ADAPTIVE CYBER DEFENCE

DIRP 2016-21 : Adaptive Cyber Defence

Designing Secure Complex Critical Public infrastructure
by Prof. Aditya Mathur

Application of SDN to Cyber Defence
By Prof. David Yau

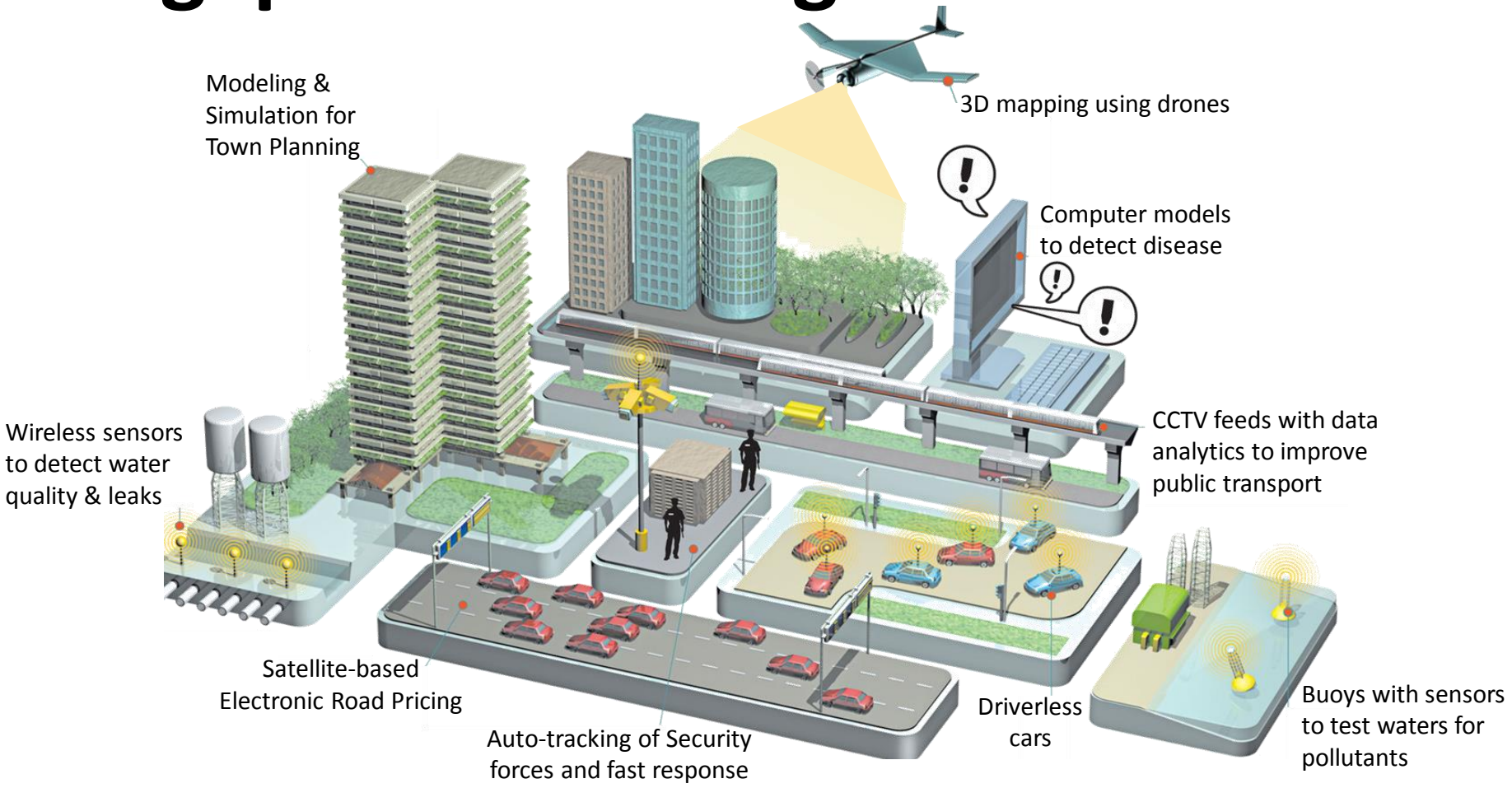
Adaptive Cyber Defence
by Mr. Chua Peng Huat
Mr. Leon Cheng,
Ms. Ang Hui Kuan

Question-and-Answer

Overview

Mr. Chua Peng Huat
Assistant Director (Cyber), FSTD

Singapore - Building a Smart Nation



Singapore will need to step up its efforts in defending the nation against cyber attacks, which extend beyond borders and threaten daily life of ever more connected global citizens.

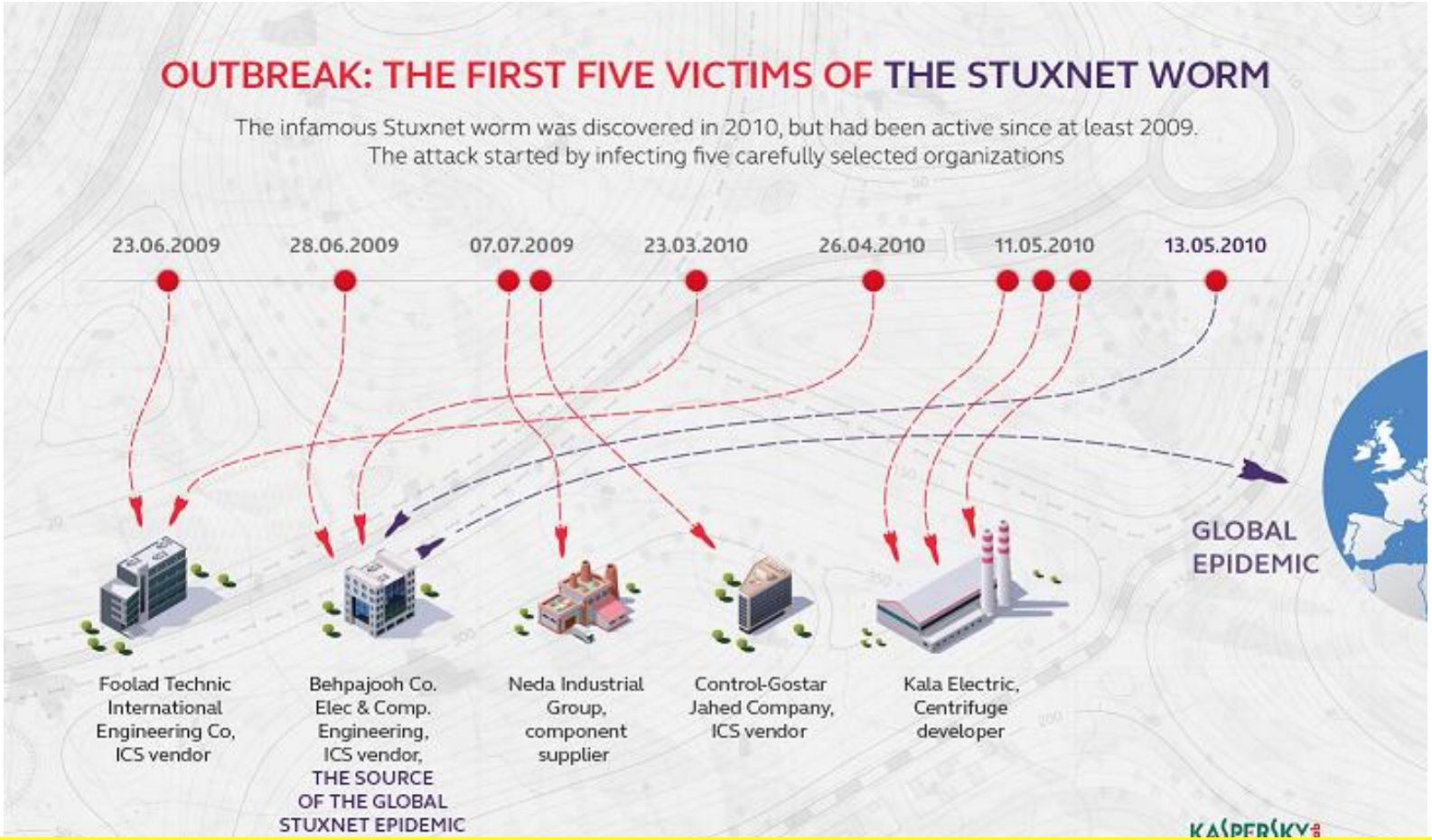
Cyber Physical Systems (CPS)

CPS used in critical infrastructures

Attacks have adverse consequences

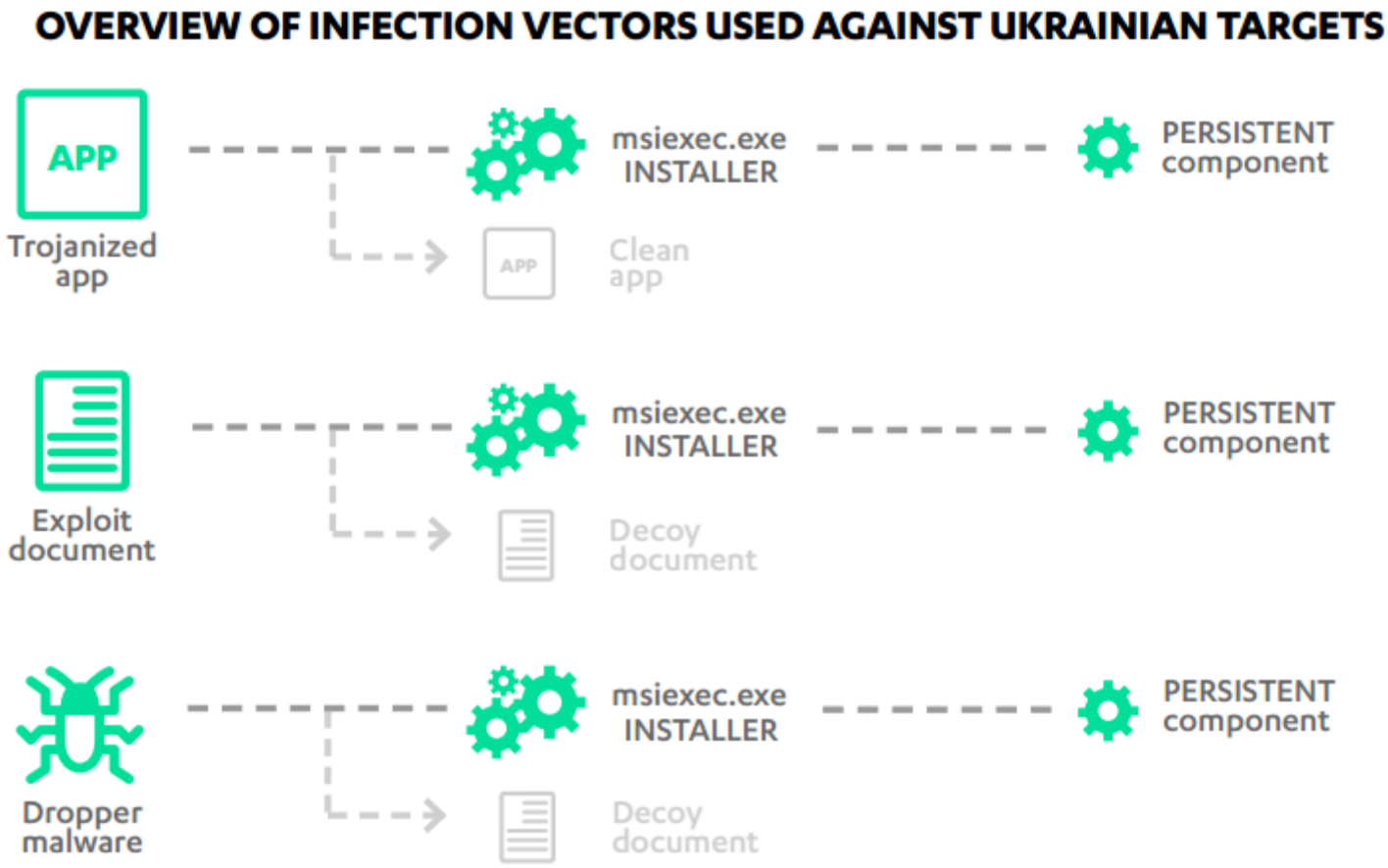
Contemporary malware expanded scope from conventional cyberspace to physical space by attacking CPS

Stuxnet Worm



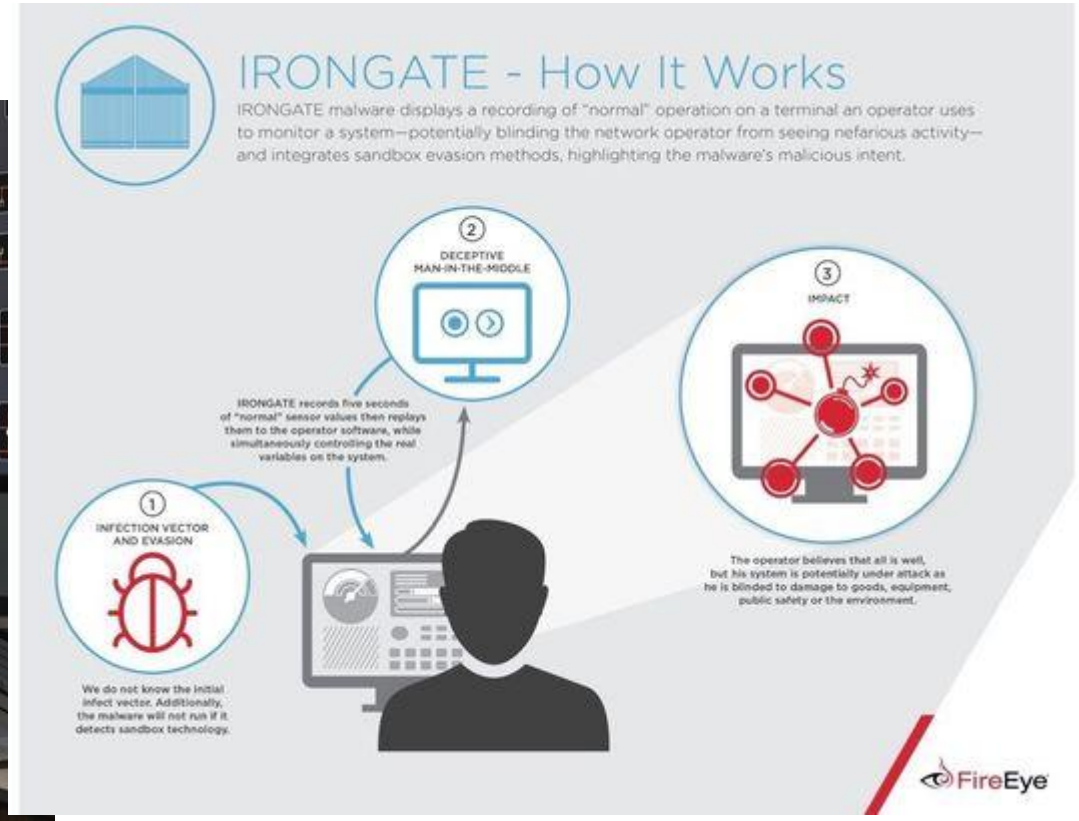
- Malicious computer worm to target Iran's nuclear plant
- Targets Programmable Logic Controllers
- Exploit four zero-day flaws by targeting Microsoft Windows and Siemens Step 7 software
- Infected by USB flash drive

BlackEnergy Malware



- Malicious trojan to target Ukrainian power grid
- Destructive plugin called KillDisk to overwrite > 4000 file types with random data and damage the operating system

Irongate Malware



- Man-in-the-middle attack
- Affects simulated Siemens computing control environment
- Record normal traffic to a PLC and play back to an HMI

Cyber Defence R&T Challenges

- Persistence of threats
- Stealth, low signature threats
- Polymorphic malwares
- Fast evolving threats

Technology Gaps

- Security as a design priority right in the Design Thinking stage of building a system
- Current detection are signature based => Need for non-signature based detections
- Current Defence systems are reactive => Need for Proactive Responsive Cyber Defence Architectures
- Self-healing systems with automated software repairs

DIRP 2016-21 : Adaptive Cyber Physical Systems (CPS)

We are soliciting innovative research proposals in the area of adaptive Cyber Physical Systems (CPS). CPS are systems of collaborative computational elements controlling a physical process, such as smart grid, autonomous vehicle networks, etc. The goal is to realize context-aware CPS that are self-configured, self-optimized and self-healed with minimal human intervention. To be resilient against cyber attacks, it is desirable to adopt a multi-disciplinary approach spanning areas such as game theory, cognitive science/psychology and deep learning.