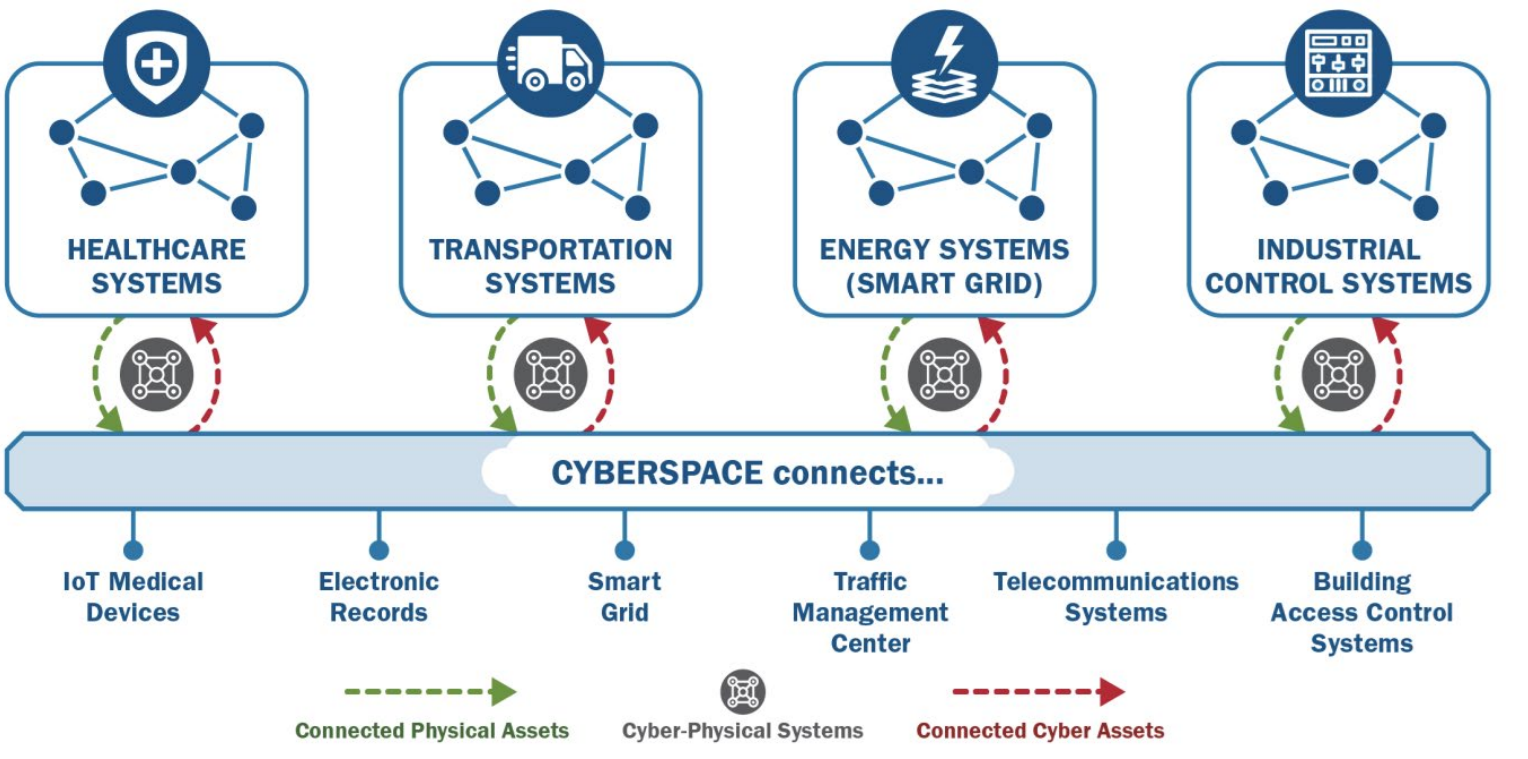
The Threats Cybersecurity Poses to Physical Security

Outline

- Introduction
- Healthcare
- Transportation
- Energy
- Trend Analysis
- Big Picture
- Future
- Takeaways

Introduction



Scope

- Past five years

- Attribution to nation - states/political motives
  - Level of attack requires resources

What is Physical Security?

- Protection of physical systems
  - People, property, assets involved

- A tenant of the *wellbeing* of the physical world

Historic Attack: Stuxnet

- Computer Worm (2009)
- Allegedly USA
  - Operation Olympic Games
- Destroyed near 1000 Iranian centrifuges

Energy & Smart Grid

Colonial Pipeline

May 7, 2021

- Attributed to Darkside Hacker Group
  - Located in Eastern Europe
- Ransomware Attack
- Energy insecurity: cut off supply to East Coast for days
  - Moves 45% of all fuel consumed on East Coast

Ukraine Viasat Attack

Feb 24, 2022

- Russian military intelligence (GRU)
- Acid Rain
  - DDoS & malware wiper
- US satellite internet provider
  - European network outages
  - Coincide with physical invasion

Transportation

MTA Breach

April, 2021

- Attributed to Chinese government
  - Attacked early April, stayed late April
- Zero-day vulnerability in Pulse Connect Secure
- No severe damages
  - 3/18 systems impacted

Metrolinx Attack

January, 2018

- Provincially run Toronto suburban transit authority
- Attributed to North Korea
  - Routed through Russia
- Firewall breach and malware
- No severe damages

Healthcare

Conti Ireland Hospital

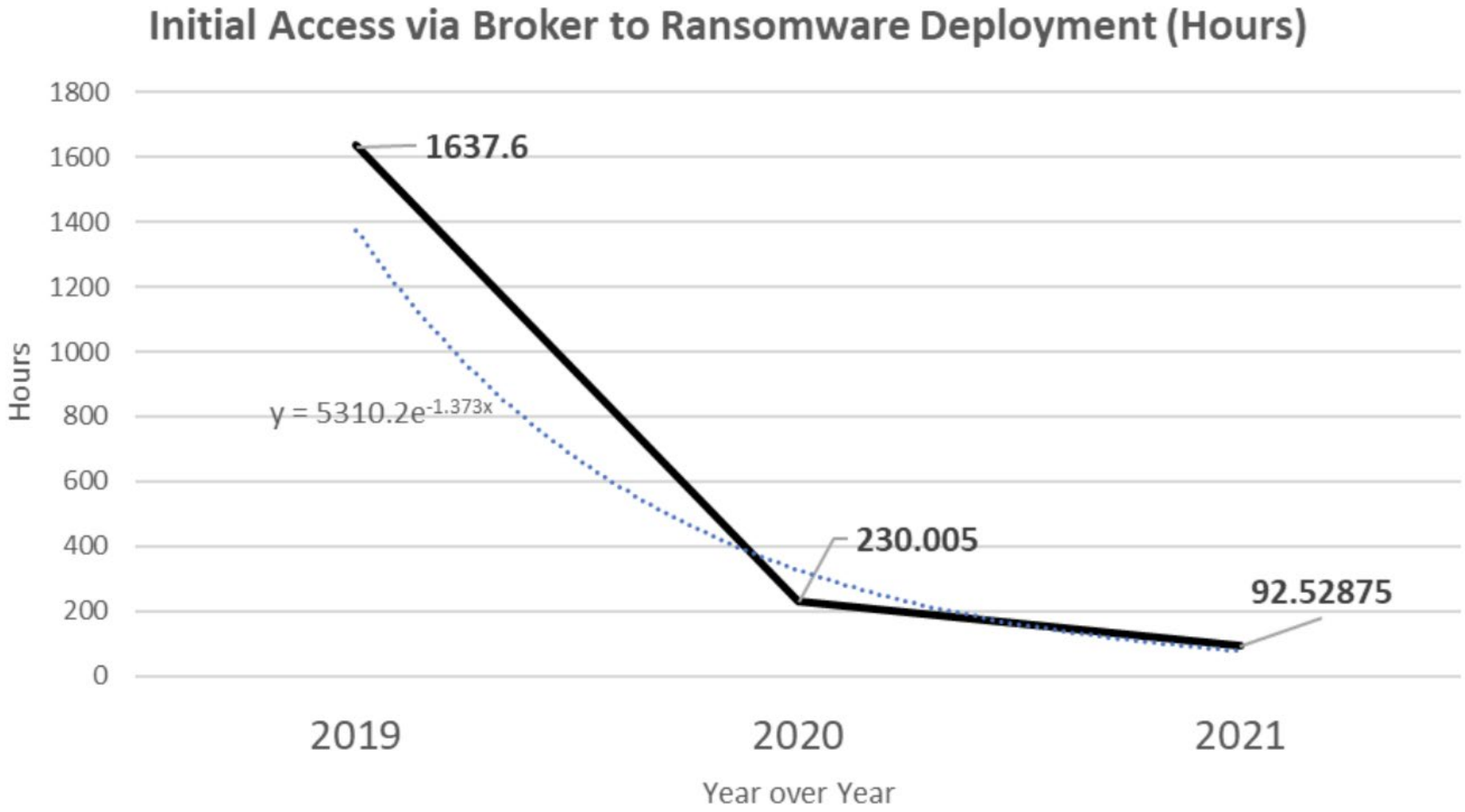
May, 2022

- Russian cybercrime group
  - Possible ties to Russian government
- Ransomware as Service
  - Two months between intrusion and attack
- Delayed hospital functions
  - Hospital treatments, surgeries

Maui Ransomware

May, 2021

- Attributed to North Korea
  - Initial access vectors unknown
- Encrypt medical data
  - electronic health records, diagnostics, imaging, and intranet
- Delay hospital operations


Initial Access via Broker to Ransomware Deployment (Hours)
1800
1600
1400
1200
1000
800
600
400
200
0
Hours
1637.6
y = 5310.2e-1.373x
230.005
92.52875
2019
2020
2021
Year over Year

Trend Analysis

- Energy
  - Widespread effect on operations
- Transportation
  - Reconnaissance
  -
- Healthcare
  - Increasingly at risk post -Covid
  - Loss of life

Trend Analysis

- Chaos
- Malware & DDOS
  - specifically ransomware
- Physical damage to loss of life
- Infrastructure increasingly at risk

Human Security

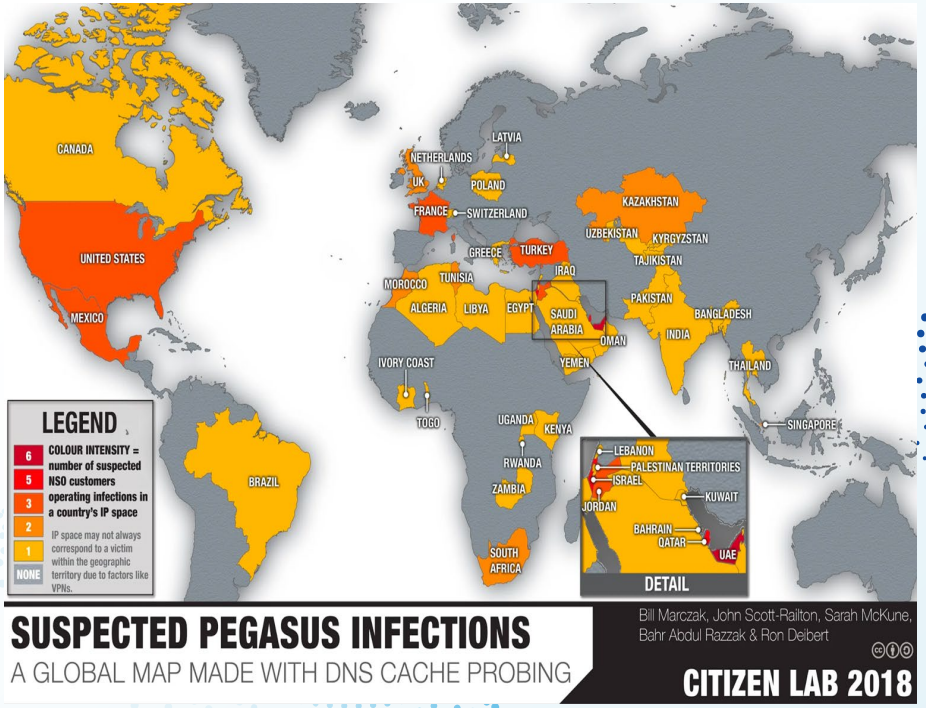
- United Nations Framework

- Seven components of human security
  - Personal
  - Community
  - Economic
  - Political
  - Food
  - Health
  - Environment

Putting Human Security in Context

- Pegasus Spyware (2016)
  - Israeli cyber -weapons firm NSO Group

- Insecurity of phone, info, people
  - Personal
  - Community
  - Economic
  - Political



Big Picture

- **Cybersecurity is Human Security**

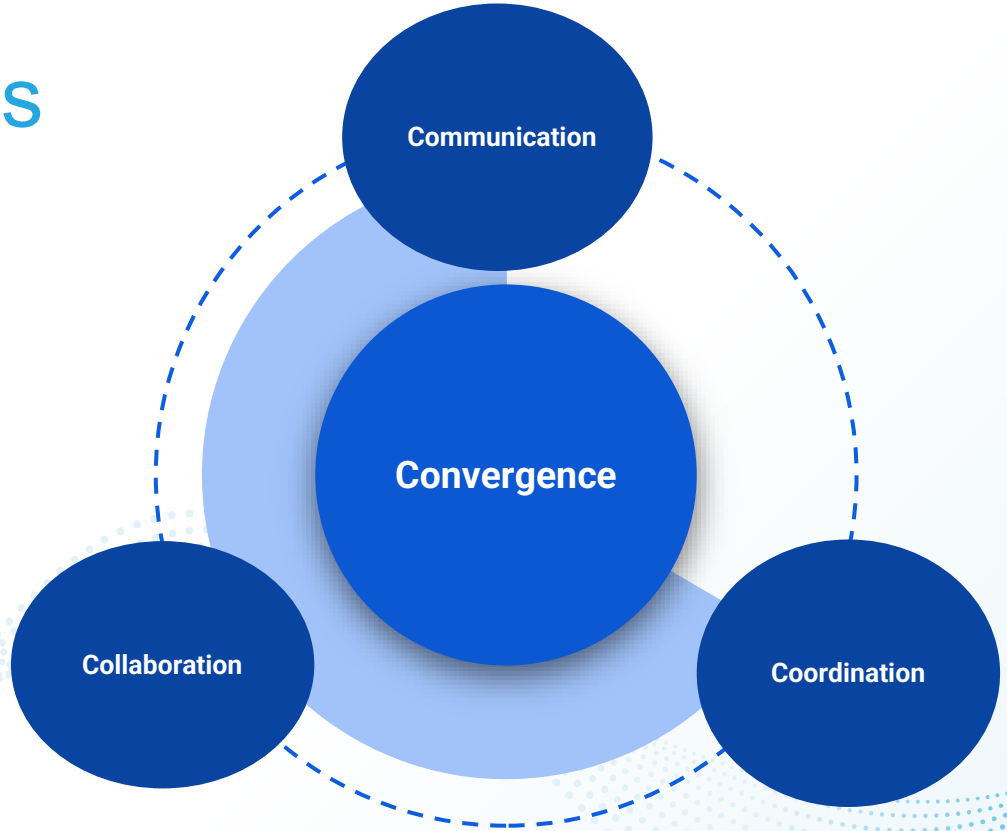
- Various intentions
  - Deliberate physical threats
  - Physical threat is byproduct

- Immense resources

Future of Cyberspace

- Attribution issue
- Spillover effects
- Declaration of war

Takeaways



Special Thank to the Sources

CISA

White House

Vox

NPR

IBM

Cyber Peace Institute

Politico

Krebsonsecurity

CISSecurity

Pelco

Hawaii

Microsoft

NBC

Cyberlaw

HHS

New York Times

Reuters

Checkpoint

SANS

Belfer Center

DFS NY

The ALS Group

Thank You

shreeya@udel.edu