

Cybersecurity and Security by Design Research

Cybersecurity for Infrastructure has been identified as the intersection of computer science, civil engineering, criminology, and environmental engineering. Risks exist in different phases of the design, construction, and operations of major infrastructure and building projects. Sectors impacted range from transportation and aviation, to water, power, and other utilities. The concept of Secure by Design starts with the software used in project planning, financing, design, and construction. It interconnects physical security parameters with those that are more ethereal. Research in 2019-20 will build upon the base of the 2018-19 CBIPS Fellows



The water supply system of NYC is vulnerable to attack



LaGuardia Airport Redevelopment factors in security concerns

The Center for Buildings, Infrastructure and Public Space held an Industry Advisory Board Meeting in May 2019, at Columbia's Faculty House, in conjunction with a Cybersecurity Colloquium. At the discussion we heard from industry experts in the public and private sectors on the implications and import of cybersecurity in relation to physical infrastructure. Specific topics included:

- Standards and regulations needed to govern response and better define Service Level Agreements
- Need for employee training and public education to raise awareness of the risks of cyber attack
- Conflict between connectivity and transparency on the one hand, and security on the other
- Costs of changes in networks and capital projects to assure physical and cyber-safety
- Benefits of collaboration and partnerships between public and private sector organizations

The goal of this year's research would be to expand on the progress made in the 2018-19 academic year by focusing on aspects of cybersecurity related to particular large-scale infrastructure projects and targets, ranging from the potable water system administered by the NYC Department of Environmental Protection (DEP), the transit facilities operated by the NYC Metropolitan Transit Authority (MTA), and the Port Authority of New York and New Jersey (PANYNJ). At the Cybersecurity Colloquium we learned that the PANYNJ has created a cybersecurity operations center that is linked to threat response from the Multi-State Information Sharing and Analysis Center (MS-ISAC), which gives real-time alerts. The PANYNJ also created a training program for employees based on a breach report, which indicated that 90% of problems are caused by employees and are avoidable. Part of the goal of the Secure by Design research initiative at CBIPS will be to ascertain the risks and responses resulting from physical design, cyber connectivity, and human interface.