influence and power. The concern used to be protecting information online; now the concern is that people who are upset about a government policy or court cases are using cyber means to protest and can cause havoc on infrastructure remotely.

This makes it all the more important to build partnerships and work together. She recommended building communities of interest, noting that Pierce County has partnered with a number of organizations in the room. She encouraged participants to participate in the day's conversations and use the dialogue to drive recommendations for improving their own systems, and direct assessments and milestones. She added that conferences like this one are a huge help in identifying partners and bringing them all together so we can collectively stay ahead of the hackers.

In cyber, the stakes are high--attacks can be a matter of life and death, not just an issue of a website being taken down. We are hearing more and more about cyber security attacks and concerns of an increasingly hackable world known as the "internet of things." She asked: Could somebody hack your pacemaker? What are new models for delivery like software as service? Are engineers trained and ready? Who has templates for recovery after event? Who has templates even to analyze that you are under an attack? She expressed her enthusiasm for meeting everyone in the room and hearing about their experiences.

The Intersection of Cyber Systems and Physical Infrastructure, featuring Alisha Griswold, Training and Exercise Program Manager, King County Office of Emergency Management

"Cyber security and information security are only as good as operational security."

Griswold began with a ground rule: Hackers are not your enemy. It's not about the act, but the intentions. She explained that parts of the presentation were based on research from Poneman Institute on operational penetration testing. They were extremely successful: Just by wearing a badge, their team could get access to sensitive information. They were not questioned by peers, were able to rummage around other's desks, look into open laptops, review open event calendars, and gain access to mobile devices, USB drives, and keys that were unsecured. We emphasize firewall, but cyber security and information security only as good as operational security. We have to balance security and access.

She shared the Kaspersky cyber security map showing cyber attacks in real time. The U.S. is third most attacked country during the day, and number one at night when the other side of the world is awake, where the majority of our attacks come from.

Griswold explained that there are a lot of legacy systems in fields like transportation and utilities that are being brought online for convenience, though they are old systems not designed for the internet. She referenced Gerull's mention of the "internet of things," the networking of physical objects, such as refrigerators, meant to increase efficiency through accessibility on the existing internet system. This can increase our vulnerability--for example hacking into things like doggy cams, which are meant to let people check on their dogs when they are away from home. Anything on the internet is accessible if not secured.

Griswold played a video of the Aurora Generator Test showing the real world physical impacts that can come from cyber attacks--in this case the complete destruction of a generator cause by a malware directive to overload itself. For this test they destroyed the generator, but Griswold emphasized that impacts need not be as extreme. If a cyber attack caused a machine to corrupt in increments or at a slow rate, the machine may be functionally unusable without damaging it enough to flag its owners that they were under attack.

Resources and Links

Kaspersky realtime cyber security map:
https://cybermap.kaspersky.com/

Aurora Generator Test (Video):
https://youtu.be/fJyWngDco3g

Shodan Search Engine
https://ics-radar.shodan.io/