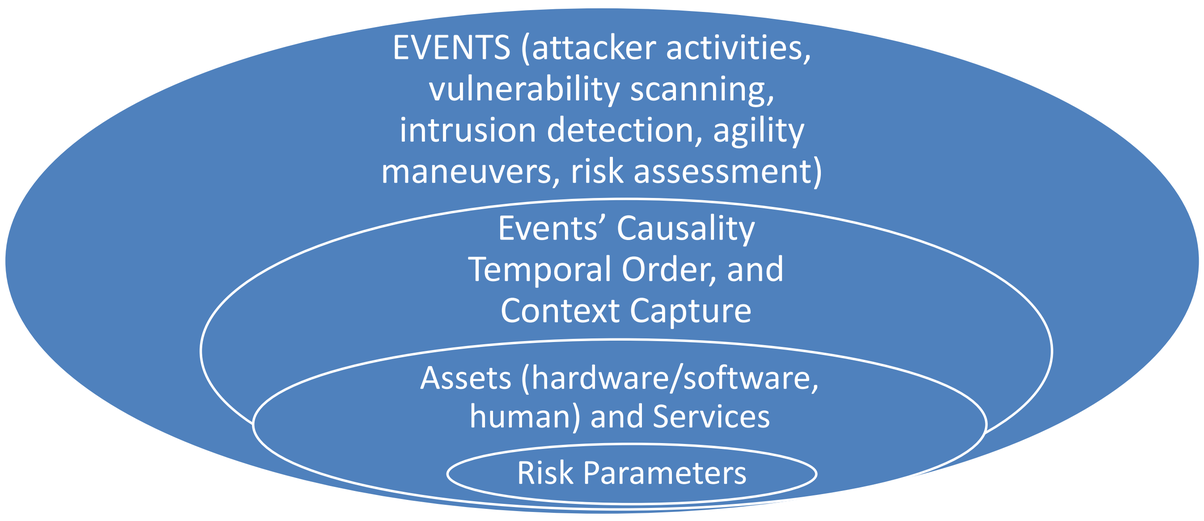
Risk Model Roadmap from Events to Parameters

S&T Campaign: Information Sciences
Cybersecurity

Hasan Cam, (301) 394 2871
hasan.cam.civ@mail.mil

Research Objective

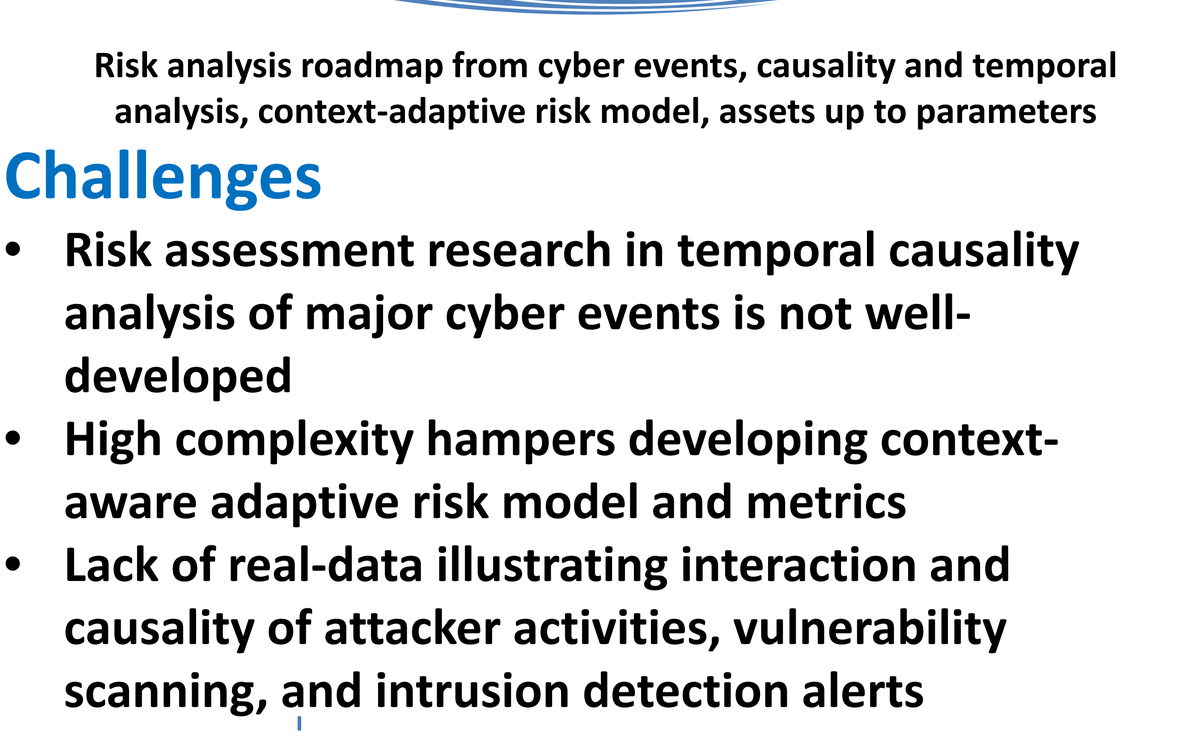
- **Detect, analyze, and assess temporal and spatial causality of cyber events representing activities**
- **or occurrences of attacker, exploit, vulnerability, intrusion, etc.**
- **Develop a holistic context-adaptive model that leverages observations and analysis results**
- **Incorporate human behaviors and cognitive analytical reasoning into risk model**



Risk analysis roadmap from cyber events, causality and temporal analysis, context-adaptive risk model, assets up to parameters

Challenges

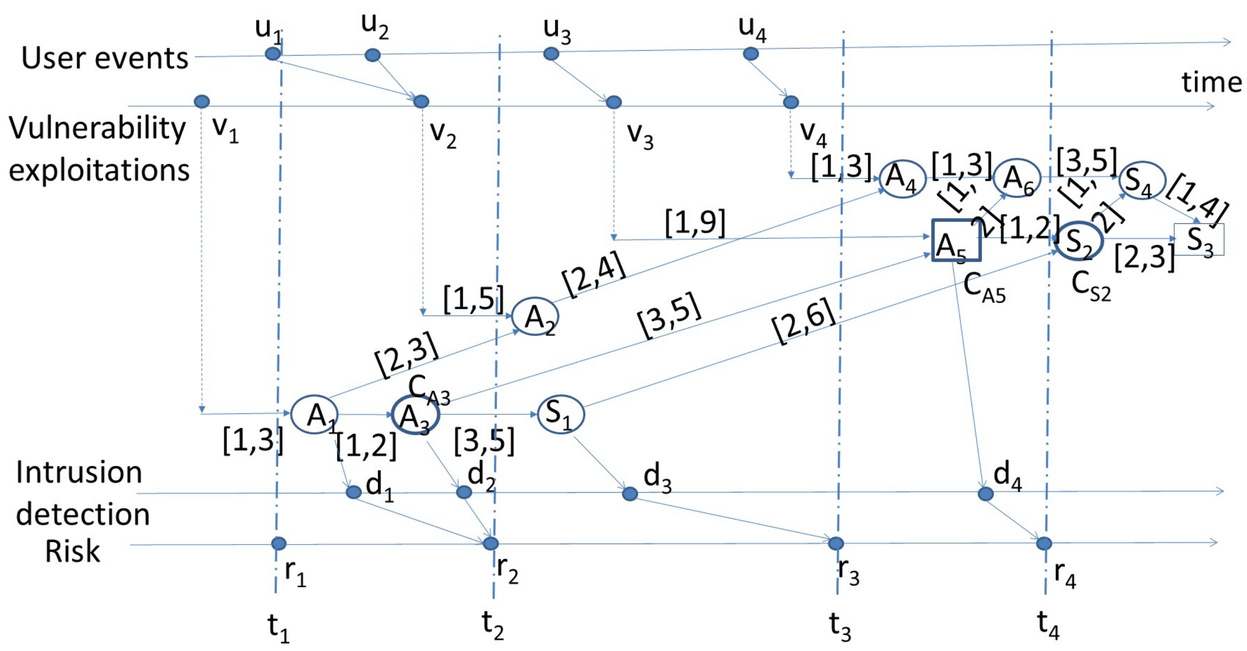
- **Risk assessment research in temporal causality analysis of major cyber events is not well-developed**
- **High complexity hampers developing context-aware adaptive risk model and metrics**
- **Lack of real-data illustrating interaction and causality of attacker activities, vulnerability scanning, and intrusion detection alerts**



Temporal causal history of cyber and user events with vulnerability-centric pairing graph

ARL Facilities and Capabilities Available to Support Collaborative Research

- **ARL Cyber Lab**
- **Network Science Research Laboratory**
  - Integrated framework for experimentation on networks
- **DOD HPC supercomputing resource center**
- **Results:**
  - Causality analysis of events
  - Risk parameterization (Identification and characterization of parameters)
  - Risk-agility interaction
  - Preliminary risk model



Controlling influence of vulnerability exploitation on assets and services

Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- **Expertise in real-time gathering and storing of interaction of multiple processes' events**
- **Desire expertise in extracting quality and outlier information from cyber events by proper data mining**
- **Modeling cognitive resilience for social vulnerability using risk and trust**

Publications:

- H. Cam, "Risk Assessment by Dynamic Representation of Vulnerability, Exploitation, and Impact," Proc. of Cyber Sensing 2015, SPIE Defense, Security, and Sensing, April 20-24, 2015, Baltimore, MD.
- James R. Morris-King and Hasan Cam, "Ecology-Inspired Cyber Risk Model for Propagation of Vulnerability Exploitation in Tactical Edge", Accepted to MILCOM 2015, Oct. 26-28, 2015, Tampa, FL, USA.
- J. Morris-King and H. Cam, "Modeling Risk and Agility Interaction on Tactical Edge", NATO Workshop IST-128-RWS-019 on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact, June 15-17, 2015, Turkey.