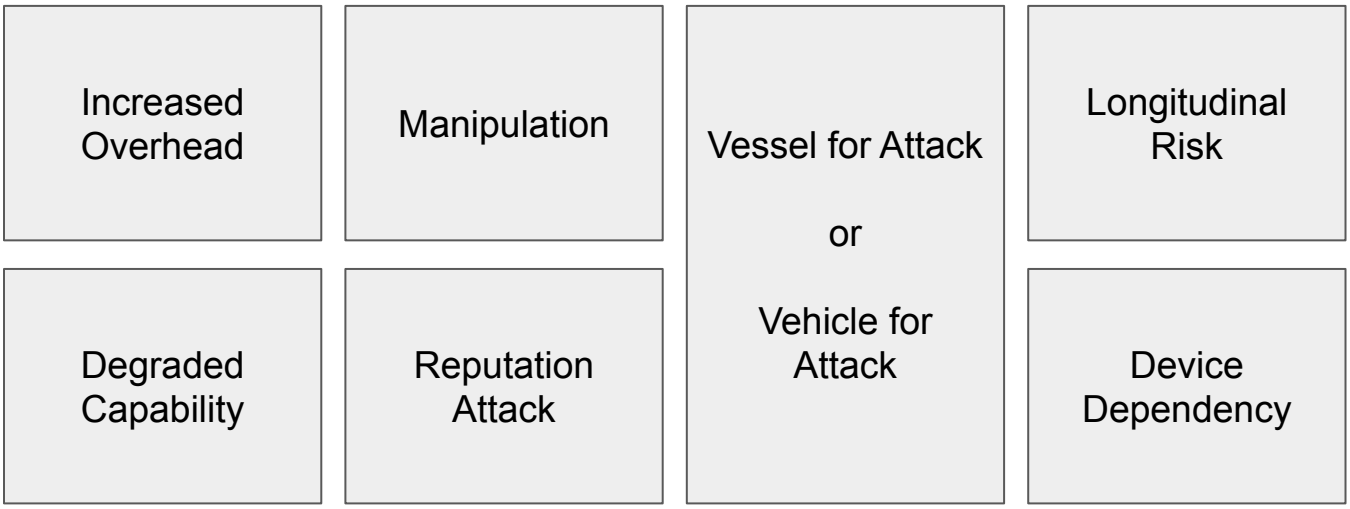
Objective Threat Model

A method from op1digital, turning strategic plans into real-world results since 2016.



The base model can be extended with sub-model definitions.

Objective Threat Model (OTM) is a problem-solving method that emphasizes impacts and outcomes of threats over the technical mechanisms of attack. Focusing on outcomes broadens understanding of how diverse mechanisms manifest.

Challenge Questions for Human Detection

1. Does this increase my burden?
2. Am I being held back or blocked?
3. Am I being manipulated?
4. Could this harm someone's reputation?
5. Does this present a vessel or vehicle for attack?
6. Am I subject to sustained risk?
7. Am I losing autonomy?

Sample Problems

- Technological vulnerabilities
- Operational impacts
- Business risks
- Non-technical threats

Key Framing Questions

- How does the user's context change threat exposure?
- How does the user's context change potential impact?

About the Technique

OTM is flexible and context-aware, adapting to evolving threats including psychological operations, competitor strategies, and information warfare. Human training, LLM and implementation materials are available.

Objective Threat Model Appendix A

Base Model Threat Definitions

The following threat definitions are included in the OTM base model:

- **Increased Overhead:** Costs, time, cognitive load, opportunity cost, and other burdens.
- **Degraded Capability:** Barriers or impediments to completing a desired action, including denial of service and communication blocks.
- **Manipulation:** Data harvesting, targeting, misinformation, or actions that trigger alterations in behavior or decision-making.
- **Reputation Attack:** Degradation of trust or perception between parties, including fabricated or leaked harmful information, spoofing, degraded reliability, and experience.
- **Vessel or Vehicle for Attack:**
    - **Vessel:** Devices or systems that are accessed as containers for their natural contents (e.g., personal data, credentials, media) or co-opted to carry a harmful payload (e.g., malware).
    - **Vehicle:** Devices or systems serving as launch points for attacks on resources, such as data exfiltration, privilege escalation, surveillance, or network attacks.
- **Longitudinal Risk:** Maintaining presence, propagating, or evolving over extended periods, leveraging interdependencies, residual data, or sustained impact to amplify risk. This includes cascading failures, latent data exposure, and threats that unfold through gradual escalation, time-based exploitation, or adaptive evolution in response to resistance.
- **Device Dependency:** Creating or exacerbating a reliance on a specific device, app, or ecosystem, reducing the user's autonomy, decision-making capability, or ability to function independently.