

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

Working Paper

Entwicklung eines ICP-LLM zur Unterstützung der Erstellung eines Intelligence Collection Plans (ICP)

Working Paper des Studiengangs Sicherheitsmanagement an der 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) : Entwicklung eines ICP-LLM zur Unterstützung der Erstellung eines Intelligence Collection Plans (ICP), Working Paper des Studiengangs Sicherheitsmanagement an der 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/10419/330339>

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.

**Working Paper des Studiengangs Sicherheitsmanagement
an der NBS Northern Business School Hamburg
Institute for Intelligence and Security Management (I2SM)**

No. 3/2025

**Entwicklung eines ICP-LLM zur Unterstützung der Erstellung eines Intelligence
Collection Plans (ICP)**

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

Zusammenfassung

Die Erstellung eines Intelligence Collection Plans (ICP) stellt einen zentralen Arbeitsschritt im Schnittpunkt aus der *Direction*-Phase¹ (siehe Abbildung 1) und dem Intelligence Requirement Management (IRM) innerhalb des Intelligence Cycle dar. Dieser soll ermöglichen, Informationsbedarfe systematisch zu strukturieren und Recherche und Aufklärung zielgerichtet zu steuern. In der praktischen Anwendung sind jedoch zeitliche, inhaltliche und technische Herausforderungen zu beobachten, die zu Verzögerungen, Inkonsistenzen und Qualitätsverlusten führen können. Mit dem **ICP-LLM** wurde ein Tool entwickelt, das Large Language Models (LLMs) nutzt, um die unteren Ebenen eines ICP - *Specific Intelligence Requirements (SIRs)* und *Essential Elements of Information (EEIs)* - automatisiert zu generieren. Dadurch wird die Erstellung von ICPs beschleunigt und vereinfacht.

Ziel dieses Working Papers ist es, den Entstehungshintergrund von ICP-LLM zu beleuchten. Außerdem soll ein Blick darauf geworfen werden, wie der Nutzen und die Anwendbarkeit des Tools im Rahmen eines Lehrgangs am NATO Civil-Military Cooperation Centre of Excellence (CCOE) experimentell evaluiert wird. Untersucht werden soll, inwieweit der Einsatz von ICP-LLM die Erstellung von ICPs effizienter gestaltet, die Strukturqualität verbessert und von Anwenderinnen und Anwendern als praxisrelevant bewertet wird. Die Ergebnisse sollen exemplarisch Aufschluss darüber geben, ob und in welchem Umfang LLM-gestützte Assistenzsysteme einen Mehrwert für die Anwendung im Intelligence-Kontext bieten können. In einem weiteren Schritt soll das Tool bei einem Forschungsprojekt am I2SM zur Organisierten Kriminalität im Rahmen der Kriminalitätsanalyse einem Praxistext unterzogen werden.

¹ Im Prozessschritt *Direction* werden alle entscheidungsrelevanten Informationsbedarfe vom Entscheidungspersonal geäußert und vom Intelligence Requirement Management (IRM) systematisiert und in Form gebracht. Siehe hierzu: Civil-Military Cooperation Centre of Excellence: NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5, S. 16 ff.

1. Zur Rolle von Intelligence Collection Plans

Intelligence dient dazu, Entscheidungsträgerinnen und Entscheidungsträgern in Unternehmen und staatlichen Institutionen einen Informations- und Entscheidungsvorsprung gegenüber Konkurrenten oder Gegnern zu verschaffen. Damit das funktionieren kann, ist die Bereitstellung von entscheidungsrelevanten Intelligence-Produkten eine Voraussetzung. Was entscheidungsrelevant ist, sollte von denjenigen, die Entscheidungen treffen müssen, selbst definiert werden. Um das zu gewährleisten, nutzt die Intelligence Welt als Rahmenprozess den sogenannten Intelligence-Cycle² (siehe Abbildung 1).

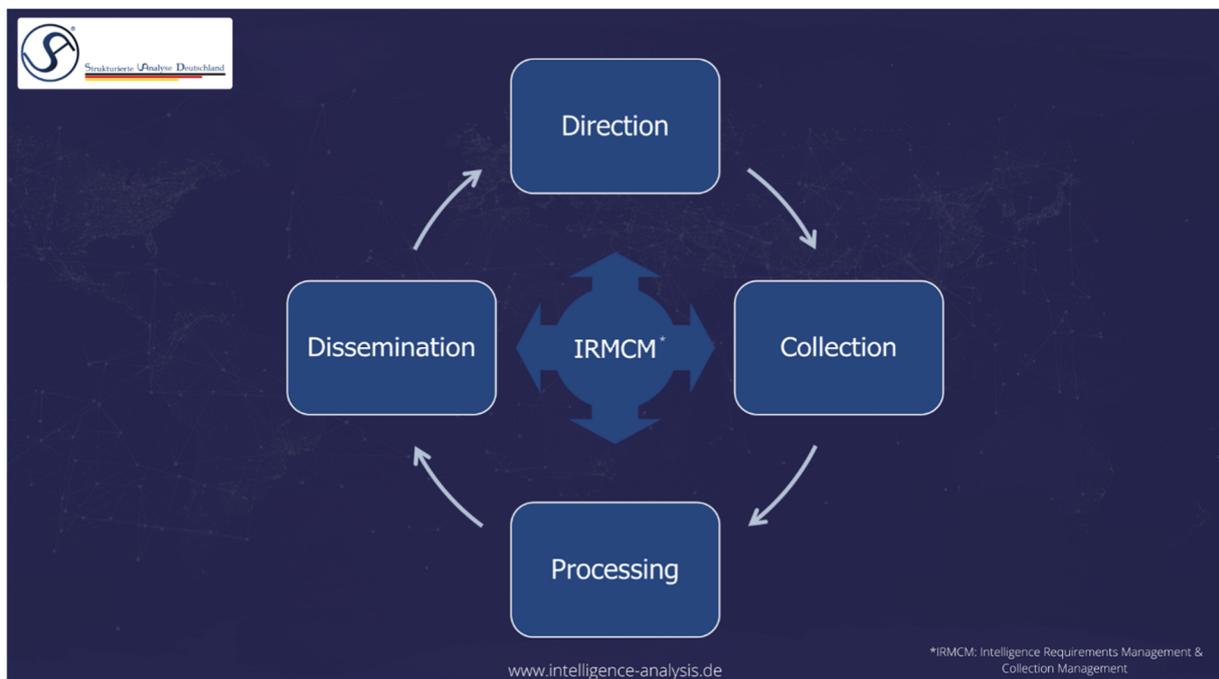


Abbildung 1: Intelligence Cycle, eigene Darstellung, 2025.

Im Prozessschritt Direction werden alle entscheidungsrelevanten Informationsbedarfe vom Entscheidungspersonal geäußert und vom Intelligence Requirement Management (IRM) systematisiert und in Form gebracht.³ Im Zuge dessen ist es oftmals notwendig, gestellte Fragen umzuformulieren oder zu operationalisieren. Beim Umformulieren kann davon gesprochen werden, dass eine ursprünglich gestellte Ausgangsfrage in eine Kernfrage überführt wird. Dies kann notwendig werden,

² Der hier zu Grunde liegende Ansatz ist der eines Rahmen-Verständnisses des Intelligence Cycle (Intelligence Cycle as a framework) und nicht eines prozeduralen Verständnisses (proceduralist approach to the Intelligence Cycle.) Siehe hierzu: 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.

³ Vgl. Civil-Military Cooperation Centre of Excellence: NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5, S. 16 ff.

wenn die Ausgangsfrage falsch formuliert wurde. Spielarten falsch formulierter Fragen sind zu weit oder zu eng formulierte Fragen, Fragen bei denen die Antwort bereits unterstellt wird oder annahmengetriebene Fragen. Die umformulierten Kernfragen sind in der Regel relativ weit gefasst, sodass diese operationalisiert und in Teilfragen zerlegt werden müssen. Hierbei können unterschiedliche Strukturierte Analysetechniken (SATs) wie die Issue Redefinition oder das Analytische Spektrum zum Einsatz kommen.

Umformulierung, Operationalisierung und Zergliederung in Teilfragen werden durch das IRM-Personal, in der Regel in Kooperation mit dem Analysepersonal vorgenommen. Die NATO nutzt zur Unterstützung dieses Prozesses das Werkzeug des Intelligence Collection Plans (ICP).

In einem ICP werden die ursprünglich gestellten Fragen – Commander's Critical Information Requirements (CCIRs)⁴ – in kleinere Teilfragen (Priority Intelligence Requirements / PIRs⁵) zerlegt. Die Systematik dahinter sieht vor, dass ein CCIR in eine beliebige Anzahl von PIRs zerlegt werden kann. Die Beantwortung aller PIRs sollte dann der Beantwortung des CCIR gleichkommen. Oder anders formuliert: Wenn alle PIRs beantwortet werden können, kann auch der CCIR beantwortet werden, für den diese PIRs erarbeitet wurden.

Jeder PIR wird dann in eine beliebige Anzahl von Specific Intelligence Requirements (SIRs)⁶ heruntergebrochen. Die vorhergehend angewandte Systematik bleibt hierbei gleich: Können alle für

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 hierzu: NATO STANDARD AJP-2 ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition B Version 1 JULY 2020; siehe auch: 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> [Zugriff: 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.", siehe: NATO STANDARD AJP-2, a.a.O.

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.", siehe: NATO STANDARD AJP-2, ebd.

ein PIR entwickelten SIRs beantwortet werden, ermöglicht dies die Beantwortung des dazugehörigen PIR.

Am Ende werden dann alle SIRs in Essential Elements of Information (EEIs)⁷ heruntergebrochen. Die Systematik bleibt abermals gleich. Nur der Fragentypus, dem ein EEI entsprechen sollte, ändert sich. Denn EEIs sollten nach Möglichkeit so formuliert werden, dass sie binär, kategoriebasiert oder mit einer Zahl beantwortet werden können (siehe Abbildung 2).

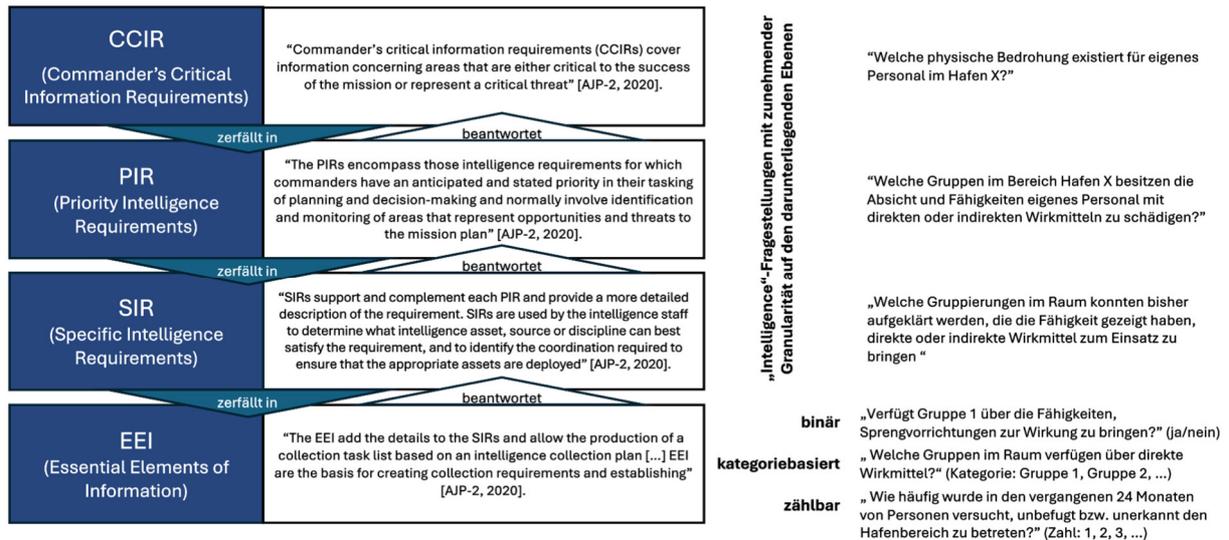


Abbildung 2: Intelligence Collection Plan, eigene Darstellung, 2025.

Der ICP dient als Organisationshilfe für die Entscheidung, welche Fragen im Prozessschritt *Processing* beantwortet werden und welche Fragen zu Collections Tasks umgewandelt werden. Diese können dann durch den Collection Manager (dem CM in IRMCM) in Absprache mit den Aufklärungsdisziplinen bzw. Sensoren in Collection Tasks umgewandelt werden. Ist ein Sensor gefunden, der einen EEI aufklären kann und der auch bereit ist, diese Aufgabe zu übernehmen bzw. der angewiesen werden kann, so kann auch dies auf dem ICP vermerkt werden. Zudem sollte auch der Zeitpunkt festgehalten werden, ab dem die Beantwortung einer Frage keinen Mehrwert mehr erzielt (Last Date of Intelligence Value).

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 and establishing", siehe: NATO STANDARD AJP-2, a.a.O., siehe auch: 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> [Zugriff; 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?
		1.1.2 ...	1.1.1.2 Does the Russian-speaking Minority possess SALW?
			1.1.1.3 Does the Russian-speaking Minority possess explosives?
			1.1.1.4 Does the Russian-speaking Minority possess means to jam signals?
			1.1.1.5 Does the Russian-speaking Minority have the capability to use SALW?
			1.1.1.6 Does the Russian-speaking Minority have the capability to use explosives?
			1.1.1.7 Does the Russian-speaking Minority have 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?
		1.1.4 ...	1.1.1.11 How has the Russian-speaking Minority harmed NATO Troops in the past?
			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 ...

Abbildung 3: Beispiel eines partiellen Intelligence Collection Plans, eigene Darstellung, 2025.

Die Erstellung eines ICP ist mit einer Reihe an Herausforderungen verbunden. Neben inhaltlichen Herausforderungen, die mit der Identifikation der richtigen und richtig formulierten Fragen zu tun haben, gibt es auch zeitliche und technische Herausforderungen sowie Herausforderungen der Priorisierung.

2. Zeitliche Herausforderungen

Intelligence kann ein schnelllebiges Geschäft sein. Was heute noch entscheidungsermöglichende Erkenntnisse sind, welche die relative Position der Entscheidungsträgerin oder des Entscheidungsträgers gegenüber Konkurrenten oder Gegnern maßgeblich verbessern, kann morgen irrelevant sein. Ist der Zeitpunkt überschritten, ab dem die Beantwortung einer Frage keinen Mehrwert mehr erzielt (Last Date of Intelligence Value), können Zeit und Aufmerksamkeit des Personals anderweitig investiert werden.

Die Generierung von Fragen, sowie das Organisieren und Priorisieren des Fragenraumes sollten daher so schnell wie möglich, aber so sorgfältig wie nötig erfolgen. Da das Erstellen eines ICP viel Zeit in Anspruch nehmen kann, stellen unterstützende Tools und Prozesse⁸ wirksame Mechanismen dar, um die Erstellung zu beschleunigen (Stichwort: Speed of Relevance).

⁸ Unter Prozessen sind hier formalisierte Abläufe gemeint, wie die Anwendung des Intelligence Cycles, Strukturierter Analysetechniken (SATs) und Feedbackschleifen zwischen allen beteiligten Akteuren, insbesondere der Führungsebene und den Bereichen IRMCM und Analyse.

3. Inhaltlichen Herausforderungen

Gute Intelligence- und Analysearbeit steht und fällt mit der Identifikation der richtigen Fragen. Werden falsche Fragen⁹ formuliert oder gute Fragen falsch formuliert¹⁰, führen auch höchste Anstrengungen in den Bereichen Collection und Processing nicht zu einer zielführenden Antwort. Denn die Wahrscheinlichkeit, dass trotz einer „suboptimalen Frage A“, aus Zufall die eigentlich von der Adressatin oder dem Adressaten gemeinte „optimale Frage A“ beantwortet wird, geht gegen Null. Das Erkennen schlechter und schlecht formulierter Fragen ist eine Fähigkeit, die Erworben und trainiert werden muss; ebenso wie die Umformulierung zu potenziell besseren Fragen.

4. Technische Herausforderungen

In vielen Unternehmen und Behörden gibt es keine speziell entwickelte Software für das Erstellen und gemeinsame Nutzen von ICPs. In der Folge greifen viele Organisationen auf MS Excel zurück. Dieses Tool kann die Struktur eines ICP im Prinzip darstellen und läuft auf den meisten Computern. Die Software bringt aber eine ganze Reihe an Schwierigkeiten mit sich. Neben allgemeinen Herausforderungen was Formate, Nummerierungen etc. angeht, liegt die größte Herausforderung in der Struktur eines ICPs.

Ein ICP fächert sich von links nach rechts auf – es werden also je weiter sich nach rechts bewegt wird, mehr und mehr Zellen benötigt. Fällt im Nachhinein auf, dass eine weitere Zelle „mittendrin“ gebraucht wird oder dass eine Zelle gelöscht werden muss, kann das zur Zerstörung der gesamten Formatierung führen.

5. Herausforderung der Priorisierung

Den Fragenraum zu erschließen ist auch deshalb wichtig, um ihn zu priorisieren.¹¹ Adressatinnen und Adressaten stellen häufig Fragen, die zu weit gefasst sind oder formulieren sogar Themen, statt Fragen. Ein fiktives Beispiel könnte lauten: „Schreiben Sie mal was zu dem Hackerangriff auf den Bundestag!“ oder „Wie ist die Lage in Mali?“ – solche Fragen werden auch „Gib mir alles Fragen“ genannt, denn sie grenzen den Fragenraum nicht ein.

⁹ Fragen sind dann falsch, wenn diese die Zeit und Aufmerksamkeit des Analysepersonals vorhersehbar verschwenden. Beispielsweise weil eine geschlossene Frage formuliert wird, für deren definitive Beantwortung nicht ausreichend Informationen vorliegen und bereits absehbar ist, dass sich an diesem Umstand nichts ändern wird. Vgl. Donner/Gnad/Pherson (2024): Klarheit im Denken: Theorie und Praxis strategischer Vorausschau und strukturierter Analysetechniken, Springer, S. 29 f.

¹⁰ Falsch formuliert können Fragen dann sein, wenn diese abhängig vom Kontext zu weit oder zu eng gefasst sind, diese annahmengengetrieben sind, rhetorische Fragen oder mangelhaft definierte Fragen. Vgl. Donner et al., ebd., S. 31 f.

¹¹ Vgl. Civil-Military Cooperation Centre of Excellence: NATO Civil-Military Cooperation Analysis and Assessment Concept, version 1.5, S. 19.

Oft müssen IRM oder Analysepersonal solche Fragen zähmen und in die richtige Form bringen (siehe Ausführungen zu inhaltlichen Herausforderungen). Es kann jedoch passieren, dass auch erfahrenes IRM oder Analysepersonal suboptimale Fragestellungen übernimmt oder formuliert und in einen hunderte Zeilen umfassenden ICP überführt. In diesem Fall ist der Fragenbedarf zwar organisiert, eine hunderte Zeilen umfassende Excel Tabelle ist allerdings am Ende nichts anderes als ein in Form gegossenes Äquivalent einer „Gib mir alles Frage“.

Es kann leicht sein, sich im Fragenraum zu verlieren. Deshalb ist es wichtig, dass Fragen priorisiert werden. Auf diese Weise kann am Ende entschieden werden, welche Fragen nicht relevant sind. Diese Fragen können dann aus dem ICP gestrichen oder gar nicht erst aufgenommen werden.

6. Nutzung von LLMs zur ICP-Generierung

Der ICP stellt, wie bereits dargestellt, ein zentrales Werkzeug innerhalb des Intelligence Cycles dar, um eine zielgerichtete, nachvollziehbare und professionelle Bearbeitung sicherzustellen. In der praktischen Arbeit sehen sich Analystinnen und Analysten jedoch regelmäßig mit den zuvor beschriebenen inhaltlichen, zeitlichen und technischen Herausforderungen, sowie Herausforderungen der Priorisierung konfrontiert. Das Entwicklungsprojekt ICP-LLM, eine Kooperation der Northern Business School, Strukturierte Analyse Deutschland und des NATO Civil-Military Cooperation Centre of Excellence untersucht praktisch, inwiefern LLMs die Erstellung von ICPs unterstützen können und damit diese Herausforderungen adressiert werden. Das hierzu entwickelte Tool ICP-LLM erstellt die Ebenen der SIRs und EEIs eines ICPs automatisch, basierend auf vom Nutzer formulierten CCIRs und PIRs.

Die in Tabelle 1 dargestellte Übersicht präsentiert einige Möglichkeiten und Herausforderungen, die von den Autoren und bisherigen Teilnehmerinnen und Teilnehmern bei der Konzeption eines LLM-gestützten Intelligence Collection Plans (ICP) antizipiert wurden. Diese Faktoren stellen eine systematisierte Auswahl dar, die für die nachfolgende Auswertung und Validierung eines solchen Systems berücksichtigt werden können.

Kategorie	Thema / Aspekt (Attribut)	Potential (Vorteil)	Neue Herausforderungen (Nachteil)
Prozess & Effizienz	Erstellungsgeschwindigkeit & Agilität	Beschleunigung & Iteration: Signifikant schnellere Erstellung und flexible, iterative Anpassung des Plans an dynamische Lagen.	Initialaufwand & Implementierungszeit: Hoher initialer Konfigurations-, Trainings- und Validierungsaufwand vor der operativen Nutzung.
	Ressourcenallokation & Optimierung	Lücken-/Redundanzanalyse: Automatische Identifikation von Informationslücken (Gaps) und Redundanzen. Optimierte Priorisierung: Datengetriebene Vorschläge zur optimalen Allokation von Sammelressourcen.	Ressourcen-Umschichtung: Bindung von IT- und Fachexperten für die Modellpflege (Governance) statt für die direkte Analyse.
	Nachvollziehbarkeit & Reproduzierbarkeit	Protokollierung & Standardisierung: Möglichkeit zur lückenlosen Protokollierung der Eingaben (Prompts) und Standardisierung des Erstellungsprozesses.	„Black-Box“-Problem & Stochastik: Eingeschränkte Nachvollziehbarkeit der LLM-Entscheidungsfindung, fehlender Determinismus (gleicher Input erzeugt nicht zwingend exakt gleichen Output).
Personal & Kompetenz	Kognitive Leistung & Belastung	Entlastung & Ermüdungsschutz: Reduktion von Routineaufgaben; Analysten fokussieren auf komplexe Analyse statt auf die Planerstellung.	Automatisierungsbias & „De“-Skilling: Gefahr der übermäßigen Abhängigkeit („Over“-Reliance) und der Reduktion von kritischem Denken bei der Planvalidierung.
	Kompetenzprofil & Training	Wissensmanagement & „Up“-Skilling: LLM als Trainings-Tool; Verschiebung hin zu spezialisierten analytisch/technischen Rollen (z.B. Validierung).	Kompetenzlücke & neuer Bedarf: Akuter Bedarf an neuen Fähigkeiten (Prompt Engineering, Model-Governance, KI-Ethik).
	Mensch-Maschine-Interaktion	„Ideaion Partner“[1]: Generierung von Einsichten oder alternativen Ansätzen, die ein homogenes Team (ohne Divergenz) eventuell übersieht.	Interaktionskomplexität: Die Qualität des Outputs ist abhängig von der Qualität des (oft schwer zu formulierenden) Inputs (Prompts).
Technologie & Daten	Datenkontrolle & Vertraulichkeit	Datenhoheit (On-Premise): Bei lokaler Implementierung (statt Cloud) verbesserte Kontrolle über sensible Daten und Anfragen.	Sicherheitsrisiken: Gefahr von Datenlecks (insb. bei Cloud-Nutzung) und Anfälligkeit für Prompt Injections (Manipulation der Ausgabe durch Eingaben).
	Modellzuverlässigkeit & Faktizität	Konsistenz: Gleichbleibende Qualität der Ausgabe, unabhängig von menschlicher Tagesform oder Ermüdung.	Halluzinationen & Faktizität: Risiko inkorrekt, „erfundener“ Planinhalte, die plausibel wirken, aber sachlich falsch sind.
	Aktualität & Kontext	Echtzeit-Anbindung (RAG): Potential zur Anbindung an aktuelle Lagedatenbanken mittels „Retrieval-Augmented Generation“ (RAG)[2].	Statische Wissensbasis: Basismodelle basieren auf statischen Trainingsdaten und kennen nicht die aktuelle Lage (ohne RAG oder Feintuning).

Tabelle 1: - Einige Möglichkeiten und Herausforderungen von ICP-LLM

Im Folgenden werden diese Aspekte detaillierter analysiert, kontextualisiert und durch neue und weiterführende Detailinformationen ergänzt, um ein umfassendes Verständnis der Thematik zu gewährleisten.

In der Literatur wird die Nutzung von LLMs im Intelligence Cycle bislang primär in der Collection- und Processing-Phase diskutiert. Beispiele hierzu sind Anwendungen in der automatischen Auswertung und Strukturierung von Cyber-Threat-Reports¹² sowie die Visualisierung von Datensätzen.¹³ Darüber hinaus werden allerdings auch weiterführende Anwendungen zur Steigerung der allgemeinen Produktivität, der automatischen Programmierung von Software und der autonomen Generierung von Intelligence Reports diskutiert.¹⁴ Das Entwicklungsprojekt ICP-LLM zielt nun darauf ab, zu evaluieren, inwiefern die Produktivität durch den Einsatz von LLMs auch in der Direction-Phase gesteigert werden kann.

Basierend auf Tests mit LLMs, den Erfahrungen aus praktischer Arbeit mit ICPs sowie der Literatur könnte ICP-LLM die zuvor beschriebenen Herausforderungen in vier Punkten adressieren. Einerseits sollte die Automatisierung den Erstellungsprozess eines ICPs erheblich beschleunigen, da die Formulierung von SIRs und EEIs die meiste Zeit in Anspruch nimmt. Dies würde es Analystinnen und Analysten erleichtern, Ergebnisse auch innerhalb enger zeitlicher Restriktionen bereitzustellen und

¹² Vgl. 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> [Zugriff: 29.10.2025].

¹³ Vgl. 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> [Zugriff: 29.10.2025].

¹⁴ Vgl. 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

fundierte Analysen rechtzeitig fertigzustellen, um Wirkung zu entfalten (Speed of Relevance). Ein weiterer Vorteil könnte darin bestehen, dass das LLM nicht ermüdet: Auch bei umfangreichen ICPs, die teilweise hunderte EEIs umfassen, wird somit gewährleistet, dass jede Frage konsequent der vorgegebenen Struktur und den Kriterien des ICP folgt. Hierdurch könnten die Strukturiertheit und Detailliertheit im Vergleich zu menschlich erstellten ICPs verbessert werden.

Zudem könnte die Zeitersparnis durch die automatische Generierung der unteren Ebenen des ICPs ermöglichen, dass das Analysepersonal mehr Ressourcen in die präzise Formulierung und Priorisierung auf der Ebene der CCIRs und PIRs investieren kann. Dieser Faktor könnte dazu beitragen, dass bessere Fragen zu Beginn des ICPs gestellt werden und somit die inhaltliche und Priorisierungshürde adressiert wird. Durch die direkte Integration in Microsoft Excel soll eine niedrige Einstiegshürde gewährleistet werden, und Analytinnen und Analysten wird durch automatische Formatierung eine weitere technische Hürde abgenommen. Hierdurch soll die technische Herausforderung zeitraubender Excel-Formatierungen adressiert werden.

Zusammengefasst könnte ICP-LLM Analytinnen und Analysten durch die automatisierte Erstellung von SIRs und EEIs eine schnellere, konsistentere und benutzerfreundlichere Aufstellung von ICPs ermöglichen und somit die zuvor beschriebenen Herausforderungen adressieren.

7. Technische Umsetzung und Arbeitsablauf ICP-LLM

Im Folgenden wird die technische Umsetzung von ICP-LLM sowie der Arbeitsprozess von Analytinnen und Analysten mit der Software erläutert. Grundsätzlich ist ICP-LLM ein in eine Excel-Makrodatei integriertes Python-Skript, das die vom Nutzer bereitgestellten CCIRs und PIRs in strukturierte Prompts einbettet und über die OpenAI-API an ein LLM sendet. Die als Antwort generierten SIRs und EEIs werden anschließend vom Skript strukturiert, gefiltert und für den Nutzer in Excel aufbereitet dargestellt. Die komplette Bedienung des Programms erfolgt über die Excel-Makrodatei, sodass keine technischen Vorkenntnisse erforderlich sind und keine Vorinstallationen notwendig werden.

Der Arbeitsablauf des Nutzers gestaltet sich wie folgt:

1. Zu Beginn definiert der Nutzer auf Grundlage des Analyseauftrags CCIRs und PIRs. Dadurch wird die inhaltliche Schwerpunktsetzung exakt an den Auftrag angepasst. Zusätzlich beschreibt der Analyst den Kontext und Hintergrund des Analyseauftrags, damit ICP-LLM diesen berücksichtigen kann.
2. Anschließend beginnt ICP-LLM mit der Generierung der SIRs und EEIs. Dazu importiert es zunächst die Excel-Daten via xlwings in die Python-Umgebung und formatiert diese.
3. Dem OpenAI-Modell wird daraufhin das ICP-Konzept erläutert sowie der spezifische Kontext für die Anfrage übergeben. Danach startet die iterative Erstellung: Zunächst wird eine SIR,

anschließend die dazugehörigen EEs generiert. Dabei werden in jedem Schritt alle CCIRs, PIRs sowie die bereits erzeugten SIRs mitgegeben, um klare Abgrenzungen zwischen den Fragestellungen sicherzustellen und Dopplungen zu vermeiden.

4. Im Anschluss filtert und strukturiert das Skript die Ergebnisse.
5. Der fertige ICP wird anschließend über xlwings zurück in Excel übertragen, dort automatisch formatiert und für das Analysepersonal leicht zugänglich sowie weiterbearbeitbar bereitgestellt.

Je nach Umfang des ICP dauert der Prozess zwischen einer und fünf Minuten. Unter der Annahme, dass das empfohlene OpenAI-Modell o4-mini genutzt wird, liegen die Kosten für die API-Nutzung zwischen 0,50 € und 3 € pro ICP – abhängig vom Umfang des erstellten Dokuments.

In der Entwicklung von ICP-LLM musste eine Balance zwischen Zugänglichkeit für die Nutzer, Qualität der verwendeten Modelle und Entwicklungsaufwand gefunden werden. Das Hauptskript von ICP-LLM wurde in Python programmiert, da Python über die xlwings-Bibliothek direkt in eine Excel-Makrodatei integriert werden kann. Zudem kann ICP-LLM durch die im Download mitgelieferte Python-Embedded-Installation ohne Vorinstallationen direkt vom Nutzer verwendet werden. Die Kombination aus Python und einer Excel-Datei mit spezifisch programmierten Makros ermöglicht es daher, die Einstiegshürde zu reduzieren, da kein technisches Vorwissen erwartet wird und das Programm direkt in bestehende Arbeitsprozesse integriert werden kann. Gleichzeitig konnte so der Entwicklungsaufwand im Rahmen eines Evaluierungsprojekts durch das Verwenden bestehender Bibliotheken begrenzt werden.

Für die Datenverarbeitung und Fragengenerierung werden über eine API-Schnittstelle LLMs von OpenAI verwendet. Diese Entscheidung wurde getroffen, um den Zugang zu in Vergleichen führenden Modellen¹⁵ auch auf Rechnern mit begrenzter Rechenleistung zu ermöglichen und so die Verwendungsmöglichkeiten der aktuell fortschrittlichsten Modelle evaluieren zu können. Zudem erlaubt die Anbindung über eine API die schnelle Integration neuer, verbesserter Modelle in das bestehende Skript. Ein Nachteil besteht darin, dass die API-Anbindung eine permanente Internetverbindung voraussetzt und keine vertraulichen Daten verarbeitet werden können. Die Integration lokal gehosteter LLMs ist daher ein notwendiger nächster Entwicklungsschritt, um ICP-LLM in weiteren Anwendungsfeldern nutzen zu können. Bei einer erfolgreichen Validierung des Nutzens von LLMs im Erstellungsprozess eines ICPs sind diese und weitere Entwicklungen, die im Ausblick ausgeführt werden, geplant.

¹⁵ Artificial Analysis: LLM Leaderboard - Comparison of over 100 AI models from OpenAI, Google, DeepSeek & others, online: <https://artificialanalysis.ai/leaderboards/models> [Zugriff: 29.10.2025].

8. Evaluation

ICP-LLM wird im Rahmen des *NATO CIMIC Analysis and Assessment Course*¹⁶ am NATO CIMIC Center of Excellence getestet werden, wenngleich klar ist, dass auf Grund von Gruppengröße und Gruppenzusammensetzung keine statistische Signifikanz erreicht werden kann.

Hierzu sollen zwei Forschungsfragen beantwortet werden:

- 1) In welchem Maße kann der Einsatz des Tools ICP-LLM den Zeitaufwand bei der Erstellung von Intelligence Collection Plans über alle Phasen hinweg erheblich reduzieren, ohne die inhaltliche Qualität der Ergebnisse zu beeinträchtigen?
- 2) Wie wird das Tool ICP-LLM von Intelligence-Analystinnen und Analysten im Ausbildungskontext hinsichtlich Benutzerfreundlichkeit und Ergebnisqualität für den Analyseprozess bewertet?

Folgende Hypothesen wurden mit Blick auf die Forschungsfragen aufgestellt und sollen im Rahmen des *NATO CIMIC Analysis and Assessment Course* überprüft werden:

- 1.1 Durch den Einsatz von ICP-LLM lässt sich der Zeitaufwand für die Erstellung eines vollständigen ICP erheblich reduzieren.
- 2.1 Die Teilnehmenden bewerten ICP-LLM als benutzerfreundlich und gut in bestehende Arbeitsabläufe integrierbar.
- 2.2 Mit ICP-LLM erstellte ICPs weisen eine höhere strukturelle Konsistenz auf (klare Hierarchie, korrekte Verknüpfung zwischen CCIR-, PIR-, SIR- und EEI-Ebenen) als manuell erstellte ICPs.

ICP-LLM soll zu einem späteren Zeitpunkt und in einem weiteren Schritt im Rahmen eines Forschungsprojektes am I2SM zur Organisierten Kriminalität im Rahmen der Kriminalitätsanalyse eingesetzt werden. Mit Hilfe des ICP-LLM sollen umfangreiche Informationen zur italienischen Organisierten Kriminalität erlangt werden, die Aussagen zulassen, die über die bisherigen Erkenntnisse der Sicherheitsbehörden hinausgehen. Kriminalitätsanalyse ist ein zielorientierter Prozess, bei dem Strukturierte Analysetechniken, Methoden und Techniken unter Einhaltung von Standards angewendet werden, um aus Daten und Informationen verwertbare Wissensprodukte zu generieren. Hierbei wird ein Sachverhalt oder eine Fragestellung zunächst in relevante Einzelfragestellungen zerlegt und es werden Hypothesen aufgestellt. Zu diesen werden Daten und Informationen zielgerichtet gesammelt, modelliert, aus unterschiedlichen Blickwinkeln betrachtet und bewertet. Die Ergebnisse der Einzelfragestellungen werden zusammengeführt, im jeweiligen Kontext interpretiert und adressatengerecht kommuniziert. Sie dienen als Basis für sicherheitsrelevantes Handeln. Die Methodik

¹⁶ Für eine Einordnung, wie am NATO CCOE normalerweise die Vermittlung des ICPs vorgenommen wird, siehe Anhang B.

der Kriminalitätsanalyse wird bisher fast ausschließlich von der Polizei verwendet.¹⁷ Die Kriminalitätsanalyse ist aber auch für die private Sicherheit relevant¹⁸ und gewinnt zunehmend an Bedeutung, denn mit der strategischen Kriminalitätsanalyse wird die Kriminalitätsentwicklung beobachtet, eingeordnet und verständlich dargestellt. Damit wird eine Entscheidungsgrundlage geschaffen für die Schwerpunktsetzung bei der Kriminalitätsbekämpfung, die Erarbeitung von Handlungskonzepten, die Ressourcensteuerung und die Ableitung von Maßnahmen. Im zukünftigen Masterstudiengang „Unternehmenssicherheit & Interdisziplinäre Kriminal-wissenschaften“ an der NBS werden Strukturierten Analysetechniken und Kriminalitätsanalyse in einem eigenen Modul vermittelt. Neben der Vermittlung der theoretischen Grundlagen fließen auch die Erkenntnisse aus dem Forschungsprojekt unmittelbar in den Lehrinhalt ein.

9. Ausblick

Die Entwicklung von ICP-LLM zeigt exemplarisch, welches Potenzial der Einsatz von Large Language Models für die Erstellung eines ICPs im Intelligence-Kontext besitzt. Während die Grundprinzipien des Intelligence Cycle und des Intelligence Requirement Managements unverändert bleiben, eröffnen LLM-gestützte Werkzeuge neue Möglichkeiten, zeitintensive Arbeitsschritte zu automatisieren, zeitliche Engpässe zu reduzieren und die methodische Konsistenz von Vorprodukten der Analyse zu sichern.

Die bevorstehende Erprobung des Tools im Rahmen des NATO CIMIC Analysis and Assessment Course und im Bereich der Kriminalitätsanalyse bietet die Gelegenheit, diese theoretischen Annahmen empirisch zu überprüfen. Dabei wird nicht nur untersucht, ob ICP-LLM die Erstellung von Intelligence Collection Plans beschleunigt, sondern auch, wie das Tool von Anwenderinnen und Anwendern im Ausbildungs- und Praxisumfeld wahrgenommen wird.

Über die geplante Evaluierung hinaus eröffnen sich weitere Forschungsfelder: So könnten künftige Arbeiten beispielsweise die Integration lokal gehosteter LLMs zur Verarbeitung sensibler Daten untersuchen. Ebenso wäre die Einbindung von Feedback-Mechanismen denkbar, mit denen das Modell aus den Bewertungen erfahrener Analytinnen und Analysten fortlaufend lernen kann.

10. Feedback und Weiterentwicklung

Die Entwicklung von ICP-LLM versteht sich als offenes, iteratives Projekt, das von Rückmeldungen aus Forschung und Praxis lebt. Hinweise, Verbesserungsvorschläge oder Erfahrungsberichte aus der

¹⁷ Für die Anwendung bei der Polizei, siehe: Deutsche Hochschule der Polizei: Berufsbegleitende Fortbildung Kriminalitätsanalyse, online: https://www.dhpol.de/departments/department_III/FG_III.2/fortbildung-kriminalitaetsanalyse.php [Zugriff: 29.10.2025].

¹⁸ Für eine leicht zugängliche Einordnung, siehe: German Intelligence Podcast, Staffel 1, online: <https://open.spotify.com/show/2mlMdBVLzMAp2f9g93c3k> [Zugriff: 29.10.2025].

Anwendung sind ausdrücklich willkommen und tragen dazu bei, das Tool und seine Einsatzmöglichkeiten weiter zu optimieren.

Kontakt:

niklas.koch@i2sm.nbs.de

Anhang A)

Versuchsaufbau (Durchführungssprache Englisch)

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).

Auszug aus Auswertungsmethodik

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.

Anhang 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 (EIs);

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 EIs; 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 [Zugriff: 26.10.2025].

Artificial Analysis: LLM Leaderboard - Comparison of over 100 AI models from OpenAI, Google, DeepSeek & others, online: <https://artificialanalysis.ai/leaderboards/models> [Zugriff: 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 [Zugriff: 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/2mIMdBVLzMAbp2f9g93c3k> [Zugriff: 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> [Zugriff: 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> [Zugriff: 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> [Zugriff: 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> [Zugriff: 29.10.2025].

Über das Institut

Das Institute for Intelligence and Security Management (I2SM) ist ein interdisziplinäres Institut der Northern Business School (NBS) in Hamburg. Am Institut sind derzeit sechs Professor:innen, zwölf Research Fellows und projektbezogen mehrere studentische Hilfskräfte tätig, über welche die Disziplinen Strafrecht/Strafprozessrecht, Wirtschaftsstrafrecht/Wirtschaftskriminalität, Kriminologie, Kriminalistik, IT-Sicherheit, Sicherheitsmanagement, Sicherheitstechnik/Robotik, Wirtschaftspsychologie, Intelligence und Analyse, Krisenmanagement, Bedrohungsmanagement, Resilienzmanagement, Risikomanagement, Strategic Foresight, und Wirtschaftsschutz mit Expertise abgedeckt werden können. Neben der Praxisnähe in der Lehre ist auch die Forschung ein wichtiges Standbein der NBS. Das I2SM ist eines von insgesamt sechs Forschungsinstituten an der NBS. Bereits heute sind zahlreiche Nachwuchswissenschaftler:innen als Research Fellows oder als studentische Hilfskräfte in verschiedenen Projekten im I2SM tätig. Gerade Studierende, aktuell des Bachelor-Studiengangs Sicherheitsmanagement und zukünftig auch des entsprechenden Masterstudiengangs Interdisziplinäre Kriminalwissenschaften und Unternehmenssicherheit, haben so die Möglichkeit, bereits zu einem frühen Zeitpunkt ihrer akademischen Karriere Einblicke in die Forschungstätigkeit zu erlangen und einzelne Teilprojekte, teilweise in Form von Haus-, Praktikums- und Abschlussarbeiten, selbstständig zu erarbeiten. Dazu haben sie auch die Möglichkeit, interdisziplinär mit den anderen Instituten an der NBS und in Kooperation mit Behörden und Unternehmen zusammenzuarbeiten und neue Ideen zu entwickeln. Da zudem die Pflichtpraktika sehr praxisorientiert ausgerichtet sind, erfolgt auch stets ein aktueller Input der Studierenden in das I2SM hinein.

Über die Autoren

Ralf Baur (OF-4, DEU Luftwaffe) ist seit Februar 2020 am CIMIC Centre of Excellence tätig. Zuvor war er als Verbindungsoffizier und Austauschoffizier beim Dutch 1 Civil-Military Interaction Command in Apeldoorn, Niederlande, tätig.

Vor seiner ersten Verwendung im CIMIC Centre of Excellence von 2010 bis 2016 war er als Ausbilder und Kursentwickler bei der Vorgängerorganisation des CCOE, dem Multinational CIMIC Command in Nienburg, Deutschland, tätig. Er blickt auf mehr als 20 Jahre Erfahrung im Bereich der zivil-militärischen Zusammenarbeit zurück. Oberstleutnant Ralf Bauers Einsatzbilanz umfasst Missionen in Bosnien-Herzegowina, im Kosovo und mehrfach in Afghanistan, wo er verschiedene CIMIC-Positionen innerhalb der Provincial Reconstruction Teams (PRT), des Regionalkommandos Nord (RC N) und des ISAF-Hauptquartiers innehatte.

Für seinen letzten Einsatz in Afghanistan wurde er gebeten, sich einem von den USA geführten Fusionszentrum anzuschließen, wo er für die Zusammenführung von CIMIC-Daten und -Informationen mit Intelligence verantwortlich war, um dem Kommandeur eine genauere Einschätzung des Einsatzgebiets zu ermöglichen.

Unter Einsatz seines umfangreichen Netzwerks aus militärischen und zivilen Partnern und Experten entwickelte er das CIMIC Analysis and Assessment Concept und die dazugehörige Schulungslösung, den NATO- NATO CIMIC Analysis and Assessment Course. Kürzlich kreierte er das zivil-militärische Kooperations-Wargame ANALYSIA, das seine Teilnehmerinnen und Teilnehmer dabei unterstützt, entlang der Linien der Integration ziviler Faktoren (CFI) als einer der beiden interagierenden Kernaktivitäten der zivil-militärischen Zusammenarbeit zu denken.

Ole Donner ist Gründer von Strukturierte Analyse Deutschland. In dieser Funktion ist er als Trainer und Berater für staatliche Institutionen wie die Kriminalpolizei, zwischenstaatliche Organisationen wie die NATO sowie nationale und internationale Wirtschaftsunternehmen tätig, um deren jeweiligen Fähigkeiten in den Bereichen Intelligence und Analyse zu stärken. Ole Donner blickt auf eine 13-jährige Dienstzeit bei der Bundeswehr zurück, in der er umfangreiche Erfahrungen als All-Source-Analyst, Intelligence Manager und Dozent sammeln konnte. Während seiner Dienstzeit gestaltete er die Analyseausbildung der Bundeswehr neu und konzentrierte sich dabei stark auf die kompetenzorientierte Vermittlung von Strukturierten Analysetechniken (SATs). Er war auch an der Entwicklung der Führungskräfteausbildung im Bereich "Intelligence Leadership" an der Führungsakademie der Bundeswehr beteiligt.

Ole Donner ist Mitautor der im Springer-Verlag erschienenen Bücher „Clear Thinking“ und „Klarheit im Denken“. Darüber hinaus ist er Initiator der German Intelligence Community Conference (GICC), Research Fellow des Institute for Intelligence and Security Management (I2SM) an der Northern Business School Hamburg und Regionaldirektor Europa der International Association of Intelligence Education (IAFIE).

Ole Donner hat einen Bachelor-Abschluss in Politikwissenschaft und einen Master-Abschluss in Internationalen Beziehungen an der Universität der Bundeswehr Hamburg erworben und wurde als Jahrgangsbester mit dem Böttcher-Preis ausgezeichnet.

Niklas Koch hat Doppelabschlüsse in Volkswirtschaftslehre und Internationalen Beziehungen von der Universität St. Gallen und studiert derzeit Volkswirtschaftslehre im Master an der Universität Mannheim. Sein akademischer Schwerpunkt liegt an der Schnittstelle von Sicherheits-, Energie- und Wirtschaftspolitik, mit besonderem Fokus auf Nord- und Osteuropa. Im Rahmen seiner Forschung befasste er sich insbesondere mit den wirtschaftlichen und strukturellen Auswirkungen der Zerstörung der Nord-Stream-Pipelines auf den europäischen Gasmarkt.

Praktische Einblicke in internationale Sicherheits- und Wirtschaftsstrukturen sammelte er während seiner Tätigkeiten bei der *Deutsch-Baltischen Handelskammer* in Litauen sowie beim *NATO Civil-Military Cooperation Centre of Excellence* in den Niederlanden. In Litauen konnte er im sicherheitspolitischen Brennpunkt des Baltikums unmittelbare Erfahrungen sammeln und arbeitete an Analysen zum regionalen Rüstungsökosystem. Das Praktikum beim NATO-Zentrum vertiefte seine Expertise in der zivil-militärischen Analyse und im Einsatz strukturierter Analysetechniken zur Bewertung komplexer sicherheitspolitischer Szenarien.

Beruflich ist Niklas Koch seit mehreren Jahren freiberuflich als Entwickler, Berater und Serious-Gaming-Designer im sicherheits- und außenpolitischen Bereich tätig. Er konzipiert und leitet eigenständig simulationsbasierte Projekte zur strategischen Entscheidungsfindung und Resilienzförderung, unter anderem für das *First German Netherlands Corps*, die *Universität St. Gallen* und verschiedene Versicherungsunternehmen. Zudem war er als Entwickler am Forschungsprojekt *ICP-LLM* beteiligt, das sich mit der Integration großer Sprachmodelle in analytische und strategische Entscheidungsprozesse befasst.

André Schulz ist Professor für Kriminalwissenschaften und Leiter des Institute for Intelligence and Security Management (I2SM) an der NBS. Er verfügt über eine kaufmännische sowie über eine Schutz- und kriminalpolizeiliche Ausbildung und studierte Verwaltungswissenschaft (Polizei), Wirtschaftsrecht, Betriebswirtschaftslehre, Kriminologie und Polizeiwissenschaft. Zudem absolvierte er ein Promotionsstudium

der Rechtswissenschaften an der Juristischen Fakultät der Ruhr-Universität in Bochum. Schulz verfügt über 30 Jahre Erfahrung im kriminalpolizeilichen Ermittlungsbereich und hat langjährige Expertise in der Politikberatung auf Landes- und Bundesebene, in der Unternehmens- und Verbandsführung, in der Personalvertretung sowie durch die Tätigkeit bei einer der „Big Four“-Wirtschaftsprüfungsgesellschaften. Er besitzt Zertifizierungen als Compliance Manager, Projektmanager und inter-/transkultureller Trainer.

Richard Weiss arbeitete als Reverse Engineer im FLARE Team von Mandiant (now Part of Google Cloud) und widmet seine Motivation im Berufsalltag und seiner Freizeit der Integration von Intelligence-Methodiken und anderen wissenschaftlichen Disziplinen, wie Mathematik, Data Sciences und Data Mining, in den Cyber Threat Intelligence (CTI) Kontext. Dabei spielt auch die Vereinheitlichung von CTI-Arbeitsweisen unterschiedlicher Aufgabenbereiche eine entscheidende Rolle. Zu diesem Zweck ist er zum zweiten Mal in Folge als Sprecher bei der CyCon – veranstaltet vom CCDCOE – eingeladen und stellte einen kleinen Ausschnitt seiner Arbeit auch bei weiteren Konferenzen vor. Richard Weiss pflegt dabei eine enge Verbindung zum öffentlichen Sektor. In seiner Freizeit betreute er in der Vergangenheit außerdem das europäische Cybersecurity Challenge Team der ENISA in Vorbereitung auf den ICSC und Studenten des Neuland e.V. an der Technischen Hochschule in Ingolstadt.