Soft Target Engineering to Neutralize the Threat Reality

RC.1: Machine Intelligence for Effective Threat Deterrence and Risk Mitigation at Soft Targets and Crowded Places: Focus on Urban Surface Transit Systems

PIs: *Auroop Ganguly (a.ganguly@northeastern.edu) and Samrat Chatterjee;* ***Postdoc:*** *Rishi Sahastrabuddhe*

Graduate Student Contributors: *Puja Das, Ashis Pal, Jack Watson*

SENTRY RC.1 Challenge

Model Threat Deterrence and Mitigate Risk

- Develop knowledge guided data science (machine learning and network science) methods for predictive understanding of threats to support risk-informed decisions
- Demonstrate on soft targets and crowded places, focusing on surface transportation such as multiscale urban and regional rail

Inform Threat Analytics and Policy

- Deter, absorb, prepare for, and adapt to threats to interconnected systems and inform interventions and investments
- Develop network-level threat deterrence that account for system connectedness

Accomplishments

Performance Evaluation

- Unit testing of data and model components for multiscale rail transit
- System testing of hybrid physics-data threat deterrence models
- Integrated testing with stakeholders in DHS and homeland security enterprise

Project Milestones

- Year 1: Acquire and simulate network topology and dynamical behaviour data relevant to multiscale rail systems
- Year 2: Develop risk assessment and threat deterrence prototypes
- Year 3: Validate and enhance prototype tools with stakeholder feedback

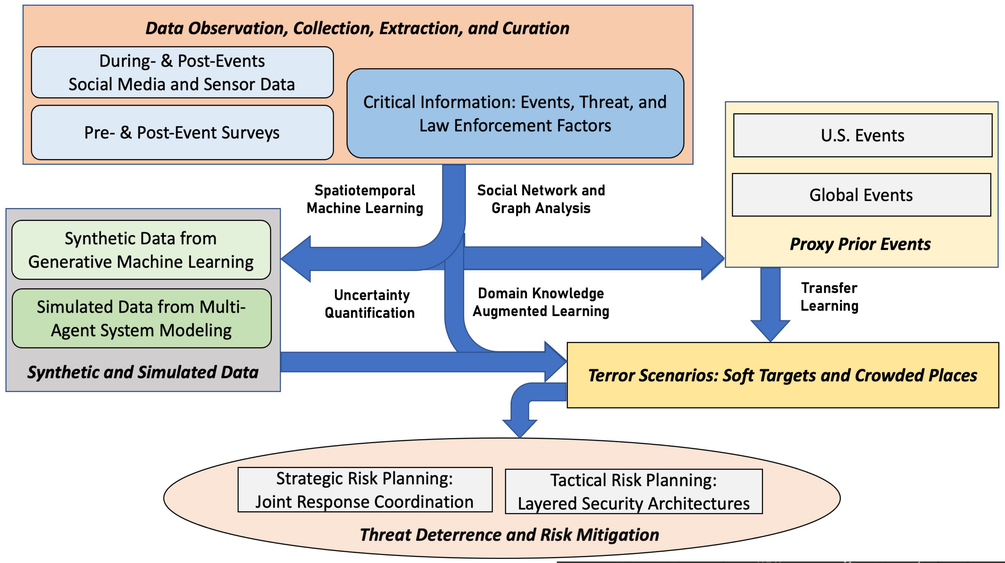
Addressing the Challenge

Challenge

- Blending disparate data and methods under uncertainty and evaluating knowledge driven data science models for generalizability under changing conditions
- Bringing together network risk and resilience elements with attacker-defender threat optimization to deter network-level threats

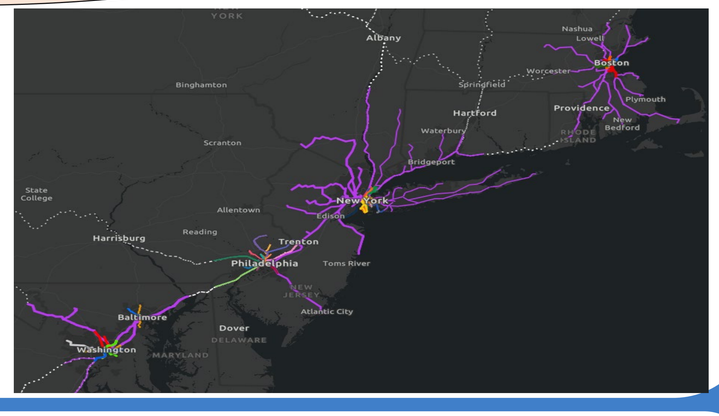
Approach

- Develop interpretable machine learning and network science methods with behavioural simulations and dynamical models for actionable insights to improve STCP security
- Develop attacker-defender models for event or location threats in a way that considers risk and resilience elements of interconnected or networked systems with a demonstration on soft targets related to urban transit systems



The SENTRY RC.1 Approach: *A hybrid knowledge-guided network science and machine learning system embedded with behavioral modeling and what-if simulations for predictive understanding of network-level threats leading to risk-informed policy and intervention or investment decisions*

The SENTRY RC.1 Case Study: *The "Bos-Wash" corridor, the highest revenue-generating megaregion on the planet, is connected by multiscale rail systems, ranging from metro rails in Boston, New York / New Jersey and Washington, DC, to regional or great city rail systems such as the greater Boston commuter rail, as well as longer distance rail that connect the cities and the urban-rural regions*



Next Steps

Future Research Plans

- Develop solution frameworks for network level threat deterrence in the soft targets with a focus on surface transportation
- Formulate hybrid knowledge-guided data science and behavioral models with a proof of concept on threats in urban rail networks
- Inform threat deterrence assessments and resource allocation, including intervention and investment strategies, for mitigating threats

Supporting the Virtual SENTRY framework

- Provide Virtual SENTRY with cutting edge STCP risk assessment prototype tools focussed on surface transportation
- Develop peer-reviewed technical publications and end user/stakeholder guidance documents

Partnerships and stakeholders

- CISA hometown security program and National Risk Management Center (NRMC)
- U.S. Secret Service National Threat Assessment Centre (NTAC)
- Surface transportation owners and operators and the broader homeland security enterprise

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award 22STESE00001-02-00. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security. 04/2023