Deep Research – Intl Research Security  
Phase 0–8 Prompt Stack (ChatGPT + Claude Code)

Best-practice prompt templates for a phased, repeatable research workflow across countries.

# Phase X — Universal Header & Run Controls

## Variables

COUNTRY = {{country\_name}}  
TIMEFRAME = 2015–present  
HORIZONS = {2y, 5y, 10y}  
LANG = EN # set to local language if needed  
REGIONAL\_COMPARATORS = {{peer\_set}} # e.g., Nordics; Balkans; Benelux

## Toggles (true/false) + #explainers

INCLUDE\_EXPORT\_CONTROLS = true  
# true → analyze EU Dual‑Use/EAR/ITAR interactions & screening gaps; false → omit.  
  
INCLUDE\_US\_NATSEC\_FRAMEWORK = true  
# true → apply 8‑dimension U.S. national‑security lens with ratings; false → omit.  
  
INCLUDE\_EWI\_CHECKLIST = true  
# true → overlay Early Warning Indicators & use in Phase‑8; false → omit.  
  
INCLUDE\_DATA\_PULLS = true  
# true → run CORDIS/OpenAIRE/Crossref/Patents/News steps in Phases 2–5; false → narrative only.  
  
INCLUDE\_COLLAB\_MAPPING = true  
# true → build co‑author/co‑project graphs in Phase‑3; false → skip.  
  
CITE\_SOURCES = true  
# true → inline citations & source log; false → provenance notes only.

## Evidence Priority Order

1) Primary government/regulatory docs; 2) EU/official databases (CORDIS, OpenAIRE, eCORDA); 3) Reputable think‑tanks/academia; 4) Major media; 5) Organization websites/press; 6) Social/open web (lowest confidence).

## Style & Output Rules (both models)

• Precision over breadth; avoid boilerplate; date‑stamp key facts.  
• Explicitly mark assumptions vs. evidence.  
• Prefer structured artifacts: tables, matrices, JSON/CSV schemas.  
• If data conflicts, log both and note a likely resolution path.  
• Do not include PII or non‑public sensitive details.

## Quick Run Instructions

1) Set variables and toggles.  
2) Run Phase 0 → Phase 8 sequentially; reuse outputs as inputs.  
3) For Claude Code runs, request both CSV/JSON where specified; save GraphML.  
4) Compile a country pack: Executive Summary + Phases + Annexes.

# Phase 0 — Scoping & Framing

## ChatGPT — Prompt

You are a senior research‑security analyst scoping COUNTRY.  
Deliver a 3‑page max scoping brief that:  
- Positions COUNTRY in advanced/emerging tech & dual‑use research.  
- Lists 5–8 priority tech areas (AI, quantum, semiconductors, biotech, space, advanced materials, smart‑city/IoT, robotics).  
- Summarizes R&D governance (ministries, funders, national strategies) with dates.  
- Maps international posture (EU, U.S., PRC, regional blocs) and key agreements/MoUs.  
- Flags strategic strengths & vulnerabilities and likely foreign‑interest vectors.  
- If INCLUDE\_US\_NATSEC\_FRAMEWORK=true, add a 1‑page annex rating the 8 categories (Critical/High/Moderate/Low) with 1–2 justifications each.  
  
Outputs: Executive bullets; one situational table/map; optional Annex A (8‑dimension U.S. framework).

## Claude Code — Prompt

Produce a single JSON object for the Phase‑0 dossier for COUNTRY with keys:  
- sectors[]  
- gov\_actors[]  
- funders[]  
- intl\_links[]  
- agreements[]  
- strengths[]  
- vulnerabilities[]  
- open\_questions[]  
- (optional) us\_natsec\_ratings[{dimension, rating, rationale}] if INCLUDE\_US\_NATSEC\_FRAMEWORK=true  
  
Use YYYY‑MM date strings where relevant. Ensure valid JSON (no comments).

# Phase 1 — Research Ecosystem Baseline

## ChatGPT — Prompt

Map COUNTRY’s research ecosystem. Include:  
- Top institutions (universities, RTOs, academies, labs) with sector focus and notable centers.  
- Public funders (ministries, councils) and major programs/calls since 2015 (with amounts if public).  
- Private sector: leading firms/startups in dual‑use spaces; public‑private labs.  
- International collaborations (EU joint centers, PPPs, MoUs).  
- Openness to foreign engagement and any screening mechanisms.  
Provide: a master table; a short narrative per sector; a list of data gaps.

## Claude Code — Prompt

Create a CSV for institutions in COUNTRY with columns:  
name, type{univ,gov,private,RTO}, sectors(list), key\_centers, intl\_collab{Y/N}, flagged\_red\_flags(list), url  
  
Return the CSV content as a code block and a JSON array reflecting the same rows.

# Phase 2 — Targeted Data Pulls (CORDIS, OpenAIRE, Crossref, Patents, News)

## ChatGPT — Prompt

Using INCLUDE\_DATA\_PULLS, compile structured tables for COUNTRY:  
- CORDIS: project id, title, dates, amount, country\_partners[], keywords[], lead/beneficiaries.  
- OpenAIRE/Crossref: top outputs (since 2015), co‑author countries, venues, dual\_use\_keywords hits.  
- Patents (WIPO/EPO): assignees, IPC/CPC codes, co‑inventors’ countries.  
- News (3–5y): relevant research‑security stories; include headline/date/outlet/link.  
Prioritize dual‑use relevance; mark any PRC/RF joint items.

## Claude Code — Prompt

Generate API‑ready query specs for each source for COUNTRY. For each, output JSON:  
{source, endpoints[], query\_params{date\_range, keywords[], country\_filters[], fields[]}, pagination\_notes, rate\_limit\_notes}  
Add a validation\_plan (dedupe, normalize names, entity‑resolution hints).

# Phase 3 — Researcher & Collaboration Mapping

## ChatGPT — Prompt

From Phase‑2 data, identify:  
- Top 20 researchers/institutions by output/impact in dual‑use sectors.  
- Repeat collaboration patterns with PRC/RF/other risk jurisdictions.  
- Academia–industry–government linkages.  
Deliver: a short narrative; a table of top actors; network insights (broker hubs, clusters); and a list of watchlist ties (if any) with cautionary language.

## Claude Code — Prompt

Produce network artifacts from entity lists:  
- Node list: id, label, type{person,institution,country}, sector\_tags[]  
- Edge list: src, dst, relation{coauthor,coproject,coinventor,grant}, weight  
- Compute centrality (degree, betweenness, eigenvector) and return as CSV + JSON.  
- Export GraphML (as a string) for Gephi.

# Phase 4 — Risk & Vulnerability Analysis

## ChatGPT — Prompt

Assess vulnerabilities across sectors in COUNTRY:  
- IP leakage, espionage, talent pipelines, dependency on foreign funding/equipment, cyber posture, research‑integrity risks.  
- Build a RAG Risk Matrix by sector with rationales and mitigations (policy, process, technical, training).  
- If INCLUDE\_EXPORT\_CONTROLS, add export‑control exposure notes and screening gaps.  
- If INCLUDE\_EWI\_CHECKLIST, map 5–10 top EWIs to sectors.

## Claude Code — Prompt

Return a machine‑readable risk table:  
sector, risk\_category, risk\_score(1–5), color{R/A/G}, evidence\_refs[], mitigation\_options[], owner{sponsor/inst}, time\_to\_implement{short/med/long}  
Include a scoring\_method block documenting the rubric.

# Phase 5 — Funding Flow & Collaboration Analysis

## ChatGPT — Prompt

Trace funding and collaboration for COUNTRY:  
- External funders (gov, foundations, corporates), joint centers, industry consortia.  
- Identify leverage points for compliance (due diligence hooks, reporting nodes).  
- Note red‑flag patterns (front orgs, opaque philanthropies, equipment grants with unusual terms).  
Provide: a flow diagram description, funder‑recipient tables, and 5–8 case vignettes.

## Claude Code — Prompt

Return two artifacts:  
1) funding\_edges.csv: source\_country, source\_entity, amount, currency, year, recipient\_entity, sector, notes  
2) collab\_edges.csv: inst\_A, inst\_B, relation, start\_year, end\_year, sector, high\_risk\_flag{Y/N}  
Include a compliance\_hooks[] list (data fields suitable for automated screening).

# Phase 6 — Capacity‑Building Program Design

## ChatGPT — Prompt

Design 1–3 targeted interventions (not awareness 101) for COUNTRY. For each:  
- Format (tabletop, workshop, red‑team, procurement due‑diligence lab, secure‑by‑design sprint).  
- Audience (PI/Lab managers, TTOs, compliance, funders, policymakers, sysadmins).  
- Objectives, inputs, outputs, metrics (pre/post checks, adoption indicators).  
- Timeline (single event or 12–18‑month limited series) with partners.  
Return a 1‑page blueprint per intervention.

## Claude Code — Prompt

Return JSON blueprints:  
{title, type, audience[], agenda\_blocks[{min, activity, artifact}], required\_inputs[], deliverables[], success\_metrics[], risks[], mitigation[]}  
Add an .ics schedule generator spec (dates placeholder) and a materials checklist.

# Phase 7 — Adversarial / Assumption Testing

## ChatGPT — Prompt

Red‑team your own conclusions for COUNTRY:  
- For each high‑confidence claim, list falsifiers, counter‑narratives, and unknowns.  
- Answer: “If this change is so valuable, why hasn’t it happened yet?” (constraints, incentives, politics, capacity).  
- Produce a Top‑10 Fragile Assumptions list with evidence rating.

## Claude Code — Prompt

Create a table:  
claim, evidence\_for[], evidence\_against[], testable\_predictions[], falsification\_steps[], fragility(1–5)  
Include a replication\_plan (datasets, scripts, recompute steps) for independent validation.

# Phase 8 — Foresight & Early Warning

## ChatGPT — Prompt

Forecast for COUNTRY at 2y/5y/10y:  
- Tech trajectories (dual‑use breakthroughs, adoption constraints).  
- Adversarial interest vectors (target techs, institutions, mechanisms).  
- Policy/market shifts impacting risk posture.  
- If INCLUDE\_EWI\_CHECKLIST, define EWIs (lead signals, confirmatory signals, likely false positives) and tie to monitoring cadences.  
Deliver: three short scenarios + a watchboard (what to track, where, how often).

## Claude Code — Prompt

Return two artifacts:  
1) scenarios.json with keys {horizon, drivers[], uncertainties[], scenario, implications[], EWI\_links[]}  
2) watchboard.csv: indicator, signal\_source, collection\_method, cadence, trigger\_threshold, owner

# Optional Annex Hooks

• Annex A — U.S. NatSec 8‑Dimension Definitions & Rating Notes (attach latest version).

• Annex B — Early Warning Indicator Category Checklist (attach universal checklist).

• Annex C — Data Source Query Library (CORDIS/OpenAIRE/Crossref/Patents/news).