Improving Resilience in Cybersecurity and Spectrum
Wednesday, November 15, 2017, 1:00 - 6:30pm
University of Colorado Law School, Boulder

Complex systems fail in complex ways. As system scope and complexity grows, the ability to discover and respond to failure locally is augmented or replaced with distributed, collaborative (or adversarial) approaches to solving problems. Engineering approaches are buttressed by legal regimes that define expectations and responsibilities.

Outages and adverse incidents are regular events in computer networks and wireless systems. It is extremely costly, and perhaps impossible, to design and manage systems that are never impeded by attacks, interference, or brownouts. Because society increasingly depends on computer networks and wireless systems, it has become essential for them to maintain an acceptable level of service in the face of various faults and challenges to normal operation—in other words, to be resilient.

Sound management must encompass up-front design strategies, ongoing vigilance, and after-the-fact responses. To the extent that computing and wireless systems are themselves critical infrastructure or support other critical infrastructure, there may be a need for government policy to support and encourage such management. This conference will explore institutional strategies to improve the resilience of computing and radio systems. They include risk assessment and management, the use of incident reporting, and strategies for learning from "near misses" or actual harms.

Different fields have different approaches to learning from incidents. Medicine, aviation and electric grid management are fields that learn from mistakes, and where other disciplines could learn from many decades of practice improving the safety and robustness of service delivery. In those areas, risk management has accepted that incidents will happen and require institutional strategies to learn from them. In the electricity arena, promoting grid resilience is a feature of a number of policy initiatives. In health care, incident reporting has taken root in the form of "mortality and morbidity" conferences (M&Ms). In the area of airline safety, the National Transportation Safety Board (NTSB) plays a comparable role to M&Ms, providing a forum for the assessment of accidents in the field and generating lessons learned that can elevate best practice. Similarly, the successful (and voluntary) Aviation Safety Reporting System (ASRS) analyzes confidential "near-miss" reports. As an incentive for participation in this program, regulators view participation as evidence of "constructive engagement" and commit to not to use any shared information for enforcement purposes.

The slow rate of improvement in security has also led to calls for imposing liability on software providers or operators. Any such regime, however, must be balanced with our ability to craft learning systems. In spectrum, where instances of radio frequency interferences are not reported or evaluated, policymakers are only starting to craft a regime that would promote greater learning and adaptation.

In all these cases, the overarching goal is to drive greater awareness and learn from experience, not to cast blame or scapegoat individuals for mistakes. In the fields of cybersecurity and spectrum, by contrast, there are no institutional strategies for capturing information around "near misses" or actual incidents, enabling learning around why such harms arise, and driving better practices to avoid them in the future. At this conference, we will bring together a range of professionals, academics, and policymakers to consider how such institutional strategies could be developed and implemented in these areas.