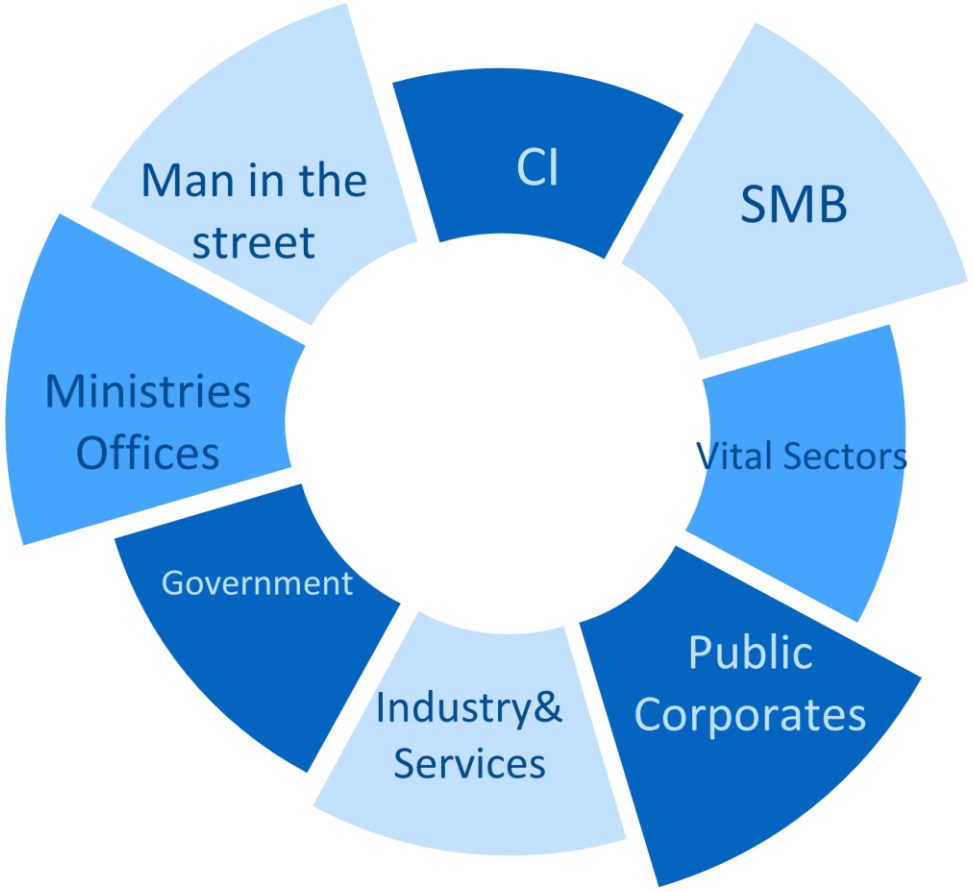
Cyber Israel
National Cyber Directorate

ICS – Industrial Cyber Scanning, The hidden world of industrial components

Itay Bochner

»»» CYBER Israel - Timeline

»»» INCD's Responsibility

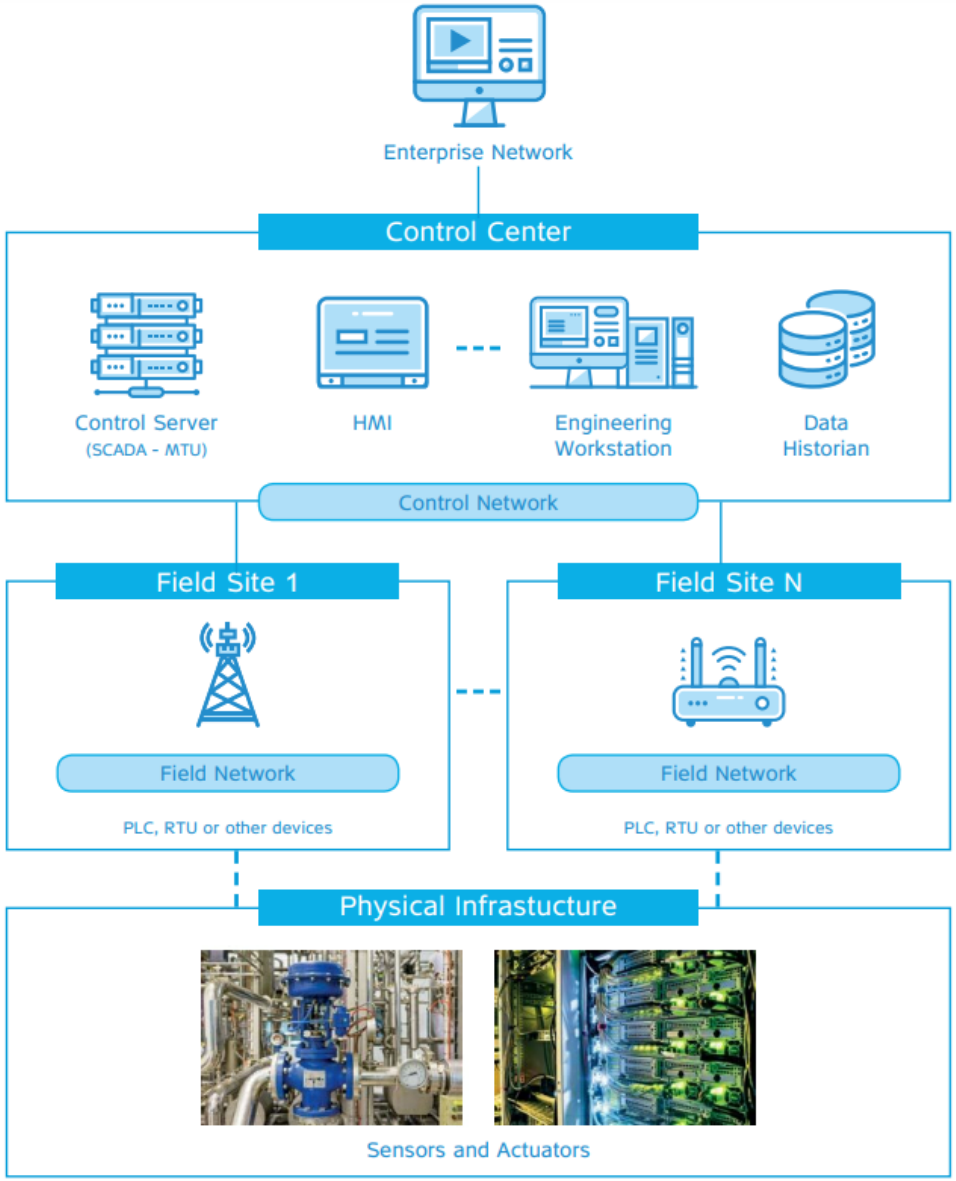


Out Of Scope

Cyber Israel
National Cyber Directorate

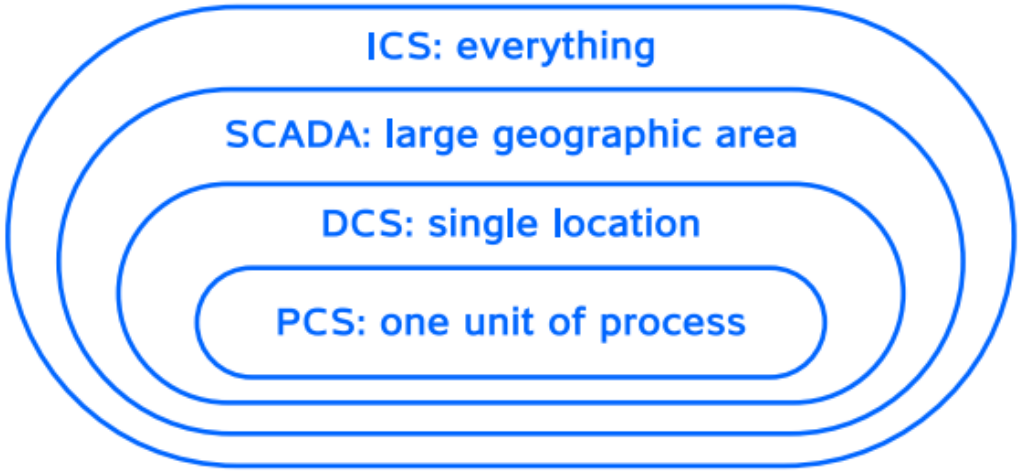
»»» ICS in a nutshell

- ICS - Industrial Control System
  - An automation control system that is used in energy, oil and gas, water, power, etc.
  - Control industrial processes locally or at remote locations
  - Monitor, gather, and process real-time data
  - Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software



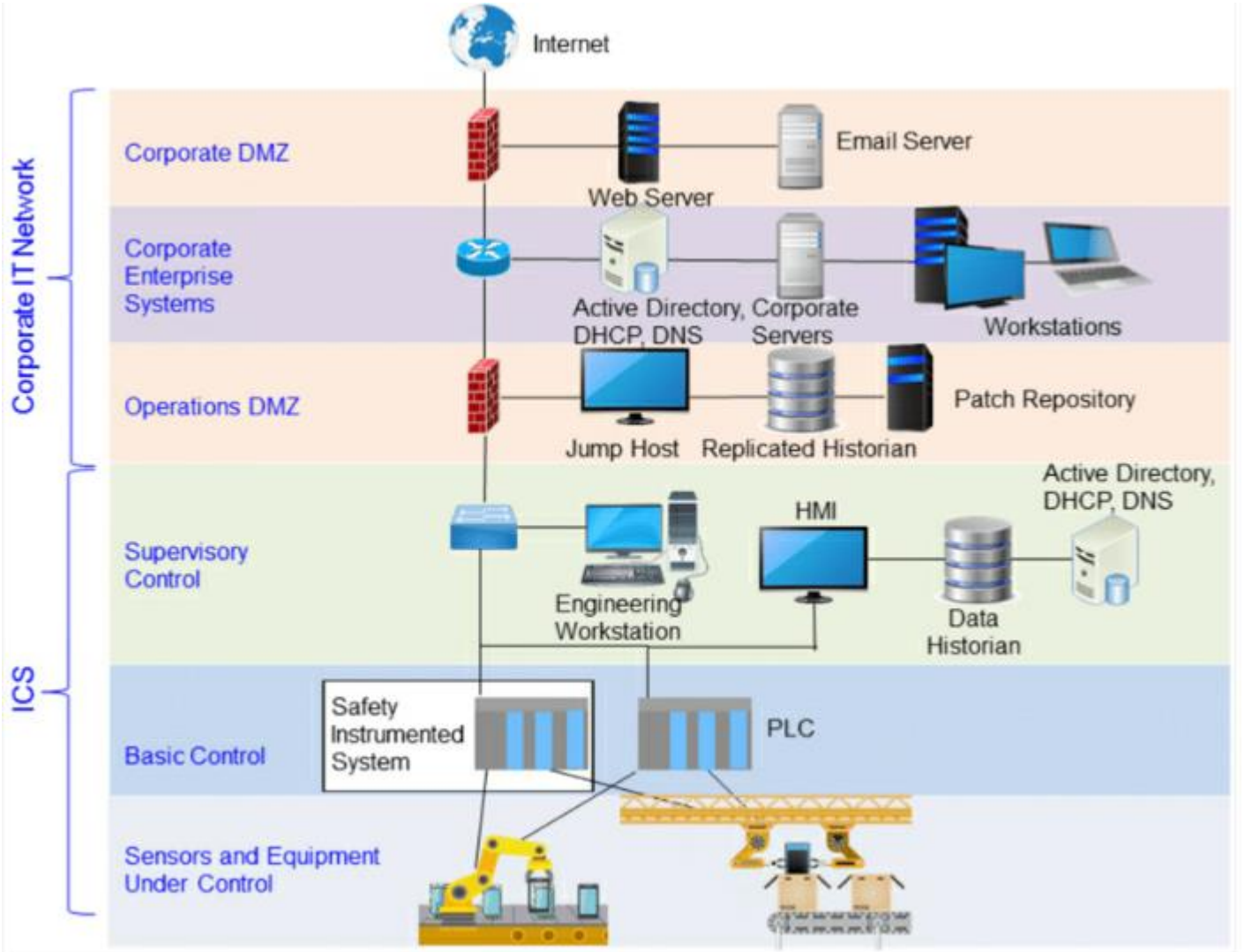
»»» ICS in a nutshell

- Main components
  - SCADA – Supervisory Control And Data Acquisition
  - DCS – Distributed Control System
  - PLC - Programmable Logic Controller
  - RTU – Remote Terminal Unit
  - HMI – Human Machine Interface
  - ES – Engineering station



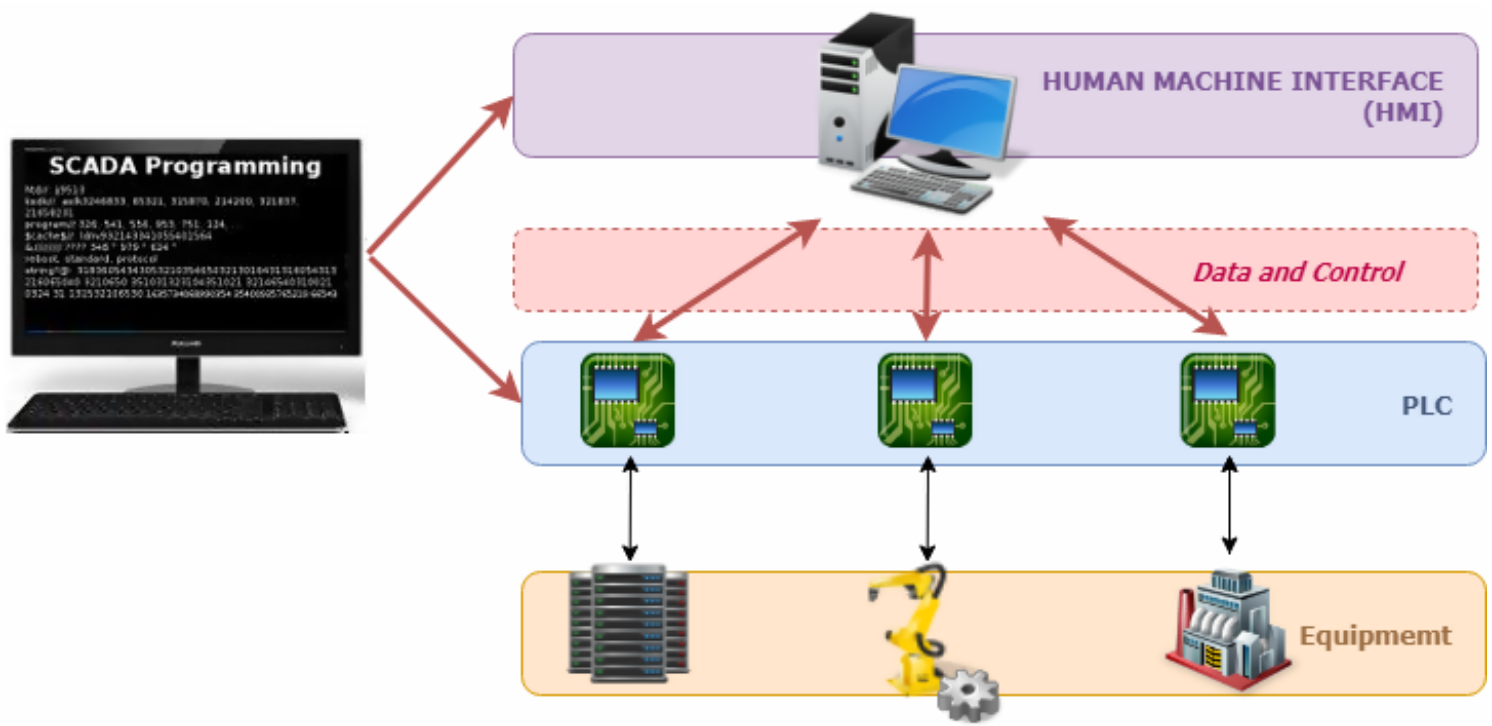
»»» ICS in a nutshell

- How PLC works
  - Cyclic Polling
    - Input – sensors
    - Output - actuators
  - Close to real time ~ 40ms/cycle
  - Embedded logic
    - Ladder diagram
    - Function blocks
  - Process vs. management communication
  - Proprietary protocols and software
    - Modbus/TCP
    - Modbus/RTU
    - S7
    - GESRTP
    - ProfiBus
    - ProfiNet
    - EtherNet/IP



Notional ICS and corporate IT network architecture

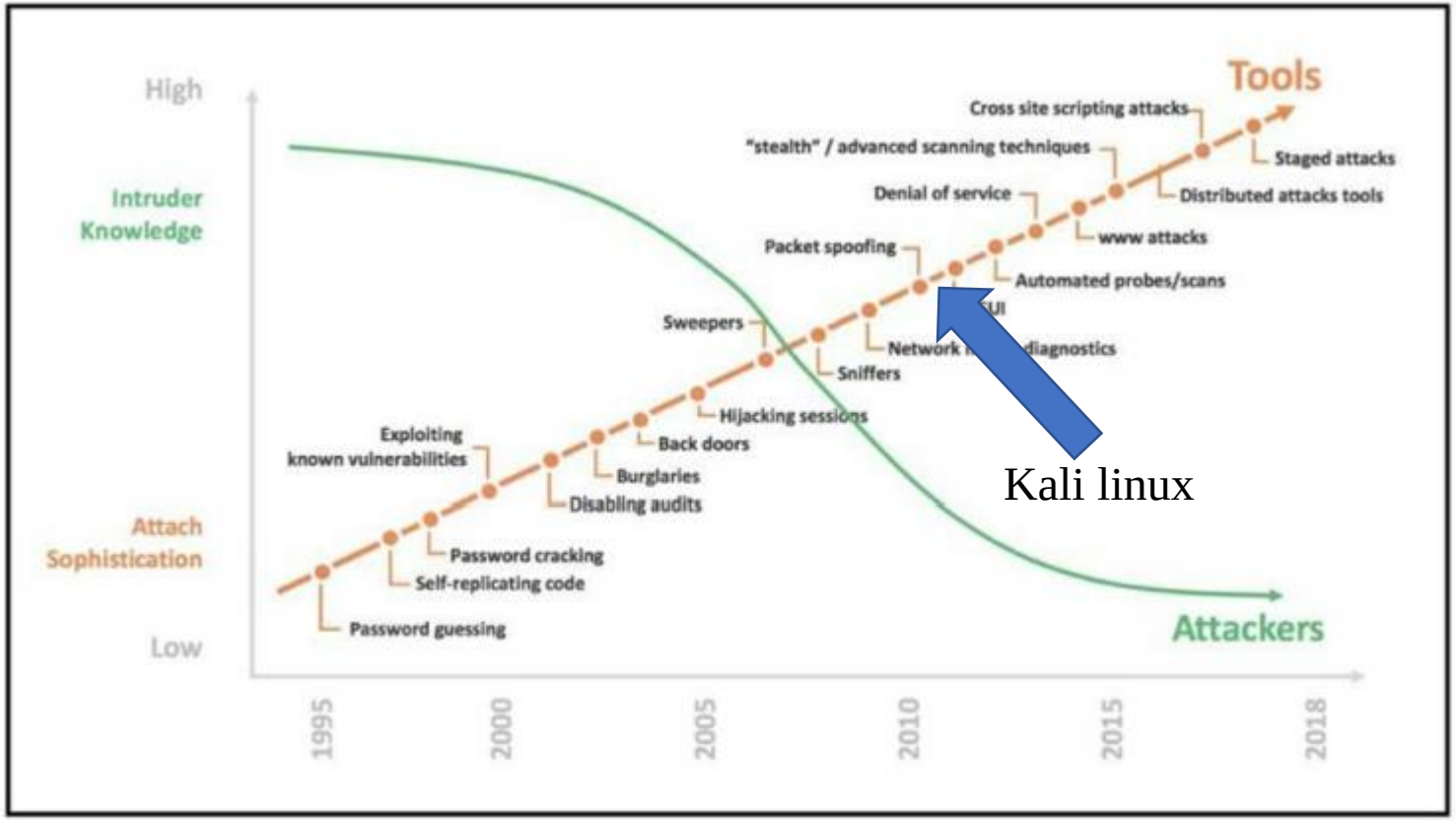
»»» Scada routine



Purdue Model for Control Hierarchy logical framework

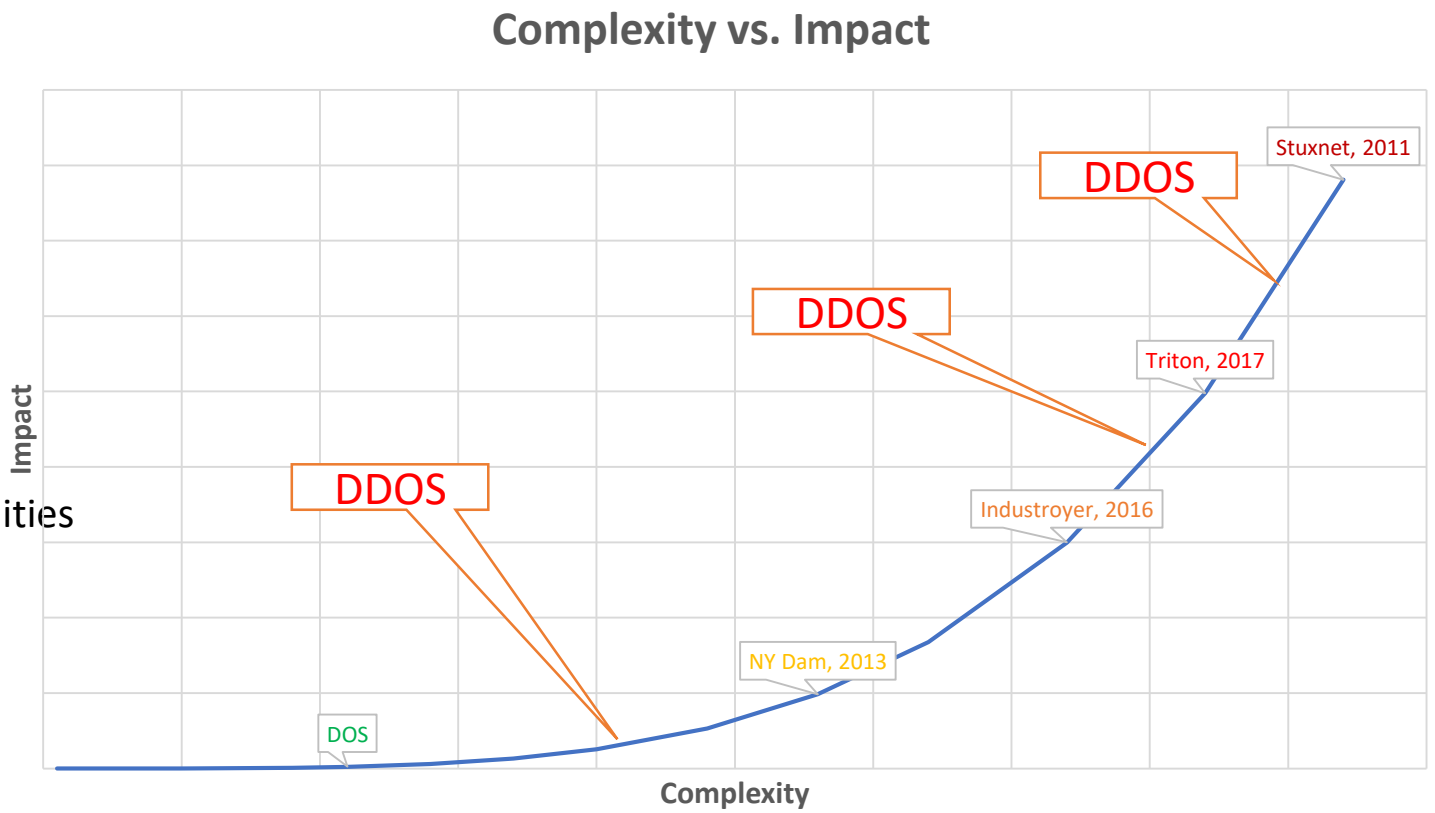
»»» Attack landscape

- Attacker skills and toolkits
- Attack purpose
  - Immediate vs. overtime damage
  - Physical or disinformation campaign
- How many targets?
  - 1 major target
  - Critical mass



National concern

- Known attacks
- The problem?
  - Exposed devices
  - Opportunistic attackers
  - Distributed attack
- Risk management
  - CI – Critical Infrastructure
  - Big & Small/Medium industrial facilities
  - Cyber Resilience prioritization
  - Influential campaign



»»» Needle in a haystack

- Queries & parsing
  - Mix & match
  - Telltale signs
  - Validity of the scan
  - Legacy components
- Challenges of scanning
  - PLCs attribution
  - Scan parameters?
  - Vendor variance
  - Legal limitation
  - No benchmark for scanning

[redacted].175
Cellcom/Netvision
Added on 2020-06-06 19:44:11 GMT
Israel, Haifa
ics

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

[redacted].20
[redacted]cc.net.il
Triple C Cloud Computing Ltd.
Added on 2020-06-07 02:54:47 GMT
Israel, Lod
ics

Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 2
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illeg...

[redacted].191
[redacted].orange.net.il
[redacted]91.orange.net.il
Partner Communications
Added on 2020-06-06 05:58:42 GMT
Israel, Tel Aviv
ics

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

[redacted].242
Cellcom Group
Added on 2020-06-07 05:23:45 GMT
Israel, Tel Aviv
ics

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

»»» Raising up the guards

- Day2day cyber resilience
  - Remote connections
  - Awareness
  - Supply chain
  - DRP

https://www.gov.il/BlobFolder/generalpage/icssolutions/he/ICS_eng.pdf

»»» Q&A

Thanks you…

itayb@cyber.gov.il