- **The problem I think we should center on**
    - Flechais & Chalhoub show that ethical issues in cybersecurity are not rare edge cases. They come up during routine work because practitioners make high-impact decisions with incomplete info, conflicting stakeholders, and real authority (access, monitoring, denial of service, disclosure choices, etc.).
        - Cyber practitioners hold discretionary power. What keeps that power constrained in practice when the work is fast, opaque, and often protected by confidentiality?
    - **Main question:**
        - How do security practitioners stay aligned with codes of ethics in ways that actually prevent abuse of power?
    - **Sub-questions**
        1. **Where does "power" show up in daily practice?**
            a. Use Flechais & Chalhoub's CyBOK mapping as the structure (human/org, attacks/defenses, systems, software, infrastructure).
        2. **What are the failure modes?**
            a. Examples: over-collection, unnecessary surveillance, retaliation, hiding incidents, "silent fixes," excessive access, and using tools beyond authorization.
        3. **What happens when someone sees misconduct?**
            a. Reporting behavior: barriers, incentives, cultural norms, mechanisms, frequency.
        4. **What would "real" ethical control look like?**
            a. Not just "have a code," but enforceable routines: approvals, logging, separation of duties, escalation ladders, protected reporting channels, and independent review.
    - **What to cover:**
        - **Barriers:** fear of retaliation, career harm, NDAs/confidentiality, "it's normal here," loyalty to team, ambiguity ("is this actually unethical?").
        - **Appetite and culture:** do leaders want to know, or just want problems to stay quiet?
        - **Mechanisms:** internal channels, hotlines, compliance, external regulators, and professional bodies.
        - **What "counts" as reportable:** misconduct vs bad judgment vs "grey-zone."

- **How the military relates:**
    - AI Prompt: “Compare military and cybersecurity professionals with relation to ethical decision making and provide academic journals that may be helpful.”
    - Both military and cybersecurity are professions where people are entrusted with power. The difference is that the military has more explicit accountability structures around authority.
    - **Compare:**
        - chain of command and responsibility expectations
        - explicit norms about accountability for decisions
        - formalized professional identity and discipline
        - reporting misconduct as part of duty, plus the realities and frictions
    - Some sources we can cite for the military side of things:
        - “Paradoxes of Professionalism” (International Security, MIT Press) MIT Press Direct
        - Naval War College Review (professional military ethics and accountability themes) Digital Commons
        - Military Review PDF on command responsibility/accountability Army University Press

1. Define “abuse of power” for this project
2. Pick 2–3 CyBOK areas to go deeper (for example: incident response + privacy/monitoring + vulnerability disclosure).
3. Draft the military comparison as a subsection: “How professions operationalize accountability for authority,” using the sources above.

- Other useful sources from the previous outline:
    - **Insider threat & misuse of access**
        - Cases where employees exfiltrate customer data, abuse admin privileges, or snoop on records (healthcare, financial institutions). PMC+1
        - Ethical angles: least privilege violations, lack of monitoring, culture that tolerates “peeking”.
    - **Cross-jurisdiction ethics (US vs EU vs more authoritarian regimes)**
        - There’s comparative legal work on privacy and surveillance, but less on:
            - How practitioners in different legal regimes handle ethical conflicts (e.g., Chinese vs EU vs US data retention, encryption, monitoring). Premier Science+1