RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M03

900 MILLION WARNING SIGNS
THE GROWING THREATS TO INDUSTRIAL NETWORKS

Galina Antova

Co-Founder
Claroty
@GalinaAntova

where were you on

JUNE 27th 2017

NotPetya brings down operations

You don’t have to be the *target* to be a *victim*

You don’t have to be the target to be a victim

- Acknowledge your **blind spot**
- Recognize your **strategic importance**
- Implement several **practical suggestions**

How many hands?

How do you protect a network that is invisible?

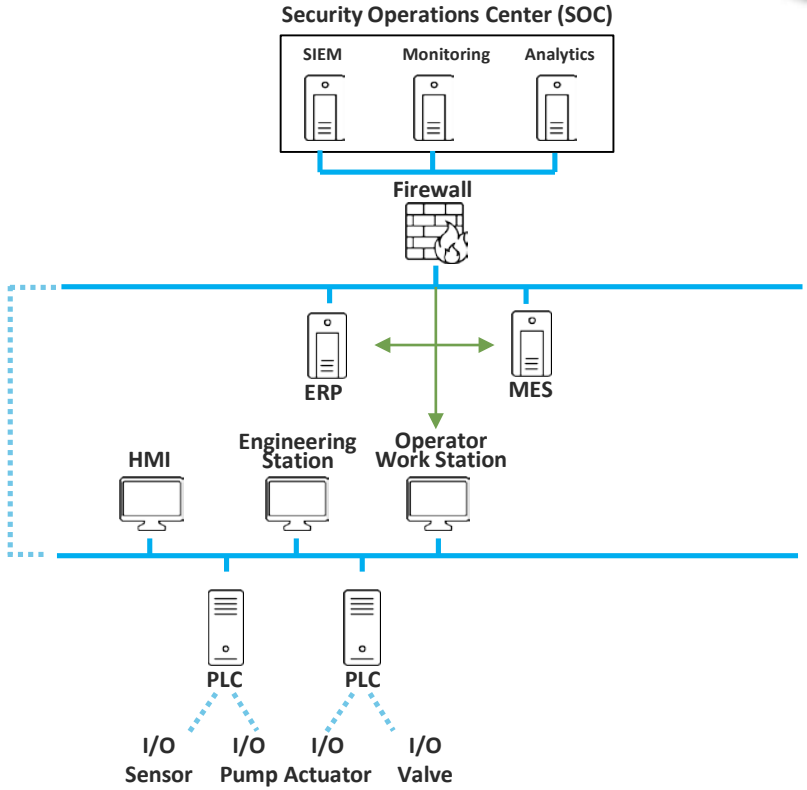
Level 4: Enterprise Zone (IT Domain)

Level 3: Operations & Control

Level 2: Supervisory Control DCS/SCADA

Level 1: Basic Control

Level 0: Process Device I/O



The world's infrastructure runs on
Operational Technology networks

The world's infrastructure runs on OT networks

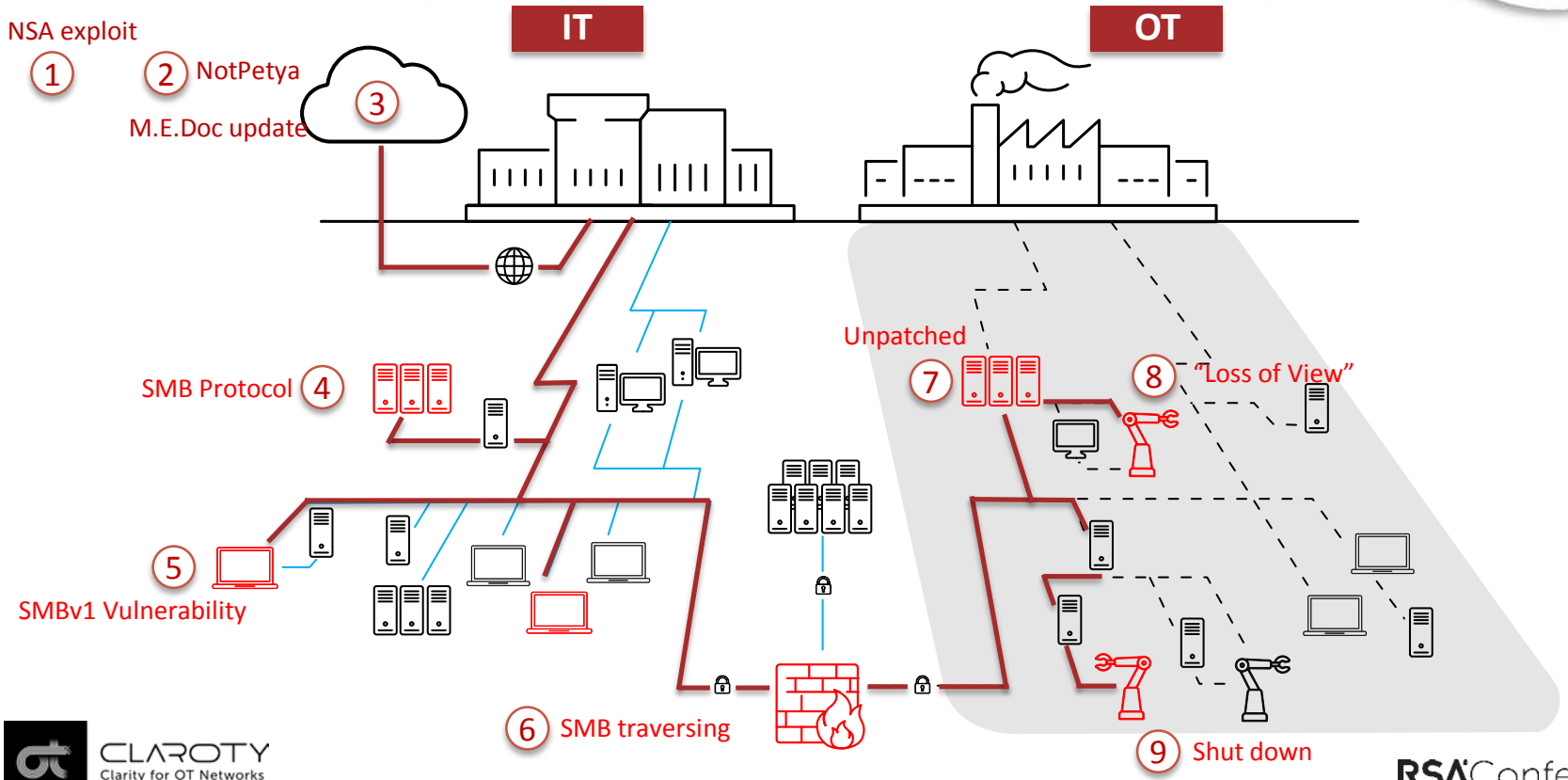
The world's infrastructure runs on OT networks







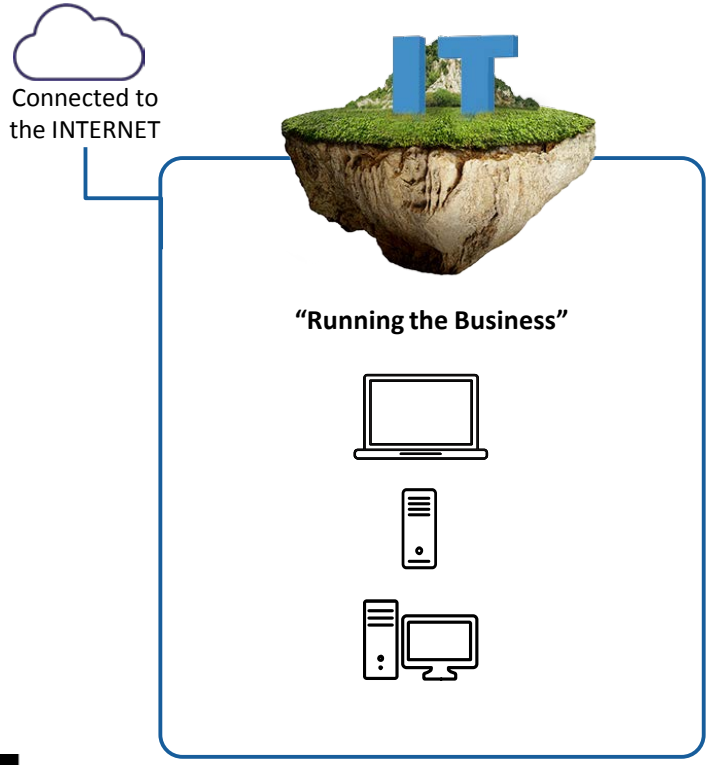

Why is NotPetya important?

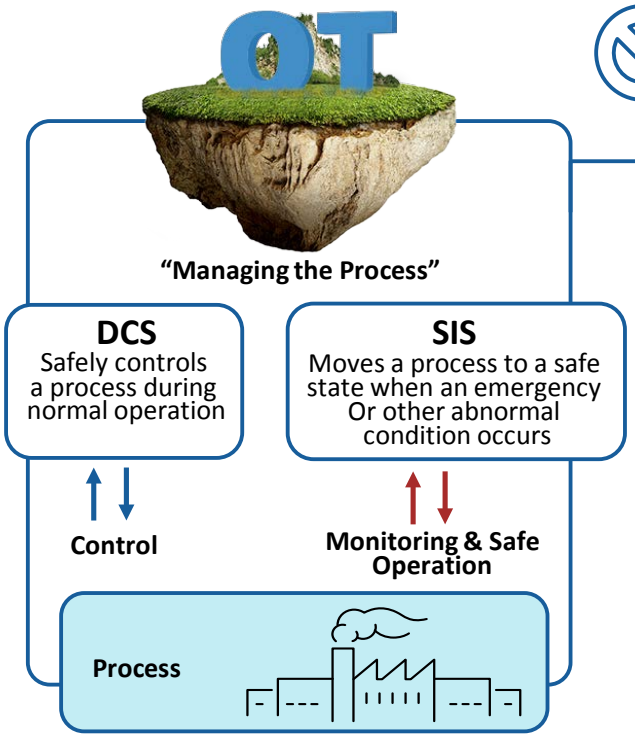


CLAROTY
Clarity for OT Networks

The most destructive and costly attack in history

An ideal world scenario – “Individual Islands”



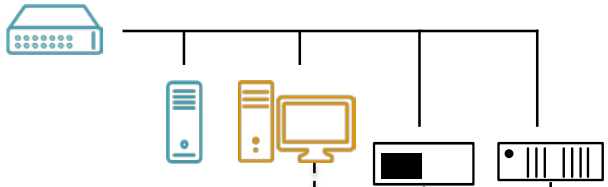


What happens in the real world – Triton

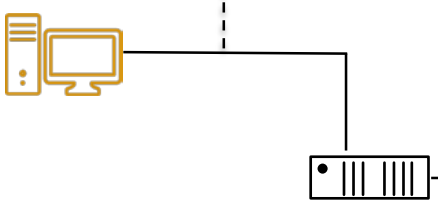
IT

DCS:

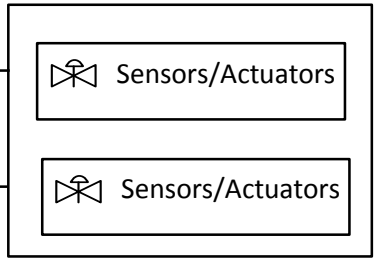
DCS components



SIS:



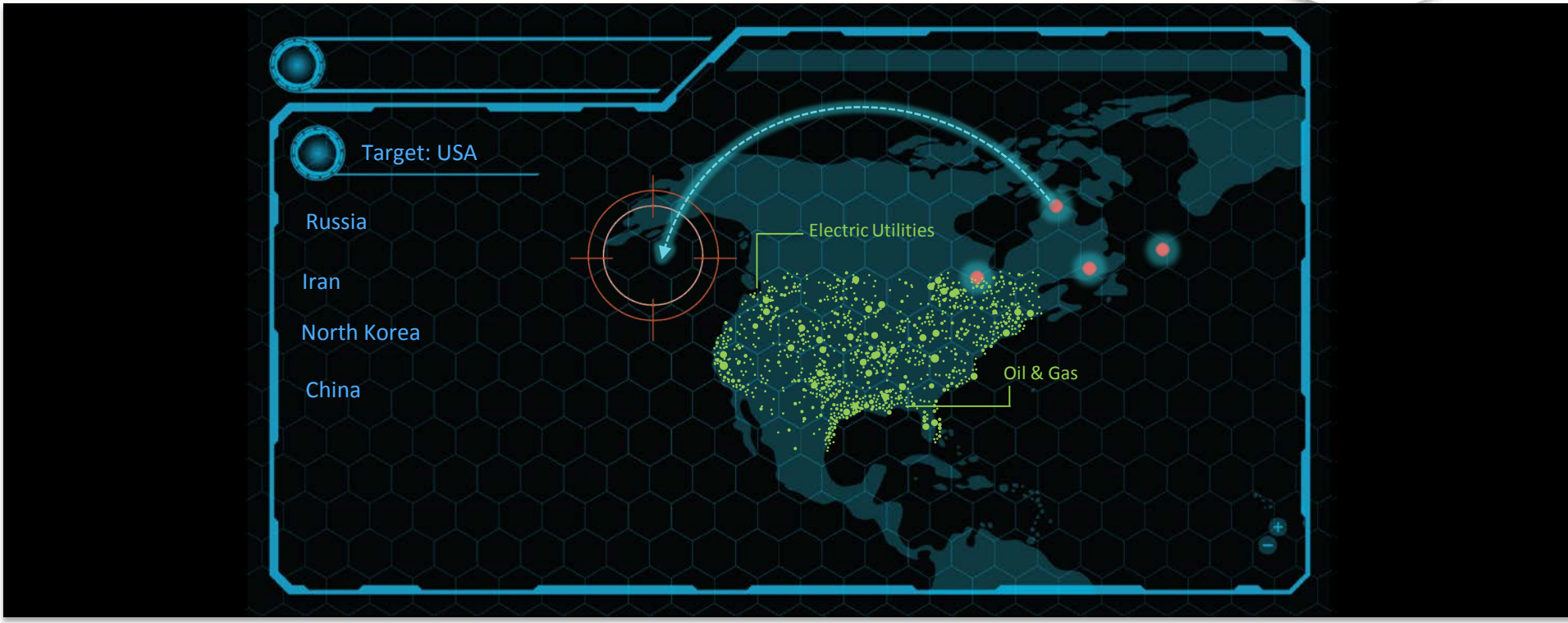
Physical Process



SIS controllers

https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

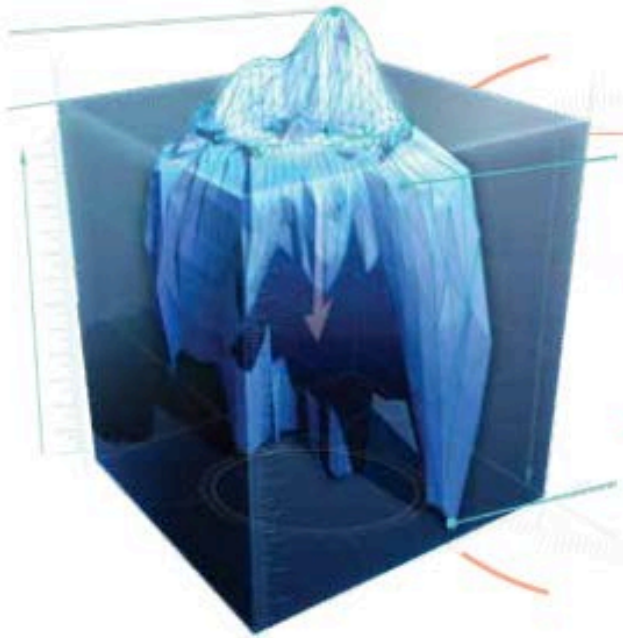
Economic warfare: the likely scenario



Cyber warfare does not give us the “luxury” of mutual assured destruction

USCYBERCOM - March 23rd

Strategic Vision: Achieve and Maintain Cyberspace Superiority



ADVERSARIES **OPERATE CONTINUOUSLY BELOW THE THRESHOLD OF ARMED CONFLICT** TO WEAKEN OUR INSTITUTIONS AND **GAIN STRATEGIC ADVANTAGES.**

How to apply what we discussed?

What you can do immediately …

- **Acknowledge** the reality
  - Your organization has OT networks and they are essential to operations
  - Those networks are invisible to your security team and traditional IT cybersecurity solutions don't work in OT networks
  - Those networks carry strategic importance to the adversary
- **Ask** the tough questions
  - Who has the responsibility and accountability to monitor / protect those networks?
  - Have you done a risk assessment of those networks?
- **Acknowledge** your blind spot
  - The absence of evidence is *not the same* as evidence of absence
  - Discover how large your blind spot is and quantify the implications

How to apply what we discussed?

What you can do in the next few months …

- **Cover** the basics, again
  - How good is your segmentation between the IT and OT Networks?
  - Know the risks to your OT networks, even if you cannot address them short-term
- **Make** your OT networks visible
  - Adopt technologies that provide visibility into all Levels of the OT networks, down to serial / fieldbus connectivity
  - Incorporate that visibility and OT-specific threat detection into your IT SOC
- **Expand** all your IR and governance to include OT networks
- **Educate** your executives and Board on the impact of potential breach

Questions?

Galina Antova
galina@claroty.com
@GalinaAntova