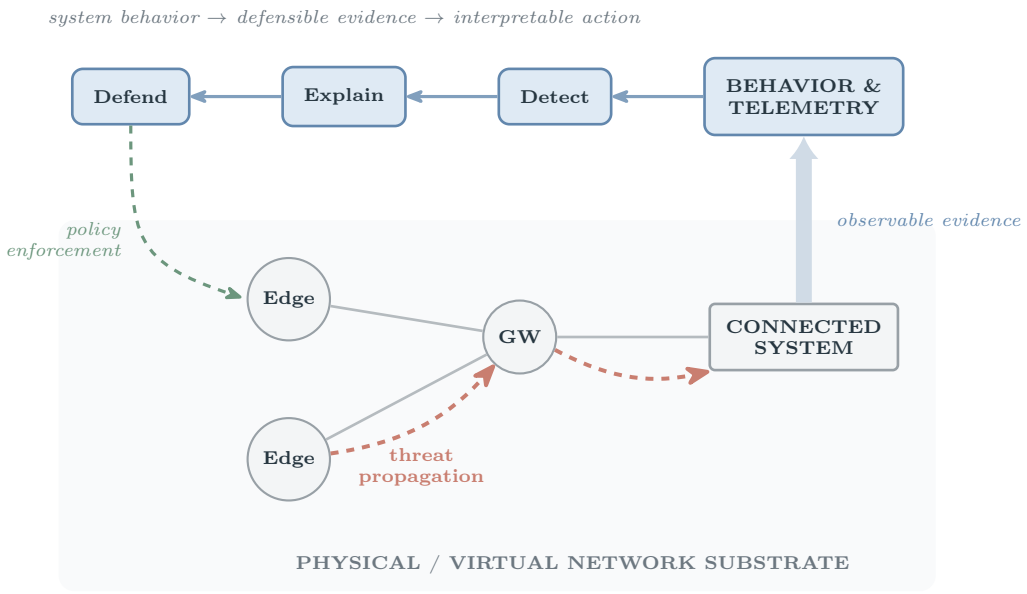
Research Interests

Tran Duc Le

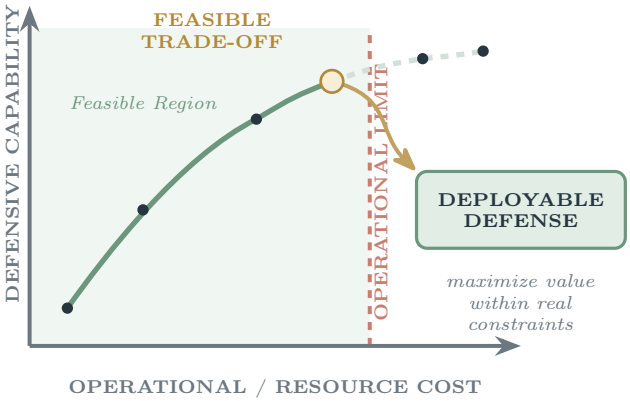
I study how networked systems can be defended when evidence is incomplete, operational resources are limited, and some defensive decisions are increasingly automated. This perspective grew from my doctoral work on wireless networking, where contention, interference, and protocol behavior led naturally to questions of resilience and adversarial behavior. My research now centers on two established themes, **network and systems security** and **deployable security analytics**, with an emerging extension into **AI-enabled cyber defense**. The common thread is practical: understand system behavior, derive defensible evidence, turn that evidence into usable controls, and automate only where doing so remains transparent and governable.

Network and Systems Security



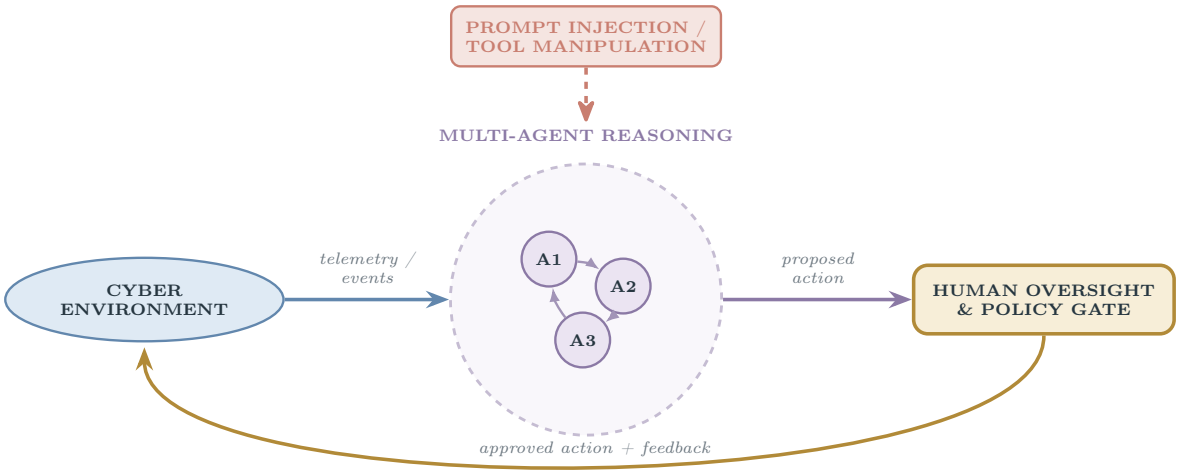
My core research examines how attacks emerge from network and system behavior and how defensive evidence can remain faithful to that behavior. Early work modeled malware propagation in vehicular and Wi-Fi networks; more recent studies address IoT/IIoT intrusion detection, malware traffic analysis, and explainable intrusion triage. Across this work, I have remained interested in protocol-aware and behavior-aware defense: how to detect attacks while preserving evidence that helps explain what happened and supports a practical response.

Deployable Security Analytics



A second line of work asks whether technically strong defenses remain useful under operational constraints. During my postdoctoral research on cybersecurity for small and medium-sized enterprises (SMEs), I examined user behavior, malicious-content threats, enterprise security analytics, and capability prioritization in organizations with limited staff, telemetry, and budgets. This work shifted my emphasis from model performance alone toward deployment feasibility: what can an organization understand, maintain, and justify? I am especially interested in methods that account for resource limits, analyst workload, explainability, and implementation cost.

AI-Enabled Cyber Defense



More recently, I have begun extending this systems-and-deployment perspective to AI-assisted and agentic cyber defense. My work in this area includes prompt-injection contagion in multi-agent systems and ongoing studies of tool-using agents. I am interested in the security risks that arise when AI systems interact with other agents, external tools, and operational environments, as well as in mechanisms that keep automated actions constrained and subject to human review.

These interests are connected by a common concern with how security mechanisms behave in real systems and how they can support practical defense. I use network and system measurement, security modeling, machine learning, and controlled experimentation as tools rather than ends in themselves. My goal is to develop cyber-defense methods that are technically grounded, practical to deploy, and understandable to the people responsible for operating them.