

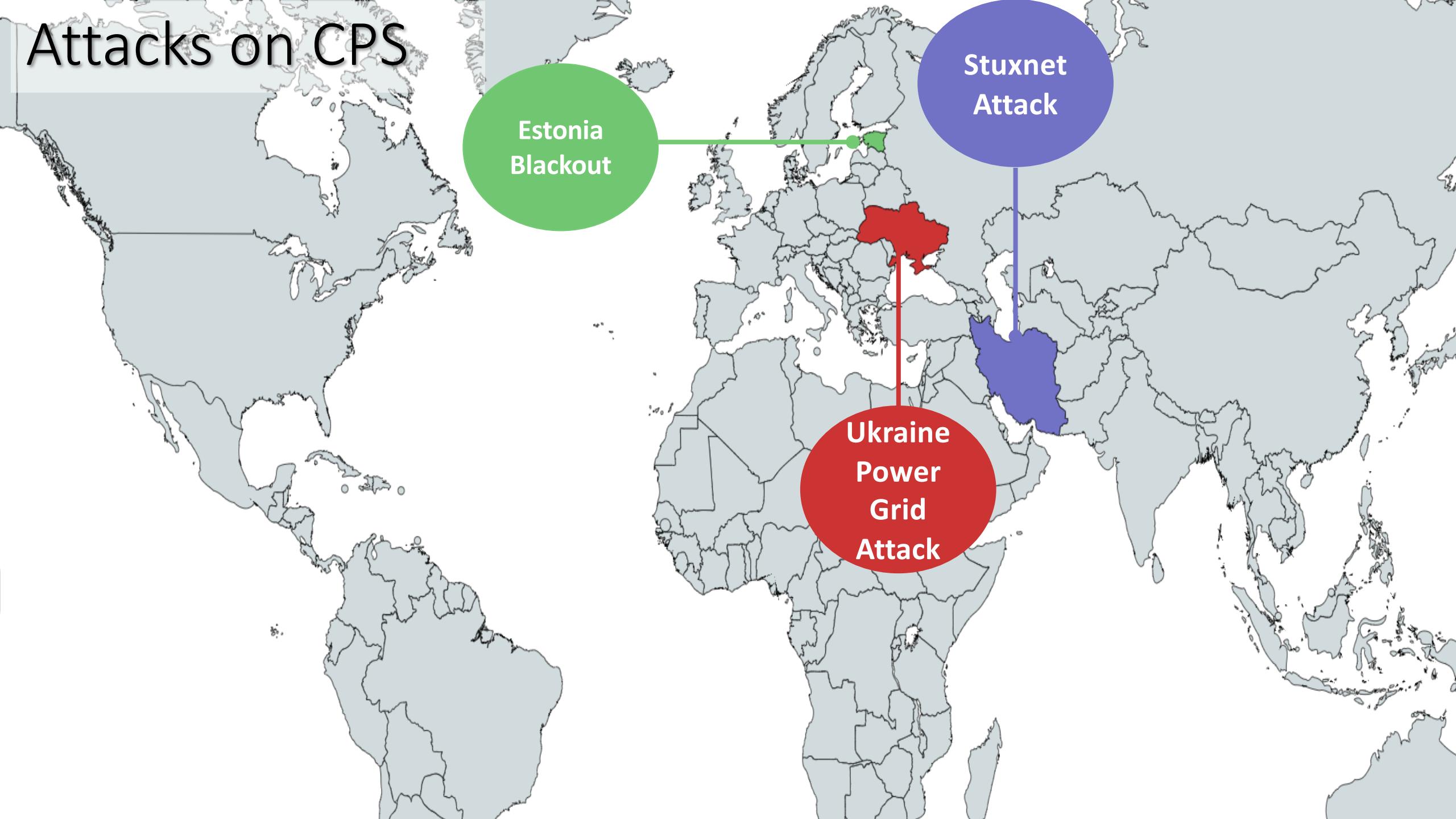
Cyber Security Threats Targeting CPS: A Novel Approach Using Honeypots

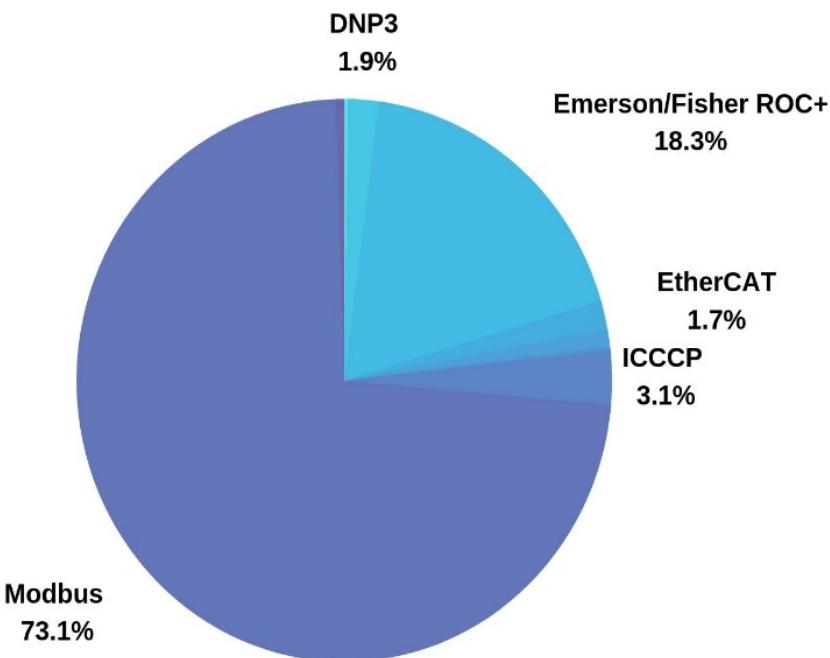
Presented by Dr. Sameera Almulla

University of Dubai

Dr. Claude Fachkha , University of Dubai and Dr. Elias Bou-Harb, Florida Atlantic University

Attacks on CPS





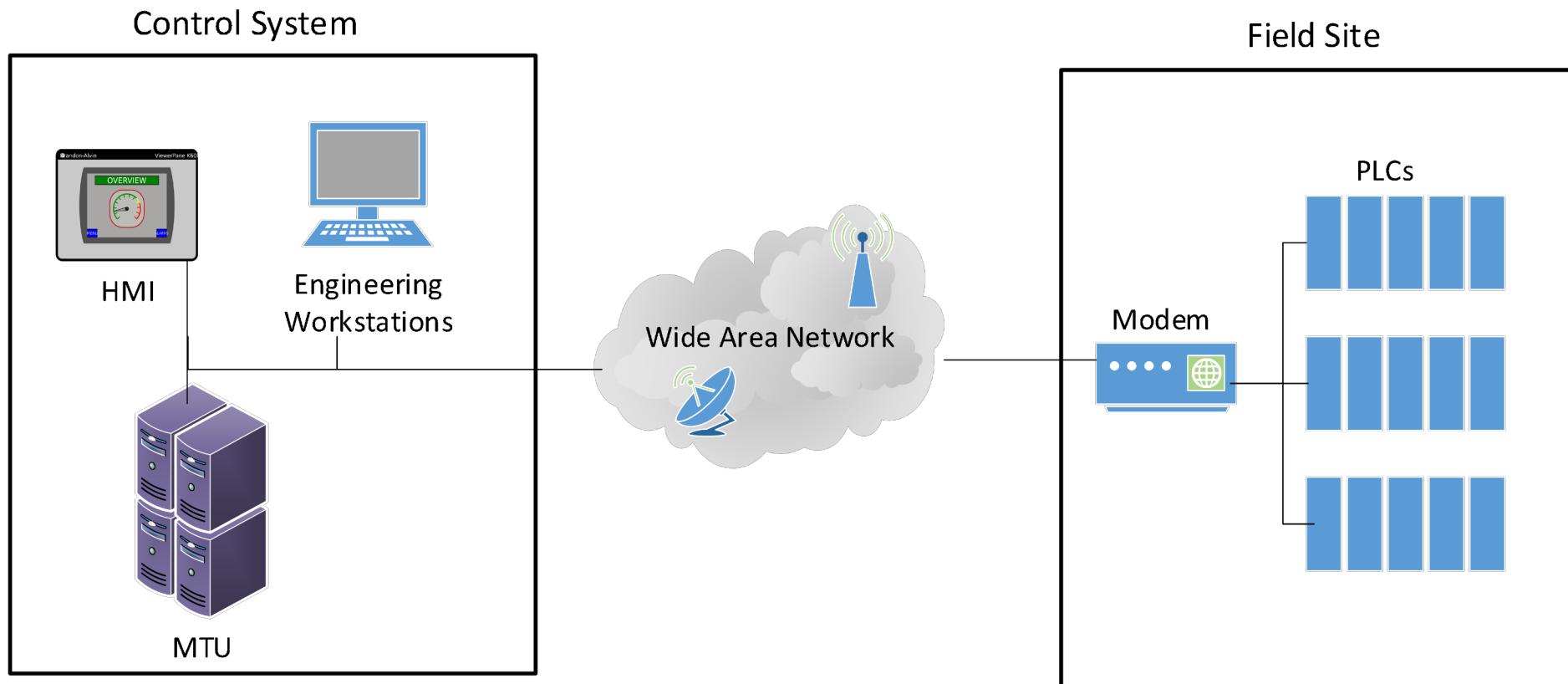
**TOTAL CPS
THREATS**

2560I

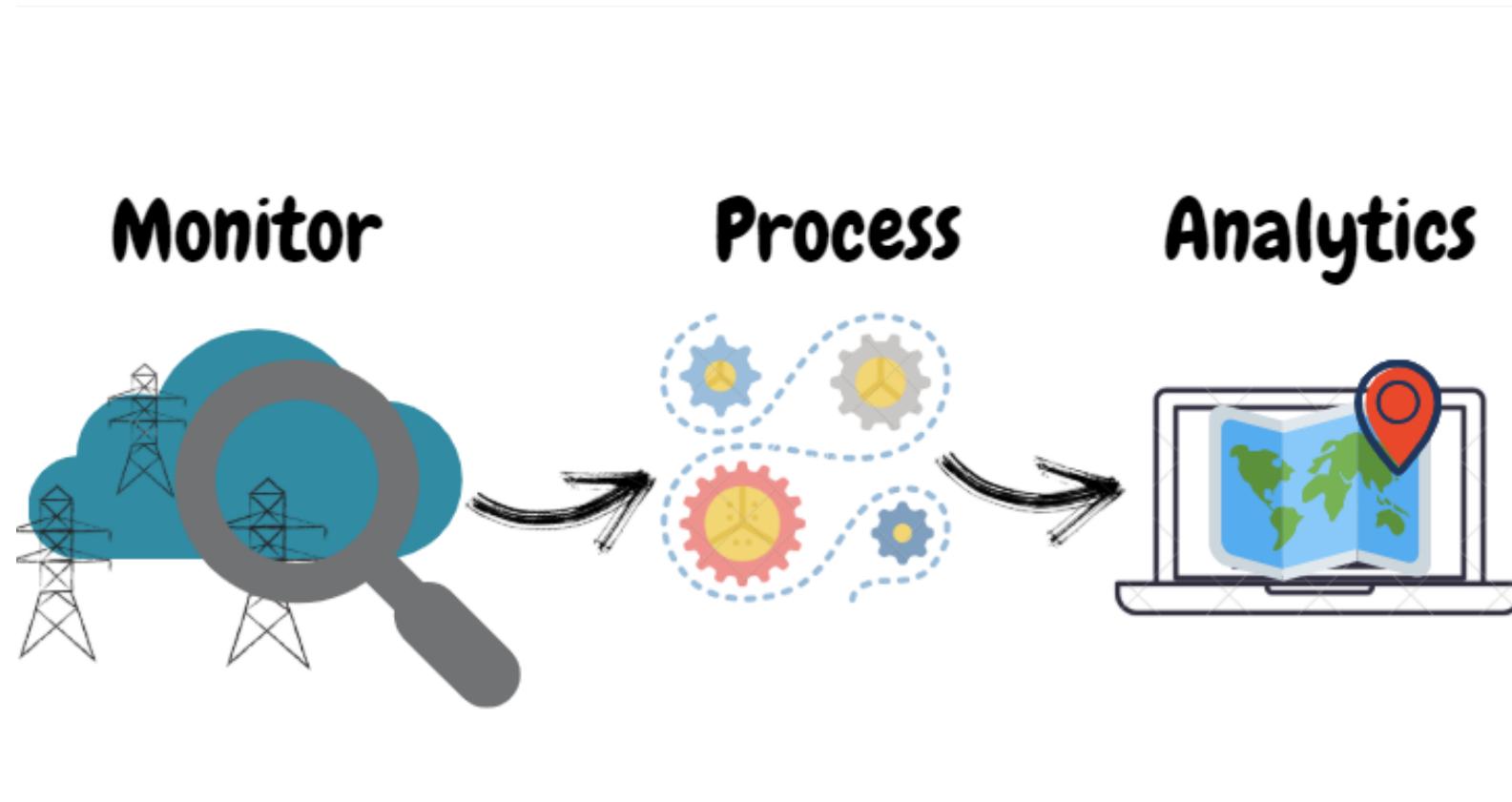


Not Yet Motivated ..

SCADA Architecture



Methodology



Alerts and Intrusions Attempts

5,300,000

Scanning Activities

61,000

Unique IP Count

80,000

Cyber Activity

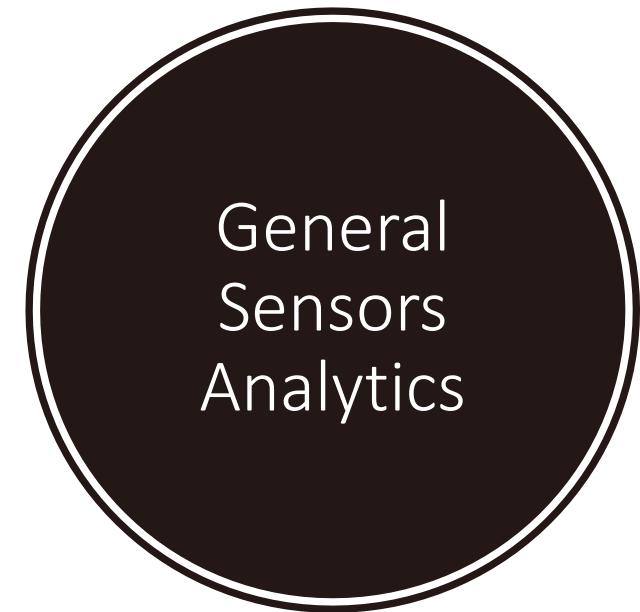
260,000

0

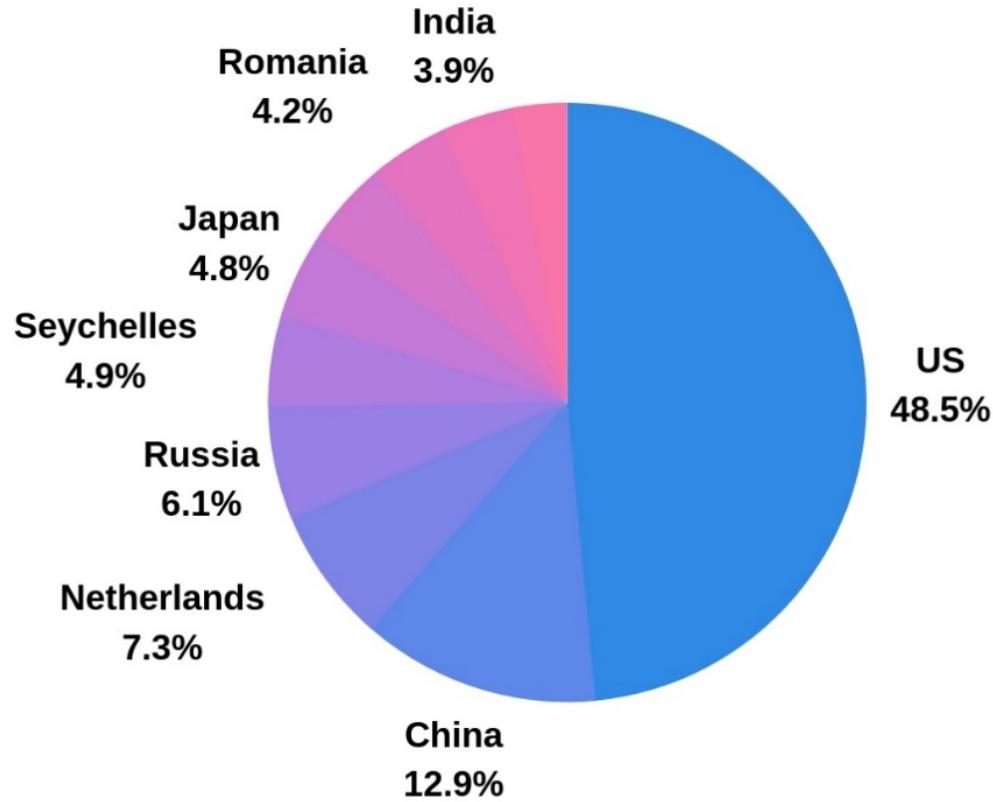
2,000,000

4,000,000

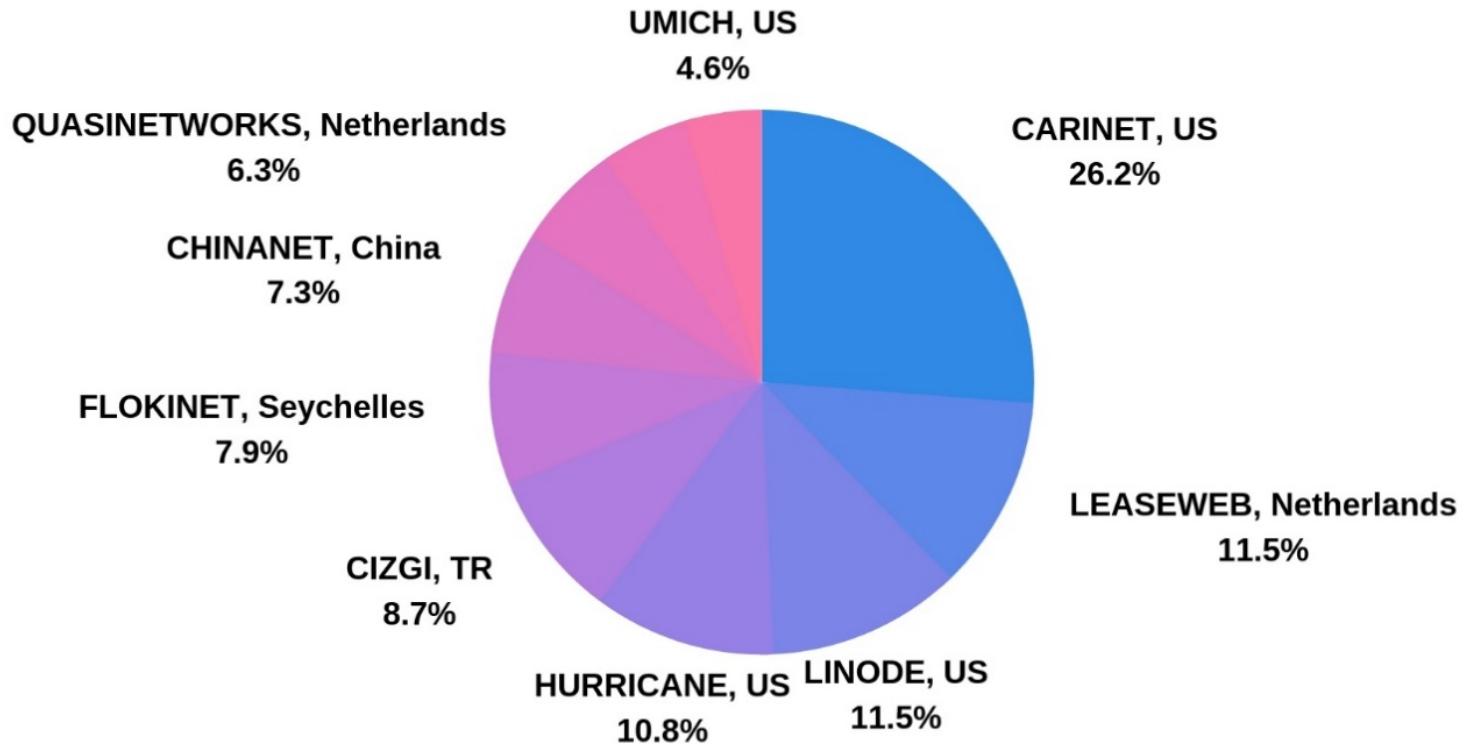
6,000,000



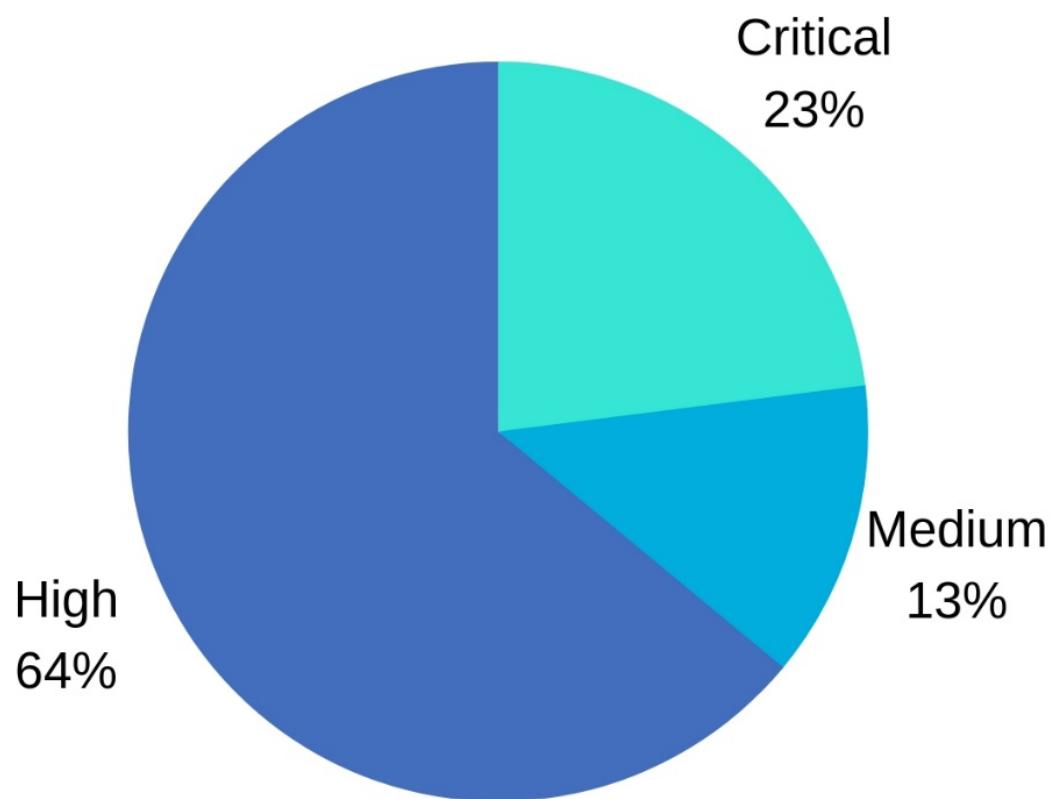
SCADA Sensors Analytics Top Countries

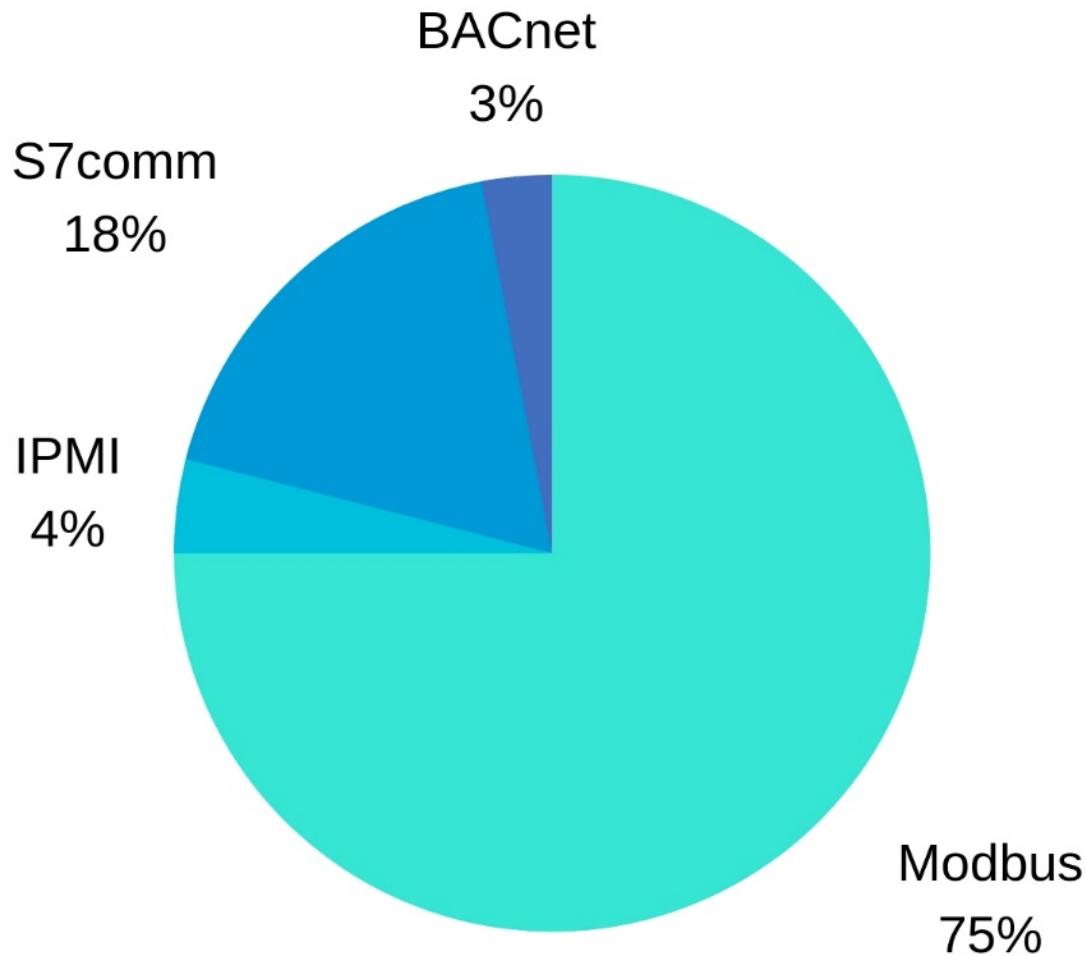
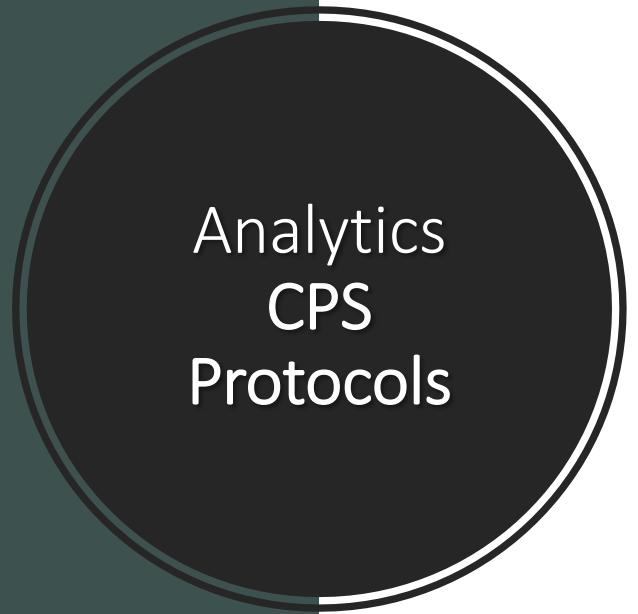


SCADA Sensors Analytics Top AS



Analytics Severity level





Analytics – Threat Classification



66.6% of malicious activities were **e-mail attacks**

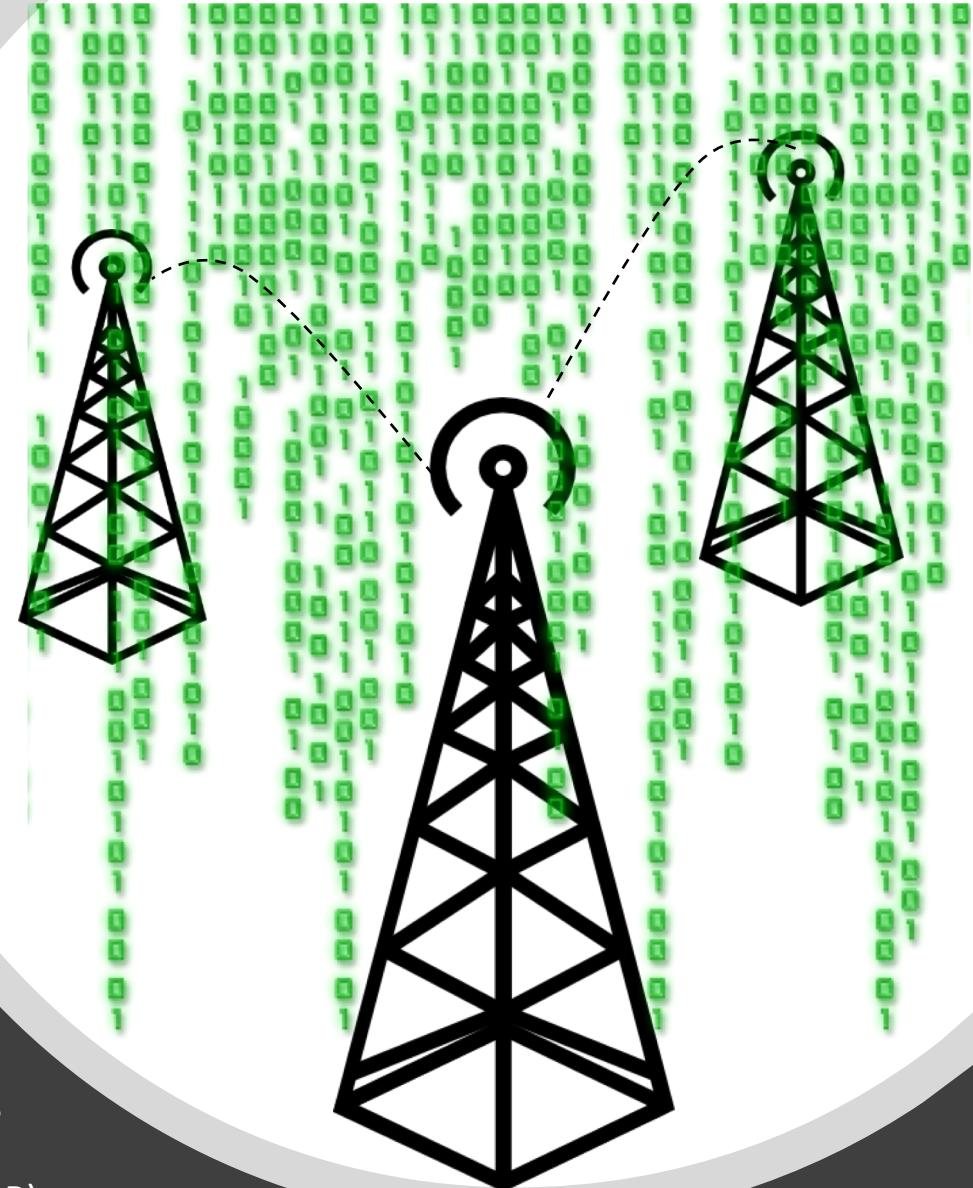


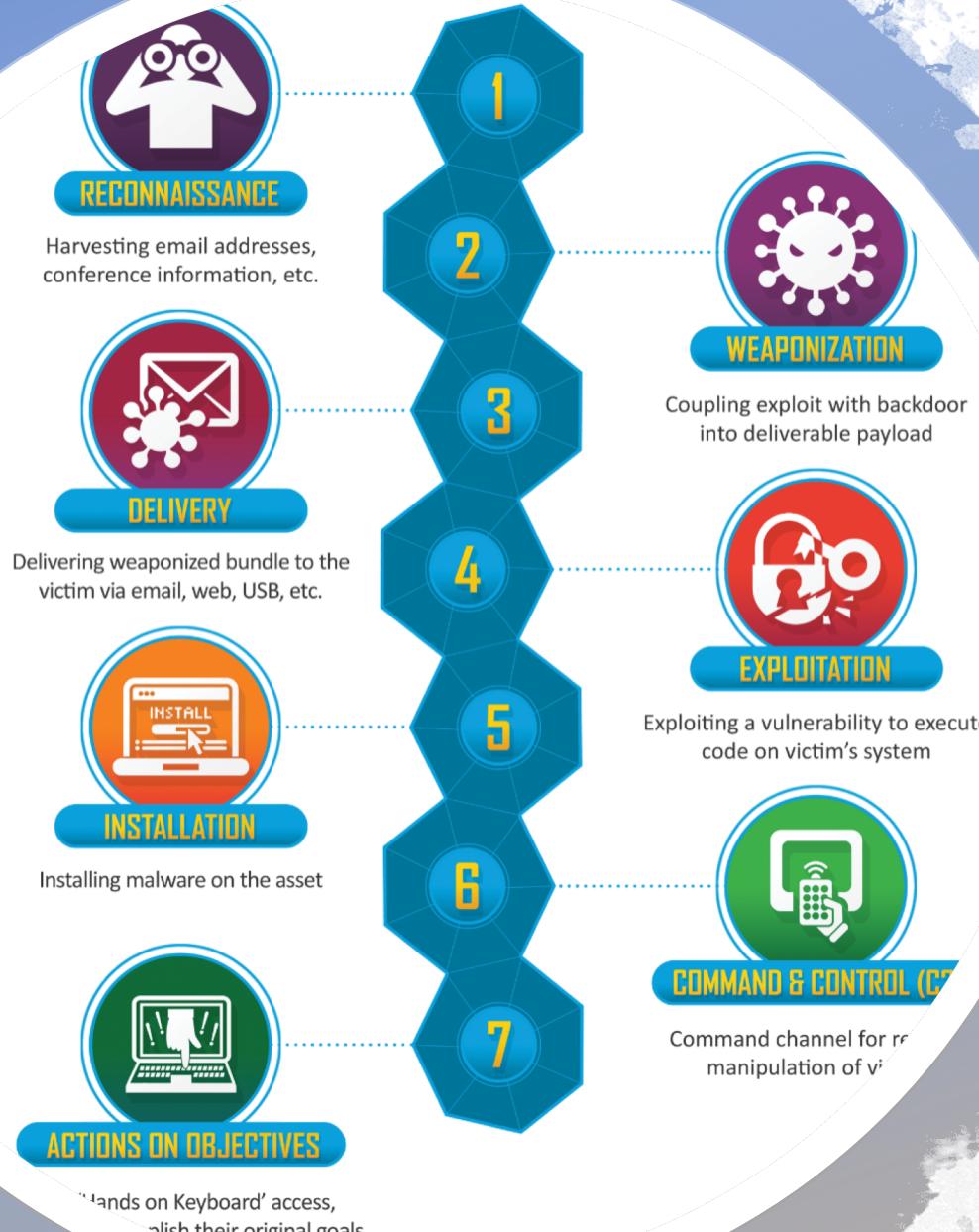
50% of the following types:

- WEB attacks, Internet Message Access Protocol (IMAP) attacks
- Secure Shell (SSH) attacks
- File Transfer Protocol (FTP) attacks

16.6% of scanning activities

- Domain Name Service (DNS) attacks
- Password disclosure attempts
- Telnet scans
- Remote Desktop Protocol (RDP) scans





Secure CPS at each stage in cyber kill chain