECONSTOR
Make Your Publications Visible.

A Service of
ZBW
Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Baur, Ralf; Donner, Ole; Koch, Niklas; Schulz, André; Weiss, Richard

Working Paper

Development of an ICP-LLM to support the creation of an Intelligence Collection Plan (ICP)

Working paper from the Security Management degree program at the NBS Northern Business School Hamburg, No. 3/2025

Provided in Cooperation with:
NBS Northern Business School – University of Applied Sciences, Hamburg

Suggested Citation: Baur, Ralf; Donner, Ole; Koch, Niklas; Schulz, André; Weiss, Richard (2025) : Development of an ICP-LLM to support the creation of an Intelligence Collection Plan (ICP), Working paper from the Security Management degree program at the NBS Northern Business School Hamburg, No. 3/2025, NBS Northern Business School, Institute for Intelligence and Security Management (I2SM), Hamburg

This Version is available at:
https://hdl.handle.net/10419/330340

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

Working paper from the Security Management degree program

at the NBS Northern Business School Hamburg

Institute for Intelligence and Security Management (I2SM)

No. 3/2025

Development of an ICP-LLM to support the creation of an Intelligence Collection Plan (ICP)

Baur, Ralf / Donner, Ole / Koch, Niklas / Schulz, André / Weiss, Richard

Summary

The creation of an Intelligence Collection Plan (ICP) is a key step at the intersection of the *direction* phase[1] (see Figure 1) and Intelligence Requirement Management (IRM) within the intelligence cycle. This is intended to enable the systematic structuring of information requirements and the targeted management of research and reconnaissance. In practical application, however, there are challenges in terms of time, content, and technology that can lead to delays, inconsistencies, and quality losses.

The ICP-LLM is a tool that uses large language models (LLMs) to automatically generate the lower levels of an ICP—specific intelligence requirements (SIRs) and essential elements of information (EEIs). This speeds up and simplifies the creation of ICPs.

The aim of this working paper is to shed light on the background to the development of ICP-LLM. It also takes a look at how the tool's usefulness and applicability are being experimentally evaluated as part of a course at the NATO Civil-Military Cooperation Centre of Excellence (CCOE). The aim is to investigate the extent to which the use of ICP-LLM makes the creation of ICPs more efficient, improves structural quality, and is considered relevant to practice by users. The results will provide insight into whether and to what extent LLM-supported assistance systems can offer added value for use in an intelligence context. In a further step, the tool will be put to the test in a research project at I2SM on organized crime as part of crime analysis.

[1] In the Direction step, all information requirements relevant to decision-making are expressed by decision-makers and systematized and formalized by Intelligence Requirement Management (IRM). See: Civil-Military Cooperation Center of Excellence: NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5, p. 16 ff.

1. The role of Intelligence Collection Plans

Intelligence serves to give decision-makers in companies and government institutions an information and decision-making advantage over competitors or opponents. For this to work, the provision of intelligence products relevant to decision-making is a prerequisite. What is relevant to decision-making should be defined by those who have to make the decisions themselves. To ensure this, the intelligence world uses the so-called intelligence cycle[2] as a framework process (see Figure 1).

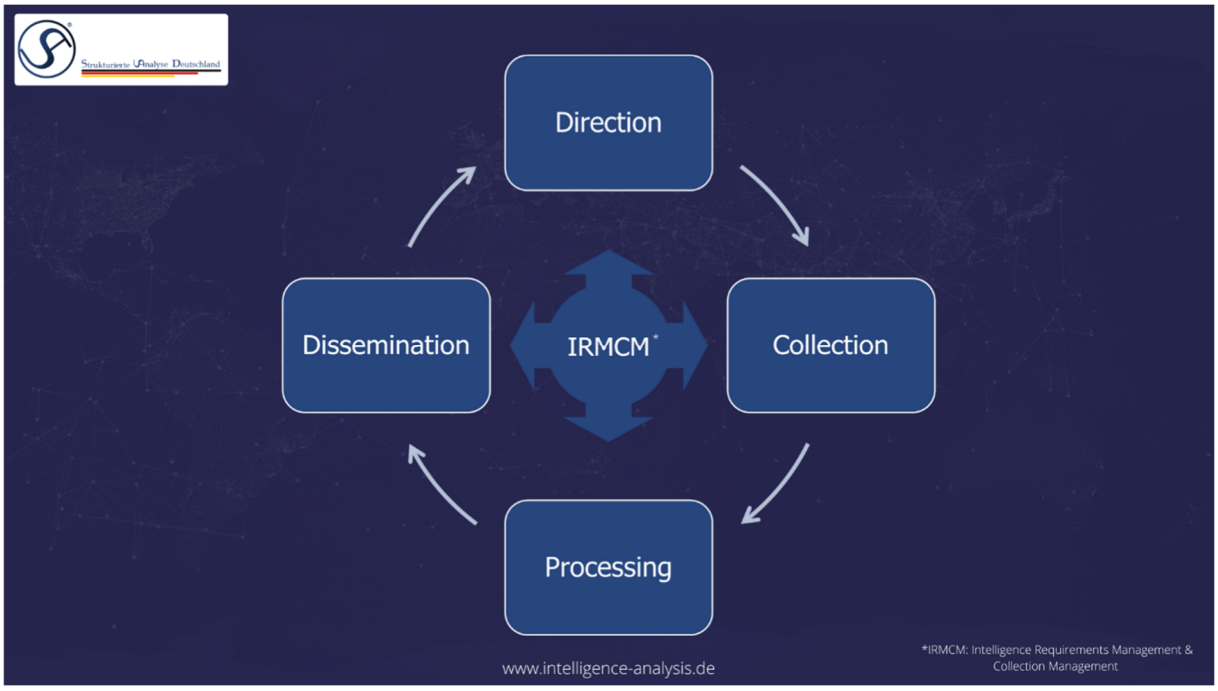

Figure 1: Intelligence Cycle, own illustration, 2025.

In the Direction step, all information requirements relevant to the decision are expressed by the decision-makers and systematized and formalized by Intelligence Requirement Management (IRM).[3] In the course of this, it is often necessary to rephrase or operationalize the questions asked. When rephrasing, it can be said that an originally asked initial question is converted into a core question. This may be necessary if the initial question was formulated incorrectly. Examples of incorrectly formulated questions include questions that are too broad or too narrow, questions that already imply the answer, or questions driven by assumptions. The reformulated core questions are usually relatively broad, so

[2] The underlying approach here is that of a framework understanding of the intelligence cycle (Intelligence Cycle as a framework) rather than a procedural understanding (proceduralist approach to the Intelligence Cycle). See: Davies, Philip et al. (2013): The Intelligence Cycle is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine, in: Phythian, Mark (ed): Understanding the Intelligence Cycle, Studies in Intelligence, Routledge, pp. 67-85.
[3] See Civil-Military Cooperation Centre of Excellence: NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5, S. 16 ff.

they need to be operationalized and broken down into sub-questions. Various Structured Analytic Techniques (SATs) such as issue redefinition or the Analytic Spectrum can be used for this purpose.

Rephrasing, operationalization, and breakdown into sub-questions are carried out by IRM personnel, usually in cooperation with analysis personnel. NATO uses the Intelligence Collection Plan (ICP) to facilitate this process.

In an ICP, the original questions – Commander's Critical Information Requirements (CCIRs[4])– are broken down into smaller sub-questions (Priority Intelligence Requirements / PIRs[5]). The system behind this is that a CCIR can be broken down into any number of PIRs. Answering all PIRs should then be equivalent to answering the CCIR. Or, to put it another way: If all PIRs can be answered, the CCIR for which these PIRs were developed can also be answered.

Each PIR is then broken down into any number of Specific Intelligence Requirements (SIRs[6]). The previously applied system remains the same: if all SIRs developed for a PIR can be answered, this enables the corresponding PIR to be answered.

Finally, all SIRs are broken down into Essential Elements of Information (EEIs[7]). The system remains the same. Only the type of question that an EEI should correspond to changes. This is because EEIs should,

---

[4] "Commander's critical information requirements (CCIRs) cover information concerning areas that are either critical to the success of the mission or represent a critical threat. CCIR cover all aspects of the commander's concern including friendly forces information requirement (FFIRs), essential elements of friendly information (EEFI) and the priority intelligence requirements (PIRs). The two key elements of CCIRs are priority intelligence requirements (PIRs) and friendly force information requirements (FFIRs)" siehe: NATO STANDARD AJP-2 ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition B Version 1 JULY 2020; see also: Headquarters Department of the Army FM 34-2 (1994): COLLECTION MANAGEMENT AND SYNCHRONIZATION PLANNING, APPENDIX A THE COLLECTION PLAN, online: https://irp.fas.org/doddir/army/fm34-2/Appa.htm#Appa [Access: 23.10.2025].

[5] "Priority intelligence requirements (PIRs) - Commander's PIRs are a vital part of the CCIRs and are normally formulated by the intelligence staffs in close cooperation with commanders. The PIRs encompass those intelligence requirements for which commanders have an anticipated and stated priority in their tasking of planning and decision-making and normally involve identification and monitoring of areas that represent opportunities and threats to the mission plan. They are a standing set of requirements that drive the collection and production effort, and provide the focus of the overall intelligence mission. They should be limited in number and provide comprehensive and coherent groupings of key issues and should be linked to commander's decision points. They may be enduring or limited to a particular phase or situation.", see: NATO STANDARD AJP-2, ibid.

[6] "Specific intelligence requirements (SIRs) - SIRs support and complement each PIR and provide a more detailed description of the requirement. SIRs are used by the intelligence staff to determine what intelligence asset, source or discipline can best satisfy the requirement, and to identify the coordination required to ensure that the appropriate assets are deployed. The SIRs allow collection and analysis agencies to develop their response or collection toward that best suited to the stated requirement. SIRs are divided in the same manner as PIRs. Some collection requirements may be submitted by other organizations to the intelligence staff.", see: NATO STANDARD AJP-2, ibid.

[7] "Essential elements of information (EEI) - SIRs are broken down into more detailed questions known as EEI. The EEI add the details to the SIRs and allow the production of a collection task list based on an intelligence collection plan (ICP83). EEI could be related to several SIRs and should provide enough guidance to allow analysts to give a complete and satisfactory answer to each requirement. EEI are the basis for creating collection requirements

if possible, be formulated in such a way that they can be answered in binary, category-based, or numerical form (see Figure 2).

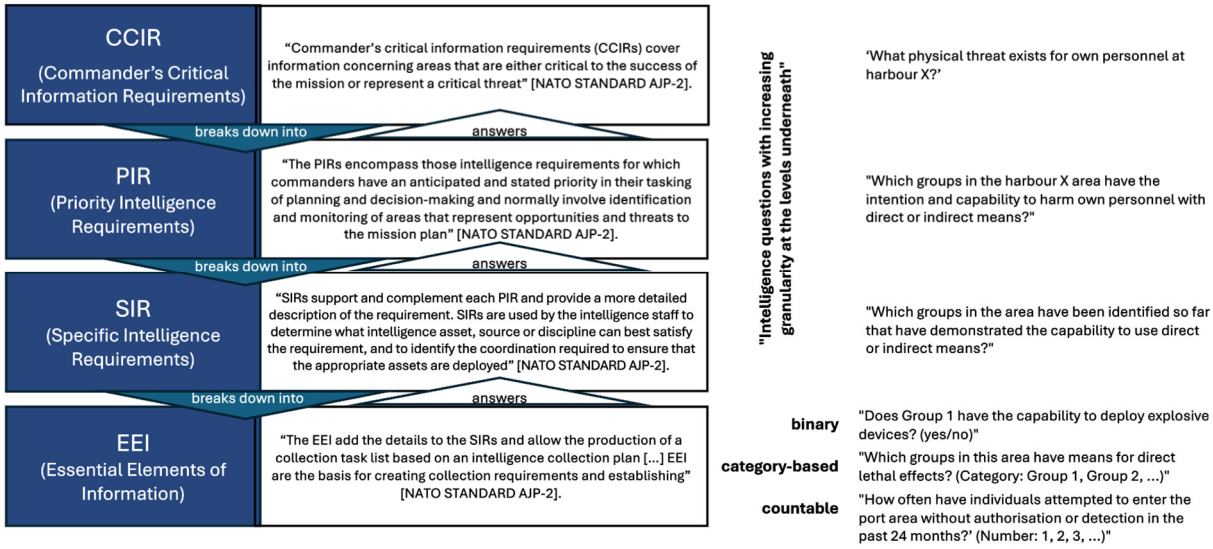

Figure 2: Intelligence Collection Plan, own illustration, 2025.

The ICP serves as an organisational aid for deciding which questions are answered in the processing step and which questions are converted into collection tasks. These can then be converted into collection tasks by the collection manager (the CM in IRMCM) in consultation with the reconnaissance disciplines or sensors. If a sensor is found that can be used to gather information on an EEI and that is also willing to take on this task or can be instructed to do so, this can also be noted on the ICP. In addition, the point in time at which answering a question no longer adds value (last date of intelligence value) should also be noted.

and establishing", see: NATO STANDARD AJP-2, ibid., also see: United Nations 2025: Lesson 3.5 PKISR Requirements Management and Prioritisation, online: https://resourcehub01.blob.core.windows.net/training-files/Training%20Materials/042%20PKISR%20RTP/042-012%20PKISR%20RTP%20Lesson%203.5%20Requirements%20management%20and%20prioritisation.pdf [Access; 23.10.2025].

CCIR	PIR	SIR	EEI
1. What Threat exists for NATO Troops in LATVIA?	1.1 What threat can arise from the Civil Environment?	1.1.1 Is the Russian-speaking minority in LATVIA a threat to NATO troops?	1.1.1.1 Is the Russian-speaking Minority located or moving near NATO Troops?
			1.1.1.2 Does the Russian-speaking Minority posses SALW?
			1.1.1.3 Does the Russian-speaking Minority posses explosives?
		1.1.2 ...	1.1.1.4 Does the Russian-speaking Minority posses means to jam signals?
			1.1.1.5 Does the Russian-speaking Minority has the capability to use SALW?
			1.1.1.6 Does the Russian-speaking Minority has the capability to use explosives?
			1.1.1.7 Does the Russian-speaking Minority has the capability to use jammers?
	1.2 ...	1.1.3 ...	1.1.1.8 Does the Russian-speaking Minority show the intention to harm NATO Troops?
			1.1.1.9 Has the Russian-speaking Minority harmed NATO Troops in the past?
			1.1.1.10 Where has the Russian-speaking Minority harmed NATO Troops in the past?
			1.1.1.11 How has the Russian-speaking Minority harmed NATO Troops in the past?
		1.1.4 ...	1.1.1.12 When has the Russian-speaking Minority harmed NATO Troops in the past?
			1.1.1.13 Why has the Russian-speaking Minority harmed NATO Troops in the past?
			1.1.1.14 ...

Figure 3: Example of a partial intelligence collection plan, own illustration, 2025.

Creating an ICP involves a number of challenges. In addition to content-related challenges associated with identifying the right questions and formulating them correctly, there are also time-related and technical challenges, as well as challenges relating to prioritisation.

2. Time-related challenges

Intelligence can be a fast-paced business. Insights that enable decisions today and significantly improve the relative position of decision-makers vis-à-vis competitors or opponents may be irrelevant tomorrow. Once the point has passed at which answering a question no longer adds value (last date of intelligence value), staff time and attention can be invested elsewhere.

The generation of questions, as well as the organisation and prioritisation of the question space, should therefore be done as quickly as possible, but as carefully as necessary. Since creating an ICP can be time-consuming, supporting tools and processes[8] are effective mechanisms for speeding up the creation process (keyword: speed of relevance).

[8] Processes here refer to formalised procedures, such as the application of the intelligence cycle, Structured Analytic Techniques (SATs) and feedback loops between all stakeholders, particularly between management level and in the units IRMCM and Analysis.

3. Content-related challenges

Good intelligence and analysis work depends heavily on identifying the right questions. If the wrong questions[9] are asked or good questions are phrased incorrectly[10], even the most intensive efforts in the fields of collection and processing will not lead to a useful answer. This is because the probability that, despite a 'suboptimal question A', the 'optimal question A' actually intended by the client will be answered by chance is virtually zero. Recognising wrong and wrongly formulated questions is a skill that must be acquired and trained, as is reformulating them into potentially better questions.

4. Technical challenges

Many companies and public organisations do not have specially developed software for creating and sharing ICPs. As a result, many organisations resort to MS Excel. In principle, this tool can represent the structure of an ICP and runs on most computers. However, the software comes with a whole host of difficulties. In addition to general challenges regarding formats, numbering, etc., the biggest challenge lies in the structure of an ICP.

An ICP fans out from left to right, meaning that the further to the right you go, the more cells are needed. If you realise afterwards that another cell is needed 'in the middle' or that a cell needs to be deleted, this can destroy the entire formatting.

5. The challenge of prioritisation

It is also important to explore the question space in order to prioritise it.[11] Recipients often ask questions that are too broad or even formulate topics instead of questions. A fictional example might be: 'Write something about the hacker attack on the Bundestag!' or 'What is the situation in Mali?' – such questions are also called 'give me everything questions' because they do not narrow down the scope of the question.

IRM or analysis staff often have to tame such questions and put them into the right form (see comments on content challenges). However, even experienced IRM or analysis personnel may adopt or formulate suboptimal questions and transfer them to an ICP comprising several hundred lines. In this case, the

[9] Questions are incorrect if they predictably waste the time and attention of the analysts. For example, because a closed question is formulated for which there is insufficient information to provide a definitive answer and it is already foreseeable that this situation will not change. See Donner/Gnad/Pherson (2024): Klarheit im Denken: Theorie und Praxis strategischer Vorausschau und strukturierter Analysetechniken, Springer, p. 29 f.
[10] Questions may be poorly formulated if they are too broad or too narrow depending on the context, if they are assumption-driven, rhetorical questions or poorly defined questions. See Donner et al., ibid., p. 31 f.
[11] See Civil-Military Cooperation Centre of Excellence: NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5, p. 19.

question requirements are organised, but an Excel spreadsheet comprising several hundred lines is ultimately nothing more than a formalised equivalent of a 'give me everything question'.

It can be easy to get lost in the question space. That is why it is important to prioritise questions. In this way, it is possible to decide at the end which questions are not relevant. These questions can then be deleted from the ICP or not included in the first place.

6. Use of LLMs for ICP generation

As already described, the ICP is a central tool within the intelligence cycle for ensuring targeted, transparent and professional processing. In practical work, however, analysts are regularly confronted with the content, time and technical challenges described above, as well as challenges of prioritisation. The ICP-LLM development project, a collaboration between the Northern Business School, Strukturierte Analyse Deutschland and the NATO Civil-Military Cooperation Centre of Excellence, is investigating in practical terms the extent to which LLMs can support the creation of ICPs and thus address these challenges. The ICP-LLM tool developed for this purpose automatically creates the SIR and EEI levels of an ICP based on CCIRs and PIRs formulated by the user.

The overview presented in Table 1 shows some of the opportunities and challenges anticipated by the authors and participants to date in the design of an LLM-supported Intelligence Collection Plan (ICP). These factors represent a systematic selection that can be taken into account for the subsequent evaluation and validation of such a system.

Category	Topic/aspect (attribute)	Potential (advantage)	New challenges (disadvantage)
Process & efficiency	Creation speed & agility	B Acceleration & iteration: Significantly faster creation and flexible, iterative adaptation of the plan to dynamic situations.	I Initial effort & implementation time: High initial configuration, training and validation effort prior to operational use.
	Resource allocation & optimisation	Gap/redundancy analysis: Automatic identification of information gaps and redundancies. Optimised prioritisation: Data-driven suggestions for the optimal allocation of collection resources.	Resource reallocation: Engagement of IT and subject matter experts for model maintenance (governance) rather than direct analysis.
	Auditability & reproducibility	Logging & standardisation: Option for seamless logging of inputs (prompts) and standardisation of the creation process.	„ 'Black box' problem & stochastics: Limited transparency of LLM decision-making; lack of determinism (the same input does not necessarily produce exactly the same output).
	---	---	---
Personnel & Competence	Cognitive Performance & workload	Relief & fatigue protection: Reduction of routine tasks; analysts focus on complex analysis instead of plan creation.	A Automation bias & 'de'-skilling: Risk of over-reliance and reduction of critical thinking in plan validation.
	Competence profile & training	Knowledge management & upskilling: LLM as a training tool; shift towards specialised analytical/technical roles (e.g. validation).	Skills gap & new demand: Acute need for new skills (prompt engineering, model governance, AI ethics)
	Human-machine interaction	„Ideation Partner" [Kim/Maher]: Generation of insights or alternative approaches that a homogeneous team (without divergence) might overlook.	I Interaction complexity: The quality of the output depends on the quality of the (often difficult to formulate) input (prompts).
	---	---	---
Technology & data	Data security & confidentiality	Data sovereignty (on-premise): Local implementation (instead of cloud) improves control over sensitive data and queries.	Security risks: Risk of data leaks (especially when using the cloud) and vulnerability to prompt injections (manipulation of output through input).
	Model reliability & factuality	K Consistency: Consistent output quality, regardless of human daily form or fatigue.	Hallucinations & factuality: Risk of incorrect, 'invented' plan content that appears plausible but is factually incorrect.
	Currency & context	Real-time connection (RAG): Potential for connection to current situation databases using 'retrieval-augmented generation' (RAG)[Lewis].	Static knowledge base: Basic models are based on static training data and are not aware of the current situation (without RAG or fine-tuning).

Table 1: Some opportunities and challenges of ICP-LLM

These aspects are analysed in more detail below, contextualised and supplemented with new and additional detailed information to ensure a comprehensive understanding of the topic.

In the literature, the use of LLMs within the intelligence cycle has so far been discussed primarily in the collection and processing phases. Examples include applications in the automatic evaluation and structuring of cyber threat reports[12] and the visualisation of data sets.[13] In addition, further applications for increasing general productivity, automatic software programming and the autonomous generation of intelligence reports are also being discussed.[14] The ICP-LLM development project now aims to evaluate the extent to which productivity can also be increased in the direction phase through the use of LLMs.

Based on tests with LLMs, experience from practical work with ICPs, and the literature, ICP-LLM could address the challenges described above in four ways. On the one hand, automation should significantly speed up the process of creating an ICP, as the formulation of SIRs and EEIs takes up most of the time. This would make it easier for analysts to deliver results even within tight time constraints and complete well-founded analyses in time to have an impact (speed of relevance). Another advantage could be that the LLM does not tire: even with extensive ICPs, some of which comprise hundreds of EEIs, this ensures that every question consistently follows the specified structure and criteria of the ICP. This could improve the structure and detail compared to ICPs created by humans.

In addition, the time saved by automatically generating the lower levels of the ICP could allow analysts to invest more resources in precise formulation and prioritisation at the CCIR and PIR levels. This factor could contribute to better questions being asked at the beginning of the ICP, thereby addressing the content and prioritisation challenges. Direct integration into Microsoft Excel is intended to ensure a low barrier to entry, and automatic formatting removes another technical hurdle for analysts. This is intended to address the technical challenge of time-consuming Excel formatting.

In summary, ICP-LLM could enable analysts to create ICPs more quickly, consistently and user-friendly through the automated creation of SIRs and EEIs, thereby addressing the challenges described above.

7. Technical implementation and workflow ICP-LLM

The technical implementation of ICP-LLM and the work process of analysts using the software are explained below. Basically, ICP-LLM is a Python script integrated into an Excel macro file that embeds the CCIRs and PIRs provided by the user into structured prompts and sends them to an LLM via the

[12] See Tseng/Yeh/Dai (2020): Using LLMs to Automate Threat Intelligence Analysis Workflows in Security Operation Centers, in: JOURNAL OF LATEX CLASS FILES, VOL. 18, NO. 9, online: https://doi.org/10.48550/arXiv.2407.13093 [Access: 29.10.2025].
[13] See Xavier et al., LLM-Powered Multi-Actor System for Intelligent Analysis and Visualization of IEC 61499 Control Systems, in: IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society, online: https://doi.org/10.1109/IECON55916.2024.10905502 [Access: 29.10.2025].
[14] See Adam/Carter: Large Language Models and Intelligence Analysis, in: Centre for Emerging Technology and Security Expert Analysis, online: https://cetas.turing.ac.uk/sites/default/files/2023-07/cetas_expert_analysis_-_large_language_models_and_intelligence_analysis.pdf

OpenAI API. The SIRs and EEIs generated in response are then structured, filtered and presented to the user in Excel by the script. The entire programme is operated via the Excel macro file, so no prior technical knowledge is required and no pre-installation is necessary.

The user's workflow is as follows:

1. At the beginning, the user defines CCIRs and PIRs based on the analytical task. This ensures that the focus of the content is precisely tailored to the task. In addition, the analyst describes the context and background of the analytical task so that ICP-LLM can take this into account.

2. ICP-LLM then begins generating the SIRs and EEIs. To do this, it first imports the Excel data into the Python environment via xlwings and formats it.

3. The OpenAI model is then presented with the ICP concept and the specific context for the query. After that, iterative creation begins: first, a SIR is generated, followed by the corresponding EEIs. In each step, all CCIRs, PIRs and previously generated SIRs are included to ensure clear distinctions between the questions and to avoid duplication.

4. The script then filters and structures the results.

5. The finished ICP is then transferred back to Excel via xlwings, where it is automatically formatted and made easily accessible and editable for the analysis staff.

Depending on the scope of the ICP, the process takes between one and five minutes. Assuming that the recommended OpenAI model o4-mini is used, the cost of API usage ranges from €0.50 to €3 per ICP, depending on the size of the document created.

In developing ICP-LLM, a balance had to be found between accessibility for users, the quality of the models used and the development effort. The main script of ICP-LLM was programmed in Python, as Python can be integrated directly into an Excel macro file via the xlwings library. In addition, ICP-LLM can be used directly by the user without any pre-installation thanks to the Python embedded installation included in the download. The combination of Python and an Excel file with specifically programmed macros therefore makes it possible to reduce the entry barrier, as no prior technical knowledge is required and the programme can be integrated directly into existing work processes. At the same time, the development effort within the scope of an evaluation project could be limited by using existing libraries.

LLMs from OpenAI are used for data processing and question generation via an API interface. This decision was made in order to enable access to leading models in comparisons[15], even on computers with limited computing power, and thus to be able to evaluate the potential usability of the most advanced models currently available. In addition, the connection via an API allows new, improved models to be quickly integrated into the existing script. One disadvantage is that the API connection requires a permanent internet connection and no confidential data can be processed. The integration of locally hosted LLMs is therefore a necessary next step in development in order to be able to use ICP-LLM in other fields of application. If the benefits of LLMs in the ICP creation process are successfully validated, these and other developments described in the outlook are planned.

8. Evaluation

ICP-LLM will be tested as part of the *NATO CIMIC Analysis and Assessment Course*[16] at the NATO CIMIC Centre of Excellence, although it is clear that statistical significance cannot be achieved due to the size and composition of the group.

The following two research questions will be addressed:

1) To what extent can the use of the ICP-LLM tool significantly reduce the time required to create intelligence collection plans across all phases without compromising the quality of the results?

2) How is the ICP-LLM tool rated by intelligence analysts in a training context in terms of user-friendliness and quality of results for the analysis process?

The following hypotheses have been formulated with regard to the research questions and will be tested as part of the NATO CIMIC Analysis and Assessment Course:

1.1 The use of ICP-LLM can significantly reduce the time required to create a complete ICP.

2.1 Participants rate ICP-LLM as user-friendly and easy to integrate into existing workflows.

2.2 ICPs created with ICP-LLM exhibit greater structural consistency (clear hierarchy, correct links between CCIR, PIR, SIR and EEI levels) than manually created ICPs.

ICP-LLM is to be used at a later date and in a further step as part of a research project at I2SM on organised crime in the context of crime analysis. With the help of ICP-LLM, comprehensive information on Italian organised crime should be obtained, allowing conclusions to be drawn that go beyond the

[15] Artificial Analysis: LLM Leaderboard - Comparison of over 100 AI models from OpenAI, Google, DeepSeek & others, online: https://artificialanalysis.ai/leaderboards/models [Access: 29.10.2025].
[16] For an overview of how the ICP is normally taught at the NATO CCOE, see Appendix B.

findings of the authorities to date. Crime analysis is a goal-oriented process in which Structured Analytic Techniques, Methods and Techniques are applied in compliance with standards to generate usable knowledge products from data and information. In this process, a situation or question is first broken down into relevant separate questions and hypotheses are formulated. Data and information are collected in a targeted manner, modelled, viewed from different angles and evaluated. The results of the individual questions are brought together, interpreted in the respective context and communicated in a manner appropriate to the target audience. They serve as a basis for security-related action. The methodology of crime analysis has so far been used almost exclusively by the police.[17] However, crime analysis is also relevant to privatesector security[18] and is becoming increasingly important, as strategic crime analysis is used to observe, classify and clearly present crime trends. This provides a basis for decision-making when setting priorities in the fight against crime, developing action plans, managing resources and deriving measures. In the future Master's programme 'Corporate Security & Interdisciplinary Criminology' at NBS, Structured Analytic Techniques and Crime Analysis will be taught in a separate module. In addition to teaching the theoretical basics, the findings from this research project will also be directly incorporated into the course content.

9. Outlook

The development of ICP-LLM exemplifies the potential of using large language models for creating an ICP in an intelligence context. While the basic principles of the intelligence cycle and intelligence requirement management remain unchanged, LLM-supported tools open up new possibilities for automating time-consuming work steps, reducing time bottlenecks and ensuring the methodological consistency of preliminary analysis products.

The upcoming testing of the tool as part of the NATO CIMIC Analysis and Assessment Course and in the field of crime analysis offers an opportunity to empirically verify these theoretical assumptions. The testing will not only examine whether ICP-LLM accelerates the creation of intelligence collection plans, but also how the tool is perceived by users in training and practical environments.

Beyond the planned evaluation, further fields of research are opening up: for example, future work could investigate the integration of locally hosted LLMs for processing sensitive data. The integration of feedback mechanisms that allow the model to continuously learn from the evaluations of experienced analysts would also be conceivable.

[17] For application in policing, see: German Police University: In-service training in crime analysis, online: https://www.dhpol.de/departments/department_III/FG_III.2/fortbildung-kriminalitaetsanalyse.php [Access: 29.10.25].
[18] For an easily accessible overview (in German), see: German Intelligence Podcast, Season 1, online: https://open.spotify.com/show/2mlMdBVLzMABp2f9g93c3k [Access: 29 .10.25].

10. Feedback and further development

The development of ICP-LLM is an open, iterative project that thrives on feedback from research and practice. Comments, suggestions for improvement, or reports on experiences with the application are expressly welcome and contribute to further optimizing the tool and its possible uses.

Contact:

niklas.koch@i2sm.nbs.de

Annex A)

Experimental setup

Element	**Description**
Setting	NATO CIMIC Analysis and Assessment Course (CCOE)
Participants	Course attendees (CIMIC & Analysis practitioners or students), divided into two groups of similar experience.
Design	Controlled comparative study with two groups: – Group A: Manual ICP creation (experimental group) – Group B: ICP-LLM-assisted ICP creation (control group)
Task	Both groups receive the same scenario and one PIR (Priority Intelligence Requirement) and are asked to develop the missing part of the corresponding ICP (SIRs and EEIs).
Duration	~90 minutes total (including briefing, task execution, debrief, feedback).

Excerpt from evaluation methodology

Variable	Metric	Collection Method
Time efficiency	Total time (minutes) to complete ICP (separated in different phases including recovery time)	Stopwatch
Structural consistency	Number of correctly linked question hierarchies (PIR–SIR–EEI)	Expert evaluation rubric
Output volume	Number of complete SIRs and EEIs produced	Manual count
Output Content	Usefulness and completeness	Comparison of both ICPs (Group A and Group B) Evaluation of used Prompt Evaluation of Recall and Precision Model Gap evaluation
User Experience (UX)	Aggregate average rating by test participants	Post-exercise survey e.g. "The tool was easy to use." (1–5)

Survey Questions (Post-Exercise)

Section A: Tool Experience (1 = strongly disagree, 5 = strongly agree)

- The tool was intuitive and easy to use.
- The tool's integration in Excel supported my workflow.
- The automated generation of SIRs and EEIs saved me significant time.
- I trust the logical consistency of the generated questions.
- I would use this tool in my daily work if available.

Documentation & Deliverables

- Screenshots or copies of completed ICPs from both groups.
- Completed surveys and time logs.

Annex B)

Use Case: Manual Establishment of an Intelligence Collection Plan (ICP) within the NATO CIMIC Analysis and Assessment Course (NCAAC)

1. Context

The NATO CIMIC Analysis and Assessment Course (NCAAC), conducted twice a year at the Civil-Military Cooperation Centre of Excellence (CCOE), is aimed at future CIMIC Analysts, as well as CIMIC and other staff members who are or will be involved in establishing the understanding of the Civil Factors of the Operating Environment (OE).

The course focuses on the CIMIC Analysis and Assessment Workflow (NCAA Workflow) - an adapted model of the Intelligence Cycle - comprising four main phases: Direction, Collection, Processing, Dissemination.

Each phase includes a series of tasks and sub-tasks designed to equip students with the skills and structured analytic discipline required to support decision-making within NATO operations.

2. Exercise Situation: Establishment of an ICP in the Direction Phase

Very early in the Direction Phase, NCAAC students are introduced to a developing but fictive operational scenario designed to simulate a complex civil-military environment. In this context, they are tasked to establish an Intelligence Collection Plan (ICP) related to civil factors that must be addressed by CIMIC in response to the Commander's Critical Information Requirements (CCIRs).

The ICP, ideally a collaborative headquarters product, serves during the course as a training tool to: Transform the CCIRs into Priority Intelligence Requirements (PIRs), Specific Intelligence Requirements (SIRs) and Essential Elements of Information (EEIs);

Provide a structured framework that links each level of requirement and ensures that subsequent collection activities can be effectively directed and coordinated; Train students in systematic reasoning, information prioritisation, and team-based analytic problem-solving.

3. Aim of the Exercise

The aim of this exercise is to enable students to understand, construct, and present a comprehensive and coherent part of the Intelligence Collection Plan by practicing the logic and mechanics of the CIMIC Analysis and Assessment Workflow.

The ICP should: Ultimately translate CCIRs related to civil factors into actionable and logically derived EEIs; Form the foundation for the Collection Phase of the NCAA Workflow; Demonstrate students'

understanding of how to operationalise information requirements into a practical and prioritised collection framework.

4. Learning Process and Methodology

After being introduced to the art of asking the right questions, students are guided through the Structured Analytic Technique (SAT) - Issue Redefinition, which helps refine and sharpen their initially broad Intelligence Requirements (IRs) into clear, targeted questions.

Following this analytic refinement, students are introduced to: The purpose and logic of an Intelligence Collection Plan; The structure and format of an ICP; The mechanisms by which an ICP directs collection, establishes coordination, and provides traceability from requirement to collection activity.

5. Execution

The class is divided into three syndicates of equal size and experience. Each syndicate is equipped with laptops for each student and a smart board in their syndicate room. Each group selects one redefined question from their collectively generated set of refined intelligence questions. Using the given ICP format, they must break the question down logically into: Priority Intelligence Requirements (PIRs), Specific Intelligence Requirements (SIRs), Essential Elements of Information (EEIs).

Each EEI should provide enough precision and direction to guide further analytical and collection activities, ensuring that each SIR and PIR can be fully addressed.

The available time for the exercise is 45 minutes.

After completion:

Each syndicate presents its partial ICP in plenary session. The results are first subjected to peer critique from the other syndicates, followed by a professional assessment from the Subject Matter Expert (SME). Feedback focuses on the clarity, completeness, logic, and feasibility of the ICP and its ability to serve as a practical basis for subsequent collection activities.

6. Observations and Lessons Identified

Time Consumption and Quality Dependency

Establishing a quality ICP manually is highly time-consuming, as it requires both analytical rigour and collaborative reasoning. Students must interpret CCIRs accurately, prioritise requirements, ensure logical consistency between levels (PIR-SIR-EEI), and define the corresponding collection tasks.

Because the task is allotted only 45 minutes, students experience a realistic operational time constraint that forces them to prioritise and manage their workflow under pressure. This often leads to the following learning observations:

When sufficient time and structured teamwork are applied, syndicates can produce detailed, logically connected, and actionable partial ICPs that effectively guide the following Collection Phase.

When time pressure dominates, results often show: Vague or overlapping EEIs; Missing links between CCIRs and EEIs; Incomplete prioritisation or poor feasibility; Reduced clarity in tasking and coordination instructions.

This mirrors the real-world challenge of producing intelligence planning products under operational tempo, where inadequate time allocation can significantly degrade collection focus and, consequently, overall mission understanding.

8. Conclusion

The manual establishment of a partial ICP in the NCAAC represents a core experiential learning element. While time-consuming, the process provides essential hands-on practice in critical thinking, structured reasoning, and collaborative problem-solving. Conversely, the observable decline in quality under time pressure serves as a valuable pedagogical reminder: a rushed ICP leads to flawed collection and weaker analytical outputs, potentially undermining the required understanding of the Civil Factors of the Operating Environment and decision-making at all levels.

Quellen- und Literaturverzeichnis

Adam/Carter: Large Language Models and Intelligence Analysis, in: Centre for Emerging Technology and Security Expert Analysis, online: https://cetas.turing.ac.uk/sites/default/files/2023-07/cetas_expert_analysis_-_large_language_models_and_intelligence_analysis.pdf [Access: 26.10.2025].

Artificial Analysis: LLM Leaderboard - Comparison of over 100 AI models from OpenAI, Google, DeepSeek & others, online: https://artificialanalysis.ai/leaderboards/models [Access: 26.10.2025].

Davies, Philip et al. (2013): The Intelligence Cycle is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine, in: Phythian, Mark (ed): Understanding the Intelligence Cycle, Studies in Intelligence, Routledge, S. 67-85.

Civil-Military Cooperation Centre of Excellence (2025): NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5.

Deutsche Hochschule der Polizei: Berufsbegleitende Fortbildung Kriminalitätsanalyse, online: https://www.dhpol.de/departments/department_III/FG_III.2/fortbildung-kriminalitaetsanalyse.php [Access: 29.10.2025].

Donner/Gnad/Pherson: Klarheit im Denken (2024): Theorie und Praxis strategischer Vorausschau und strukturierter Analysetechniken, Springer.

German Intelligence Podcast, Staffel 1, online: https://open.spotify.com/show/2mlMdBVLzMABp2f9g93c3k [Access: 29.10.2025].

Headquarters Department of the Army FM 34-2 (1994): COLLECTION MANAGEMENT AND SYNCHRONIZATION PLANNING, APPENDIX A THE COLLECTION PLAN, online: https://irp.fas.org/doddir/army/fm34-2/Appa.htm#Appa [Access: 23.10.2025].

Kim, J. / Maher, M. L. (2023): The effect of AI-based inspiration on human design ideation, Int. J. Des. Creat. Innov., Bd. 11, Nr. 2, S. 81–98, doi: 10.1080/21650349.2023.2167124.

Lewis, P. et al. (2020): Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks, arXiv. doi: 10.48550/ARXIV.2005.11401.

NATO STANDARD AJP-2 (2020): ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition B Version 1.

Tseng/Yeh/Dai (2020): Using LLMs to Automate Threat Intelligence Analysis Workflows in Security Operation Centers, in: JOURNAL OF LATEX CLASS FILES, VOL. 18, NO. 9, online: https://doi.org/10.48550/arXiv.2407.13093 [Access: 29.10.2025].

United Nations 2025: Lesson 3.5 PKISR Requirements Management and Prioritisation, online: https://resourcehub01.blob.core.windows.net/training-files/Training%20Materials/042%20PKISR%20RTP/042-012%20PKISR%20RTP%20Lesson%203.5%20Requirements%20management%20and%20prioritisation.pdf [Access; 23.10.2025].

Xavier et al.: LLM-Powered Multi-Actor System for Intelligent Analysis and Visualization of IEC 61499 Control Systems, in: IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society, online: https://doi.org/10.1109/IECON55916.2024.10905502 [Access: 29.10.2025].

About the Institute

The Institute for Intelligence and Security Management (I2SM) is an interdisciplinary institute at the Northern Business School (NBS) in Hamburg. The institute currently comprises six professors, twelve research fellows, and several student assistants working on project-related tasks. Through this diverse team, the institute covers a broad range of disciplines, including criminal law and criminal procedure, corporate and economic criminal law, criminology, forensic science, IT security, security management, security engineering and robotics, business psychology, intelligence and analysis, crisis management, threat management, resilience management, risk management, strategic foresight, and corporate security.

In addition to its strong practical orientation in teaching, research is a central pillar of the NBS. The I2SM is one of six research institutes at the NBS. Numerous early-career researchers are already involved in various projects at the I2SM, either as research fellows or as student assistants. In particular, students from the Bachelor's program in Security Management—and in the future also from the Master's program in Interdisciplinary Criminology and Corporate Security—are given the opportunity to gain early insights into research activities and to independently develop subprojects, often as part of term papers, internships, or final theses.

Moreover, students have the chance to collaborate across disciplines with other institutes at NBS as well as with public authorities and private-sector organizations, fostering innovation and the development of new ideas. Since the mandatory internships are highly practice-oriented, the I2SM continuously benefits from the current practical input and perspectives provided by the students.

About the authors

Ralf Baur (OF-4, DEU Air Force) was serving as Liaison and Exchange Officer with the Dutch 1 Civil-Military Interaction Command in Apeldoorn, The Netherlands, before joining the CIMIC Centre of Excellence in February 2020. Prior to his first encounter with the CIMIC Centre of Excellence from 2010-2016, within the capacity of a trainer and course developer, he was serving with the predecessor organisation of the Multinational CIMIC Command in Nienburg, Germany. He is looking back to more than 20 years of experience within the capacity of Civil-Military Cooperation.

Lieutenant Colonel Ralf Baur's mission record involves missions in Bosnia-Herzegovina, Kosovo and multiple times Afghanistan where he had experienced different CIMIC positions within Provincial Reconstruction Teams (PRT), Regional Command North (RC N) and ISAF Headquarters.

For his latest mission in Afghanistan, he was asked to join a US-led Fusion Centre, were he was responsible for CIMIC data and information to be fused with traditional intelligence aiming at providing the commander with a more accurate assessment of his Area of Operations.

Employing his wide network of military and civilian partners and experts, he has developed the CIMIC Analysis and Assessment Concept and the respective training solution, the NATO CIMIC Analysis and Assessment Course. He recently founded the Civil-Military Cooperation wargame ANALYSIA which supports its participants to think along the lines of civil factor integration (CFI) as one of the two interacting core activities of Civil-Military Cooperation.

Ole Donner is the founder of Strukturierte Analyse Deutschland. In this position, he acts as trainer and consultant for governmental institutions such as the Criminal Police, intergovernmental organizations such as NATO as well as national and international business enterprises to increase their respective intelligence and analysis capabilities.

Mr. Donner looks back on 13 years of service with the Federal Armed Forces of Germany, which provided him with extensive experience as All-Source-Analyst, Intelligence manager and lecturer. During his service, Mr. Donner redesigned the analysis training of the German Armed Forces, focusing heavily on the competency-based teaching of Structured Analytic Techniques (SATs). He also contributed to the development of executive training in the field of "Intelligence Leadership" at the Military Academy of the German Armed Forces in Hamburg.

He is co-author of the books Clear Thinking and Klarheit im Denken , published by Springer-Verlag. He is also the initiator of the German Intelligence Community Conference (GICC), research fellow at the Institute for Intelligence Security Management (I2SM) at the Northern Business School Hamburg, and Regional Director Europe of the International Association of Intelligence Education (IAFIE).

Ole Donner received a Bachelor's degree in Political Science and a Master's degree in International Relations from the University of the Armed Forces in Hamburg and was awarded the Böttcher Prize as best in his graduating class.

Niklas Koch holds dual Bachelor’s degrees in Economics and International Affairs from the University of St. Gallen and is currently pursuing a Master’s degree in Economics at the University of Mannheim. His academic focus lies at the intersection of security, energy, and economic policy, with a particular emphasis on Northern and Eastern Europe. His research has examined, among other topics, the economic and structural consequences of the Nord Stream pipeline attacks on the European gas market.

He gained practical experience in international security and economic structures through positions at the German-Baltic Chamber of Commerce in Lithuania and the NATO Civil-Military Cooperation Centre of Excellence in the Netherlands. During his time in Lithuania, he obtained first-hand insights into the security dynamics of the Baltic region and contributed to analyses of the local defense industry ecosystem. His internship at NATO’s CIMIC Centre further deepened his expertise in civil-military analysis and the application of structured analytical techniques for complex security assessments.

Professionally, Niklas Koch has been working as a freelance developer, consultant, and serious game designer in the field of security and foreign policy for several years. He independently designs and leads simulation-based projects on strategic decision-making and resilience for clients such as the First German Netherlands Corps, the University of St. Gallen, and various insurance companies. In addition, he contributed as a developer to the ICP-LLM research project, which explores the integration of large language models into analytical and strategic decision processes.

André Schulz is a Professor of Criminological Sciences and Head of the Institute for Intelligence and Security Management (I2SM) at the NBS. He holds both commercial and protective/criminal police training and studied Public Administration (Police), Business Law, Business Administration, Criminology, and Police Science. In addition, he completed a doctoral program in Law at the Faculty of Law of Ruhr University Bochum.

Schulz has over 30 years of experience in criminal police investigations and possesses extensive expertise in policy consulting at both the state and federal levels, in corporate and association management, in employee representation, as well as through his work at one of the “Big Four” auditing firms. He also holds certifications as a Compliance Manager, Project Manager, and Inter-/Transcultural Trainer.

Richard Weiss worked as a reverse engineer in the FLARE team at Mandiant (now part of Google Cloud) and devotes his professional and personal time to integrating intelligence methodologies and other scientific disciplines, such as mathematics, data sciences and data mining, into the cyber threat intelligence (CTI) context. The standardisation of CTI working methods across different areas of responsibility also plays a crucial role in this. To this end, he has been invited to speak at CyCon – organised by the CCDCOE – for the second time in a row and has also presented a small excerpt of his work at other conferences. Richard Weiss maintains close ties to the public sector. In his spare time, he has also mentored ENISA's European Cybersecurity Challenge Team in preparation for the ICSC and students from Neuland e.V. at the Technical University of Ingolstadt.