The Fourth ACM International Workshop on Critical Infrastructure Network Security (CINS) will be held fully virtually on June 14, 2021 in conjunction with ACM SIGMETRICS.

**Workshop Organizers**
Sergiy Butenko (Texas A&M University, USA)
Pavlo Krokhmal (University of Arizona, USA)

**Call for Papers**

The modern critical infrastructure networks are characterized by increasing complexity and pervasiveness. Realistic mathematical models of such networks should take into account their multilayered, interdependent, heterogeneous, and dynamic nature. Modeling the security aspects of critical infrastructure requires understanding of risks and uncertainties associated with potential natural disasters and adversarial attacks involving multiple interacting agents. On top of this, the impact and dependence of human-made infrastructure on ecosystems, biodiversity, and socio-economic interactions are becoming increasingly important and cannot be overlooked. Therefore, motivated by recent crises related to pandemics, cascading blackouts, and forest fires, this workshop aims to focus on issues related to the interdependence of infrastructure and ecological, biological, and social networks, in addition to more traditional topics concerning security, robustness, and vulnerability of infrastructure networks. More specifically, the workshop participants will discuss recent progress and will seek to identify promising future research directions on the following topics, among others:

- Mathematical models describing structures that characterize the network's robustness and vulnerability to a cyber/physical attack or a natural disaster.
- Probability-based risk measures characterizing a network’s vulnerability to edge/node failures.
- Exact, approximate, and heuristic algorithms for designing minimum cost robust network topologies and for detecting robust structures of interest in networks.
- Mathematical models and algorithms for identification of critical network components.
- Optimization and machine learning techniques to predict, restrict and control the damages and losses associated with various risk factors that affect the operations of interdependent networked systems.
- Case studies concerning ecosystems, as well as large-scale real-life supply chain, communication, social, and energy networks.

We invite submissions of short abstracts (up to one page) of proposed talks by email (butenko@tamu.edu and krokhmal@arizona.edu).

**Important Dates**
May 17, 2021: Abstract submission.
May 31, 2021: Author notification.
June 14, 2021: Workshop