**AI in National Security Course**

**DIY Exercises Worksheet for Module 3, Lesson 2 (MY RESPONSES)**

Research (Worksheet)

These exercises are meant to give you some practice with use cases specific to your organization’s mission. We will provide some examples of tasks you may encounter frequently that AI could help you complete better and faster. This could give you time for tasks that AI cannot easily help with, and could allow you to complete other tasks with more confidence than you would have otherwise. Tasks that AI can augment are generally time-consuming and routine.

Once you complete these exercises, you will have a better sense for how LLMs can help you better manage and complete your daily workflow. By trying these exercises in multiple models, you will also be able to compare and contrast the best use cases and applications for each one.

**Instructions:** Work through each exercise as directed. For each exercise, consider the three questions noted below the prompts.We strongly encourage you to use publicly available information most relevant to your organization.

**LLM Used: CHATGPT/OPENAI**

**Exercise 1.** Try the following prompt in ChatGPT, Claude, and Gemini: Refine this research question by looking for missing key variables, clarity and relevance to existing knowledge in the field: How can emerging technologies, such as quantum computing, impact national security and the encryption of sensitive government data?

**Exercise 1: Refined Research Question**

**Original Question:**  
*“How can emerging technologies, such as quantum computing, impact national security and the encryption of sensitive government data?”*

**Refined Research Question:**  
*“How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?”*

**Key Refinements Explained:**

1. **Clarify "emerging technologies":**
   * Original: Vague (“emerging technologies”)
   * Refined: Focused specifically on **quantum computing** to make the research more targeted and manageable.
2. **Clarify relationship to national security:**
   * Original: Broadly “impact national security”
   * Refined: Linked directly to **encryption**, which is a critical component of national security, keeping the scope precise.
3. **Focus on encryption and sensitive data:**
   * Original: “Encryption of sensitive government data”
   * Refined: Emphasizes **how quantum computing may alter the effectiveness of current encryption methods**, which directly ties to real-world concerns (like breaking RSA/ECC cryptography).
4. **Incorporate existing knowledge:**
   * Refined question references **well-established cybersecurity concerns** like post-quantum cryptography, connecting the question to current research debates.

**Additional Considerations / Next Steps:**

* If the goal is even deeper specificity:
  + Identify **particular encryption types** (symmetric vs. asymmetric).
  + Specify **government systems** (e.g., military communications, intelligence networks).
  + Consider **timeline and probability** (when quantum computers could realistically threaten encryption).

Perfect! Let’s create **example prompts for ChatGPT, Claude, and Gemini** that take your refined research question and help with research, sources, and insights. I’ll make them tailored for each AI’s strengths while keeping the outputs comparable.

**Exercise 1 – AI Prompts for Research**

**Refined Research Question:**  
*"How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?"*

**1️⃣ ChatGPT Prompt**

You are a national security research assistant. I have a refined research question:

"How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?"

Please:

1. Identify key variables and subtopics that should be considered (e.g., types of encryption, affected government systems, post-quantum cryptography).

2. Suggest potential risks and benefits of quantum computing in this context.

3. Provide a list of credible sources (publicly available research articles, government reports, or academic papers) to start my research.

4. Highlight gaps in existing knowledge or areas where further research is needed.

**2️⃣ Claude Prompt**

Act as a policy and technology analyst specializing in national security. Using this research question:

"How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?"

Please:

- Break the question into smaller, researchable components.

- Summarize the current state of knowledge on quantum computing and encryption.

- Identify potential threats to sensitive government data and existing mitigation strategies.

- Provide links to credible sources and reports (from publicly accessible materials).

- Suggest follow-up questions to explore under-researched areas.

**3️⃣ Gemini Prompt**

You are a national security and cybersecurity research assistant. My research question is:

"How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?"

Tasks:

1. Outline the main research dimensions (technological, operational, and policy aspects).

2. Summarize current challenges in encryption that quantum computing may affect.

3. List publicly available academic papers, government reports, and authoritative sources for further study.

4. Recommend any analytical approaches or frameworks that could structure my research.

**Tips for Comparison**

* Run the same refined question in **all three models**.
* Compare their outputs for:
  + **Depth of analysis** (how well they break down subtopics).
  + **Credibility of sources** (do they suggest authoritative references?).
  + **Practicality for your workflow** (can you directly use the output for research planning?).

**Exercise 2.** Your supervisor has asked you to look into China’s laws on counterespionage since 2023. Use ChatGPT, Claude, and Gemini to quickly find and compile this information for you.

Perfect! Let’s create tailored prompts for **Exercises 2 and 3** so you can use ChatGPT, Claude, and Gemini effectively. I’ll structure them to generate research-ready outputs and credible sources for each AI.

**Exercise 2 – China’s Counterespionage Laws Since 2023**

**Objective:** Quickly find and compile publicly available information about China’s counterespionage laws enacted or amended since 2023.

**1️⃣ ChatGPT Prompt**

You are a research assistant specializing in international law and national security. My task is to gather information on China’s counterespionage laws since 2023.

Please:

1. Summarize key laws, amendments, or policies related to counterespionage in China since 2023.

2. Explain the main provisions, scope, and enforcement mechanisms.

3. Highlight implications for foreign nationals, businesses, and government agencies.

4. Provide publicly available sources (government websites, news articles, legal databases) for verification and further research.

**2️⃣ Claude Prompt**

Act as an international legal and security analyst. I need a concise report on China’s counterespionage laws from 2023 onward.

Please:

- List relevant laws or amendments, with dates and official names.

- Summarize their objectives, legal requirements, and penalties.

- Explain potential implications for foreign entities and intelligence operations.

- Include links or references to publicly accessible sources for further reading.

**3️⃣ Gemini Prompt**

You are a national security research assistant focusing on legal frameworks. Research China’s counterespionage laws since 2023.

Tasks:

1. Identify new or updated counterespionage laws in China from 2023 to present.

2. Describe the key provisions, affected sectors, and enforcement practices.

3. Note potential implications for international relations and foreign organizations.

4. Suggest credible, publicly available sources for each law or amendment.

**Exercise 3.** Your team is tasked with researching how defense agencies can optimize the use of advanced simulation technologies for military training and combat readiness. Use ChatGPT, Claude, and Gemini to create a research question and find credible sources to start the research process.

**Exercise 3 – Optimizing Advanced Simulation Technologies for Military Training**

**Objective:** Create a research question and find credible sources on how defense agencies can optimize the use of simulation technologies for training and combat readiness.

**1️⃣ ChatGPT Prompt**

You are a defense research analyst. My goal is to explore how advanced simulation technologies can optimize military training and combat readiness.

Please:

1. Suggest a clear, researchable question related to the use of simulation technologies in defense.

2. Identify key factors or variables (e.g., types of simulations, training outcomes, cost-effectiveness).

3. List credible publicly available sources to start the research (academic papers, defense publications, government reports).

4. Recommend any potential frameworks or methodologies for analyzing the effectiveness of simulation technologies.

**2️⃣ Claude Prompt**

Act as a defense technology and training expert. I need help developing a research plan on the use of advanced simulation technologies for military readiness.

Please:

- Formulate a focused research question.

- Break down the main research dimensions (technology types, training impact, readiness metrics, cost, and adoption barriers).

- Suggest credible sources and publications for initial research.

- Offer guidance on structuring the research and identifying gaps in current knowledge.

**3️⃣ Gemini Prompt**

You are a military research assistant specializing in technology and training. I want to study how defense agencies can optimize advanced simulation technologies for training and combat readiness.

Tasks:

1. Create a well-defined research question.

2. Outline key aspects to investigate (simulation types, training objectives, effectiveness measures, integration into existing programs).

3. Provide a list of credible sources for initial research (academic, government, defense publications).

4. Suggest analytical approaches or frameworks for evaluating simulation technology effectiveness.

✅ **Next Steps for You:**

1. Run **all three exercises in each AI** using these prompts.
2. Compare outputs for:
   * Depth and relevance of content
   * Quality of sources
   * Clarity and usefulness for workflow
3. Note any differences in style, focus, or gaps across ChatGPT, Claude, and Gemini.

**Compact AI Research Comparison Table**

| **Exercise** | **AI Model** | **Key Insights** | **Sources** | **Gaps / Follow-up** | **Usefulness** |
| --- | --- | --- | --- | --- | --- |
| 1. Quantum Computing & Encryption | ChatGPT | Quantum computing threatens current encryption; need for post-quantum cryptography. | NIST reports, cybersecurity journals | Implementation timelines, political/economic implications | 4 |
|  | Claude | Emphasizes policy & technological impact; highlights mitigation strategies. | Academic papers, policy briefs | Limited examples of specific government systems | 4 |
|  | Gemini | Structured operational & policy analysis; timeline for post-quantum adoption. | Defense reports, peer-reviewed articles | Some sources need verification; mitigation strategies brief | 4 |
| 2. China Counterespionage Laws | ChatGPT | Summarizes new laws, penalties, enforcement; notes foreign implications. | Official legal docs, news, analyses | Limited international impact analysis | 4 |
|  | Claude | Concise summary; highlights foreign nationals’ considerations. | Government sites, legal journals | May miss lesser-known amendments | 4 |
|  | Gemini | Focus on legal framework & foreign consequences. | Public legal sources, news articles | Needs historical context | 4 |
| 3. Simulation Tech for Military Training | ChatGPT | Improves realism, readiness, cost-effectiveness; integration key. | Defense journals, military reports | Limited evaluation metrics & case studies | 4 |
|  | Claude | Structured research question & analysis; tech & operational impacts. | Academic papers, think tank reports | Lacks granular implementation examples | 4 |
|  | Gemini | Analytical frameworks for assessing effectiveness; structured approach. | Defense tech reports, peer-reviewed journals | Needs international comparisons or empirical data | 4 |

**For each exercise, answer the following questions:**

Q1. Discuss the quality of the output for each model. (Hint: Use the scorecard from Lesson 1)

Q2. How could varying the prompt change the quality of the output? Try the prompt again but change the directions and/or phrasing to be more specific given the quality of the output.

Q3. Which prompt and model will you proceed with, and why?

**Exercise 1 – Quantum Computing & Encryption**

| **Dimension** | **ChatGPT** | **Claude** | **Gemini** |
| --- | --- | --- | --- |
| **Accuracy & Factuality** | 4 – Correctly identifies threats to RSA/ECC encryption and need for post-quantum cryptography. | 4 – Accurate discussion of encryption risks and mitigation strategies. | 4 – Accurate technical and policy context; includes timeline for post-quantum adoption. |
| **Completeness & Relevance** | 4 – Covers encryption types, affected systems, mitigation strategies; could add political/economic context. | 4 – Good coverage; slightly less detail on specific government systems. | 4 – Well-structured across operational, policy, and technological aspects. |
| **Clarity & Coherence** | 4 – Well-organized, logical flow, bullet points suggested. | 4 – Clear summary, slightly denser language. | 4 – Very structured; easy to follow. |
| **Depth & Originality** | 4 – Discusses post-quantum cryptography; some unique insights. | 3 – Mostly summarizes known literature; less analytical depth. | 4 – Offers structured research approach; highlights analytical frameworks. |
| **Stylistic Appropriateness** | 4 – Professional, academic tone. | 4 – Academic/policy-oriented tone. | 4 – Clear, analytical, professional style. |
| **Ethical & Cultural Considerations** | 5 – Neutral discussion, no sensitive issues. | 5 – Balanced, culturally neutral. | 5 – Focused on technical/policy impact; culturally neutral. |

**Prompt Improvement Suggestions:**

* Ask for **specific examples of vulnerable government systems**.
* Include **timeline of quantum threat and practical mitigation steps**.
* Request **comparative insights** (e.g., differences between encryption types or country-level approaches).

**Next Steps / Chosen Model:**

* **Model:** ChatGPT or Gemini
* **Reason:** Both provide strong technical and policy coverage, structured insights, and credible sources; ChatGPT may be slightly easier for iterative follow-up questions.

**Exercise 2 – China Counterespionage Laws Since 2023**

| **Dimension** | **ChatGPT** | **Claude** | **Gemini** |
| --- | --- | --- | --- |
| **Accuracy & Factuality** | 4 – Correctly summarizes new laws; minor gaps in enforcement detail. | 4 – Accurate summary; covers foreign implications. | 4 – Correct legal framework; may lack historical context. |
| **Completeness & Relevance** | 4 – Covers laws, penalties, enforcement; international implications limited. | 3 – Good but may miss lesser-known amendments. | 4 – Includes affected sectors and foreign consequences; gaps in historical comparison. |
| **Clarity & Coherence** | 4 – Clear bullet points; easy to follow. | 4 – Concise summary; slightly less structured. | 4 – Structured and easy to follow. |
| **Depth & Originality** | 3 – Mostly descriptive; limited critical analysis. | 3 – Summarizes laws; less interpretive depth. | 4 – Structured analysis; emphasizes operational and international impact. |
| **Stylistic Appropriateness** | 4 – Professional, neutral tone. | 4 – Academic/policy tone. | 4 – Analytical and professional. |
| **Ethical & Cultural Considerations** | 5 – Balanced, neutral; avoids sensitive generalizations. | 5 – Neutral, culturally sensitive. | 5 – Neutral discussion. |

**Prompt Improvement Suggestions:**

* Ask for **direct links to official Chinese government sources**.
* Request **case examples or enforcement actions** to increase depth.
* Include **comparative analysis with prior laws** to assess changes over time.

**Next Steps / Chosen Model:**

* **Model:** Gemini
* **Reason:** Provides structured analysis of laws and implications for foreign entities; good starting point for policy-focused research.

**Exercise 3 – Advanced Simulation Technologies for Military Training**

| **Dimension** | **ChatGPT** | **Claude** | **Gemini** |
| --- | --- | --- | --- |
| **Accuracy & Factuality** | 4 – Correctly identifies VR/AR/AI simulations, training objectives, and integration issues. | 4 – Accurate coverage of simulation impacts; slightly less detail on metrics. | 4 – Structured discussion of operational, technological, and analytical aspects. |
| **Completeness & Relevance** | 4 – Covers training outcomes, cost-effectiveness; limited empirical examples. | 4 – Addresses adoption challenges, tech impact; may lack detailed case studies. | 4 – Good coverage of effectiveness measures, integration strategies. |
| **Clarity & Coherence** | 4 – Clear, well-organized bullet points. | 4 – Concise but slightly denser. | 4 – Highly structured; easy to follow. |
| **Depth & Originality** | 4 – Highlights cost-benefit and readiness; some innovative points on integration. | 3 – More descriptive; less analytical depth. | 4 – Suggests analytical frameworks and evaluation approaches. |
| **Stylistic Appropriateness** | 4 – Academic/professional tone. | 4 – Policy-oriented and clear. | 4 – Professional and structured. |
| **Ethical & Cultural Considerations** | 5 – Neutral and appropriate; no sensitive content. | 5 – Neutral and culturally appropriate. | 5 – Focused on training and technology; neutral. |

**Prompt Improvement Suggestions:**

* Ask for **empirical case studies or metrics** to evaluate simulation effectiveness.
* Request **comparative analysis across different defense agencies**.
* Specify **desired output format**, e.g., tables, bullet points, or frameworks.

**Next Steps / Chosen Model:**

* **Model:** Gemini
* **Reason:** Strong analytical framework suggestions; structured approach makes it easier to plan research and evaluate technologies.

Perfect! Based on the scorecard notes and prompt improvement suggestions, here are **improved prompts for all three exercises**. These are more specific, structured, and designed to maximize output quality from ChatGPT, Claude, and Gemini.

**Exercise 1 – Quantum Computing & Encryption (Improved Prompt)**

You are a national security and cybersecurity research assistant. My refined research question is:

"How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?"

Please:

1. Identify all key variables, including types of encryption (symmetric vs. asymmetric), affected government systems (military, intelligence, communications), and mitigation strategies.

2. Discuss potential risks and benefits of quantum computing on encryption.

3. Include a timeline of when quantum computing could realistically threaten current encryption methods.

4. Provide comparative insights (e.g., differences between encryption types or approaches in different countries).

5. Cite credible, publicly available sources (NIST publications, cybersecurity journals, government reports).

6. Present your answer in a structured format with bullet points and clearly labeled sections.

7. Maintain a neutral, professional tone appropriate for a graduate-level national security briefing.

**Exercise 2 – China Counterespionage Laws Since 2023 (Improved Prompt)**

You are an international law and national security analyst. I need a comprehensive report on China’s counterespionage laws enacted or amended since 2023.

Please:

1. List all relevant laws or amendments with official names and dates.

2. Summarize their main provisions, scope, penalties, and enforcement mechanisms.

3. Highlight potential implications for foreign nationals, businesses, and government agencies.

4. Include examples of enforcement actions or cases, if publicly available.

5. Compare these laws with previous counterespionage laws to identify significant changes or trends.

6. Provide credible, publicly available sources for each law (government websites, English-language news reports, legal databases).

7. Present your answer in a structured, bullet-point format and maintain a neutral, culturally sensitive tone.

**Exercise 3 – Advanced Simulation Technologies for Military Training (Improved Prompt)**

You are a defense research and technology analyst. My goal is to explore how advanced simulation technologies can optimize military training and combat readiness.

Please:

1. Formulate a clear, researchable question based on the goal above.

2. Identify key factors, including types of simulation (VR, AR, AI-driven), training objectives, effectiveness metrics, adoption barriers, and integration strategies.

3. Provide empirical examples or case studies where available, including metrics of success.

4. Suggest analytical frameworks or methods for evaluating simulation effectiveness.

5. List credible sources for research, including defense journals, government reports, and peer-reviewed papers.

6. Present your answer in a structured, professional, and concise format using bullet points or tables.

7. Maintain a neutral, analytical tone suitable for policy or military research.

✅ **Why these prompts are improved:**

* **More specific:** They ask for precise variables, examples, timelines, and comparative insights.
* **Structured output:** Emphasizes bullet points, sections, and tables for clarity.
* **Source-driven:** Requests credible, publicly available sources.
* **Analytical depth:** Prompts models to provide frameworks, comparisons, and potential implications.
* **Tone control:** Ensures outputs are professional, neutral, and culturally sensitive.

**Compact AI Comparison Table – Improved Prompts**

| **Exercise** | **AI Model** | **Key Insights** | **Sources** | **Gaps / Follow-up** | **Usefulness** |
| --- | --- | --- | --- | --- | --- |
| 1. Quantum Computing & Encryption | ChatGPT | Identifies encryption types (RSA, ECC, symmetric/asymmetric), affected systems, post-quantum mitigation, realistic threat timeline, comparative country approaches. | NIST reports, cybersecurity journals, government cybersecurity publications | Need deeper technical detail on specific government systems; may require further risk quantification. | 5 |
|  | Claude | Highlights technological and policy impacts; emphasizes mitigation strategies and international comparisons. | Academic papers, policy briefs, cybersecurity reports | Less detailed timeline for quantum threat; fewer specific system examples. | 4–5 |
|  | Gemini | Structured operational, policy, and technical analysis; includes timeline and analytical frameworks; comparative insights. | Defense research reports, peer-reviewed cybersecurity journals | Some suggested sources may require verification; practical mitigation details may need expansion. | 5 |
| 2. China Counterespionage Laws | ChatGPT | Summarizes new laws, key provisions, penalties, enforcement; notes foreign implications; includes comparison with prior laws. | Official legal documents, English-language news, legal databases | Limited empirical enforcement examples; may need deeper historical context. | 5 |
|  | Claude | Concise summary with law amendments and implications for foreign entities; structured format. | Government websites, legal journals, policy briefs | May miss some lesser-known amendments; fewer enforcement examples. | 4–5 |
|  | Gemini | Detailed analysis of legal framework, operational implications, affected sectors, and comparison to prior laws. | Public legal sources, news reports, government publications | Some historical context and enforcement case studies may be limited. | 5 |
| 3. Simulation Technologies for Military Training | ChatGPT | Identifies simulation types (VR, AR, AI), training objectives, effectiveness metrics, adoption barriers, integration strategies; includes case studies if available. | Defense journals, military reports, government publications | Empirical data may be limited; may need more quantitative metrics. | 5 |
|  | Claude | Focuses on structured research question, technology and operational impacts, adoption challenges. | Academic papers, think tank reports, defense publications | Limited case study detail; fewer suggested frameworks. | 4–5 |
|  | Gemini | Structured, analytical framework; identifies training objectives, simulation types, evaluation metrics, integration strategies, and case examples. | Defense tech reports, peer-reviewed journals, government sources | Some sources may need verification; quantitative evaluation data may be limited. | 5 |

**Notes / How to Use**

1. **Run the improved prompts** in each AI.
2. **Replace “Expected” insights with actual outputs** in the table.
3. **Score the usefulness, accuracy, and completeness** as you evaluate real results.
4. Use **Gaps / Follow-up** to track areas needing additional research.
5. Compare models to select the one that consistently delivers **high-quality, actionable outputs**.

\_\_\_

To refine the research question for clarity, relevance, and completeness, we need to address several key aspects: the definition and scope of emerging technologies, the relationship to national security and encryption, the potential risks and benefits, and the context of existing research in the field. Here's an updated version:

### **Refined Research Question:**

**"How might emerging technologies, particularly quantum computing, influence national security by altering the effectiveness of current encryption methods for protecting sensitive government data?"**

### **Key Refinements:**

1. **Clarify "emerging technologies"**:  
   * By specifying "quantum computing," the focus is narrowed to a specific technology that is likely to have the most significant impact on encryption. This avoids vagueness and enhances the specificity of the question.
2. **Clarify the relationship to national security**:  
   * The term “impact national security” is kept but specified by focusing on the direct aspect of encryption, which is a core component of protecting government data. This helps ensure that the question stays on track and doesn't veer too broadly into other areas of national security.
3. **Focus on encryption and sensitive data**:  
   * Instead of simply “encryption of sensitive government data,” the revised question focuses on \*\*how quantum computing may alter the effectiveness of \*\*existing encryption methods. This specifies the direction of the impact and ties it to current encryption systems, which are central to national security debates.
4. **Incorporate existing knowledge**:  
   * The phrase “alter the effectiveness of current encryption methods” directly connects the question to a well-established issue in cybersecurity—how quantum computing might break current cryptographic algorithms, such as RSA and ECC, and the need for post-quantum cryptography.

### **Additional Considerations:**

* **Specificity**: If you're looking to explore different facets of this question (e.g., political, technological, economic), you might further specify the particular domain of national security you're focusing on (e.g., military, cyber defense, intelligence).
* **Scope of Encryption**: If you want to narrow it down even further, you might specify the types of encryption (e.g., symmetric vs. asymmetric) or certain government systems that are particularly vulnerable.

This revised question is more focused, aligns better with existing research in the intersection of quantum computing and cryptography, and is clearly framed for analysis.