Ciências
ULisboa

Utopia or Reality?

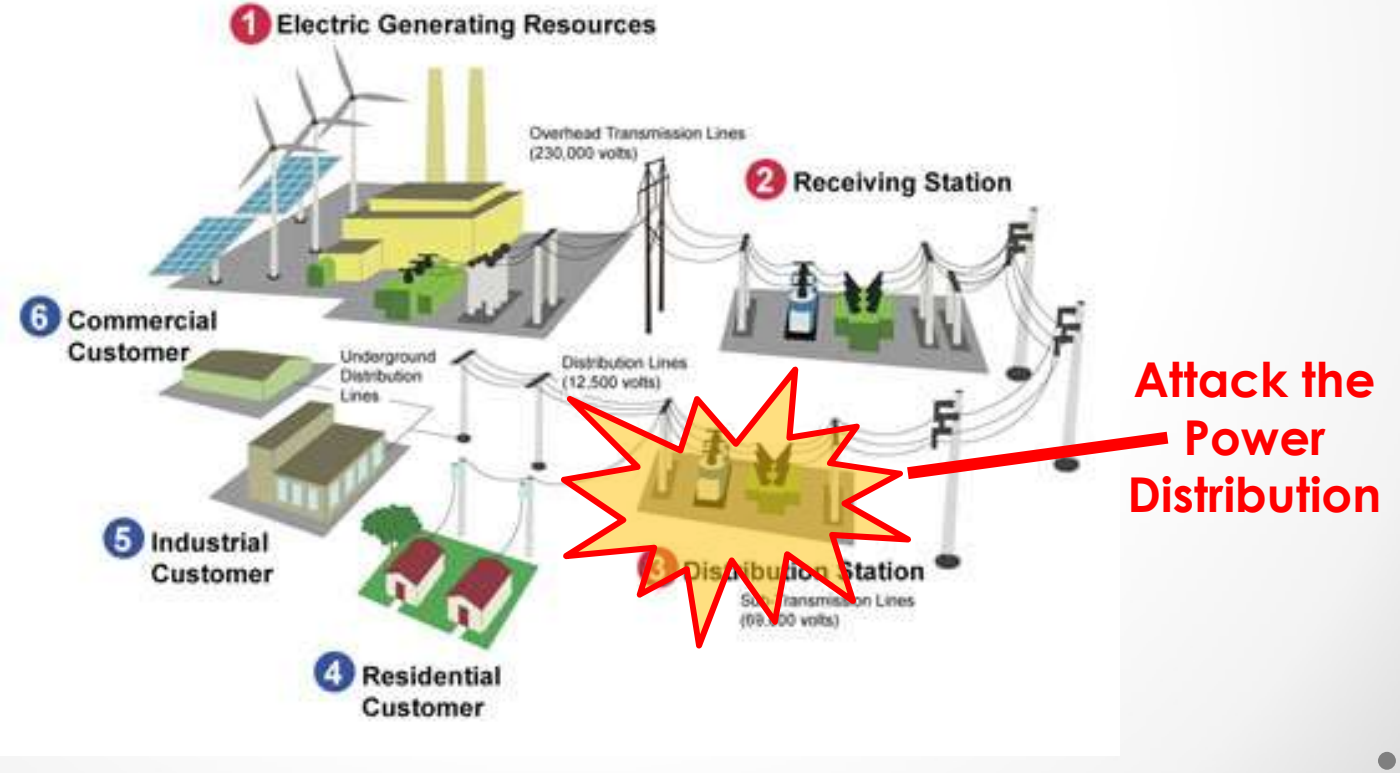
An Attack Scenario for a Power Grid

Nuno Ferreira Neves

Universidade de Lisboa
Faculdade de Ciências, Dept. Informática
nuno@di.fc.ul.pt

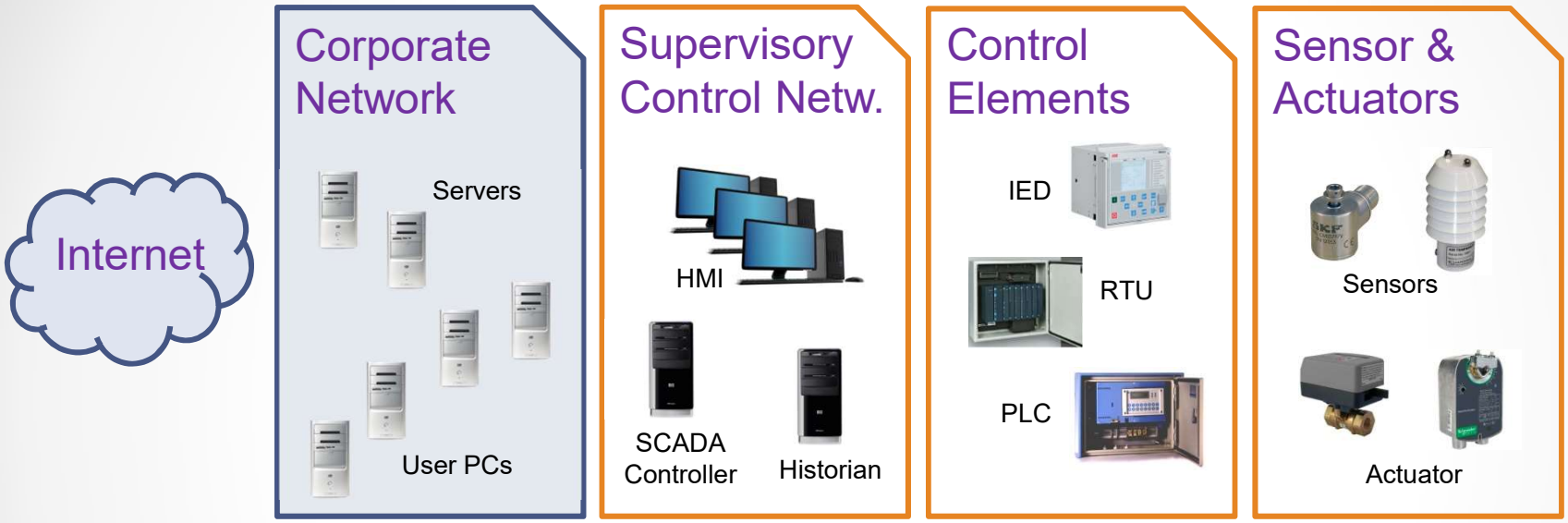
Objective

- Disrupt the power grid operation at the distribution level, preventing access to electricity for the longest period of time
  - perform a coordinated attack to several DSOs
  - limit the capability to recover from the attack

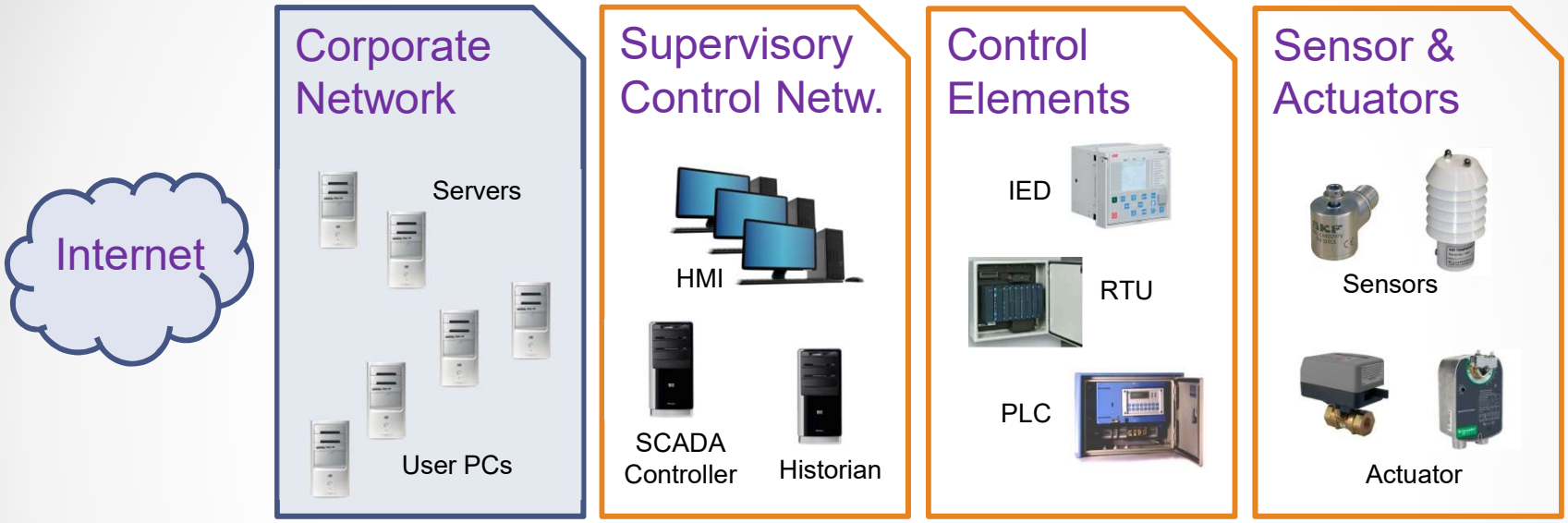


Ciências ULisboa

Stage 1: Intrusion

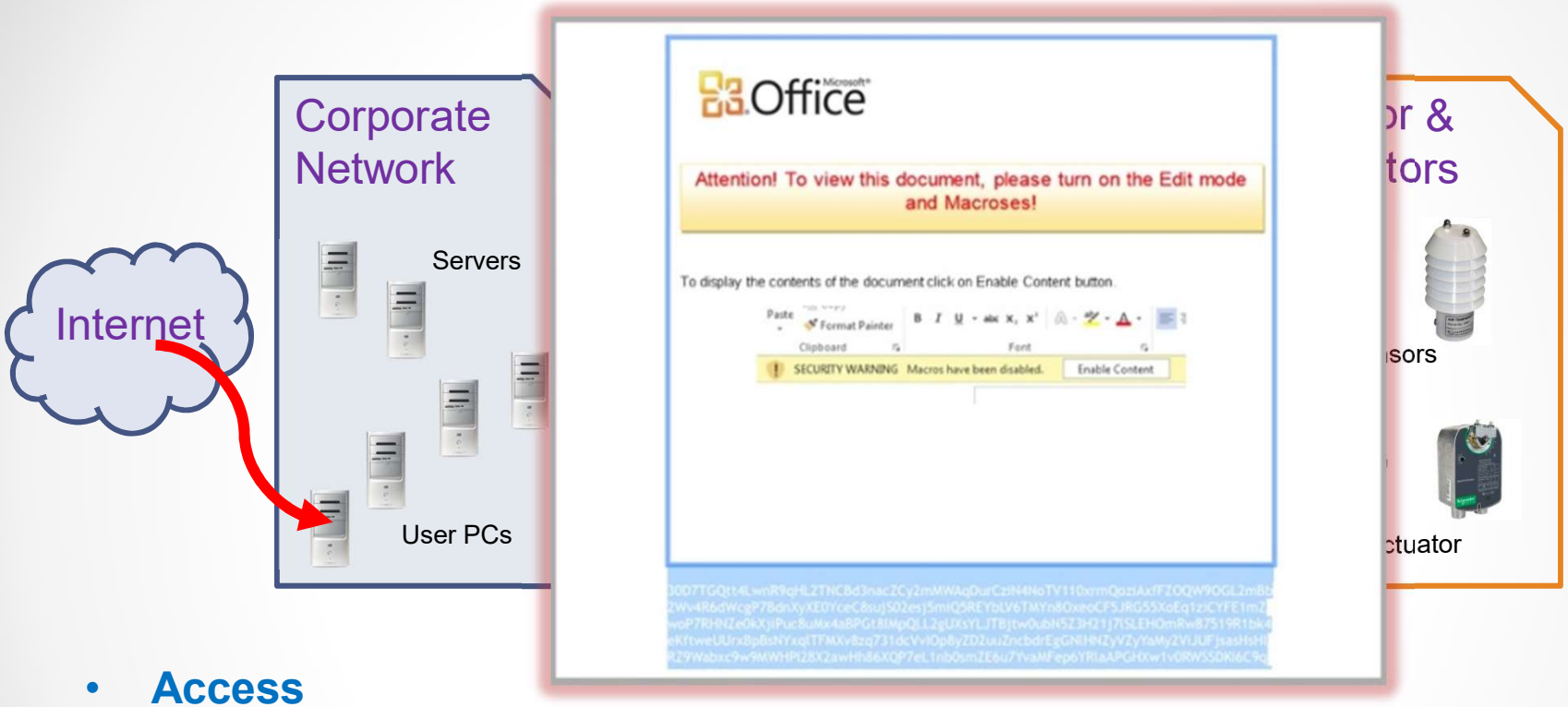


Stage 1: Intrusion



- **Reconnaissance**
  - collect diverse public information about
    - people and the internal organization of the DSO
    - control systems and other elements that are in use

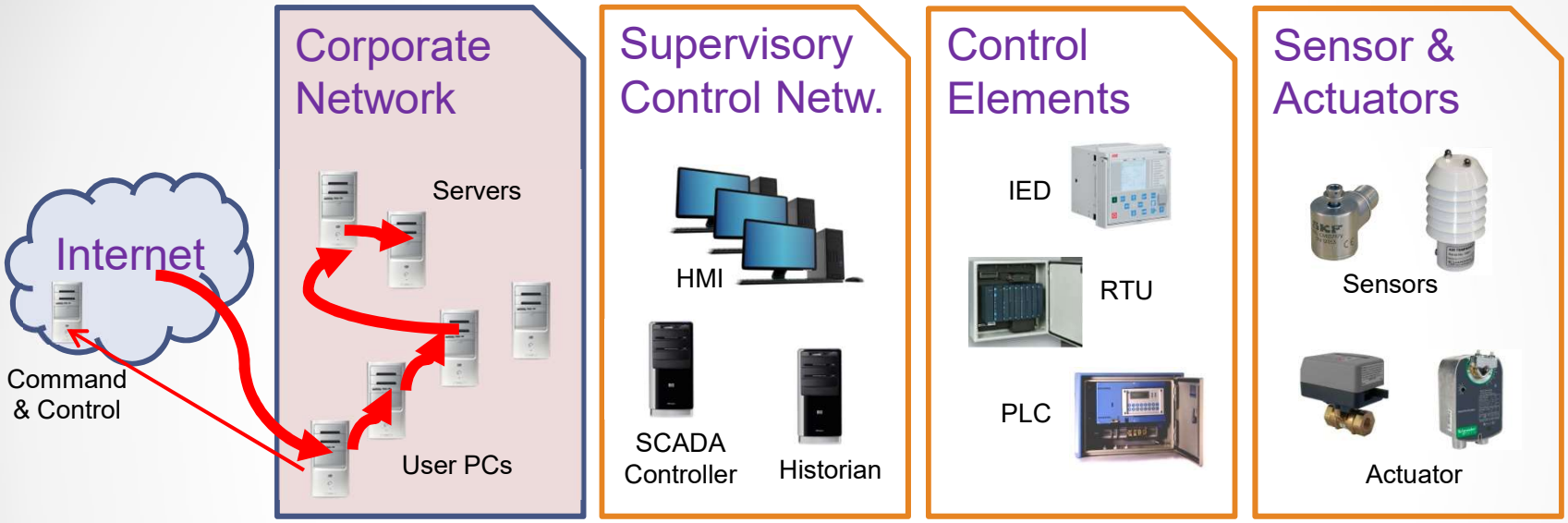
Stage 1: Intrusion



- **Access**
  - email campaign to the DSO employees containing Microsoft Office documents
    - malicious macros are included in Excel/Word
    - expectation that users enable the use of macros

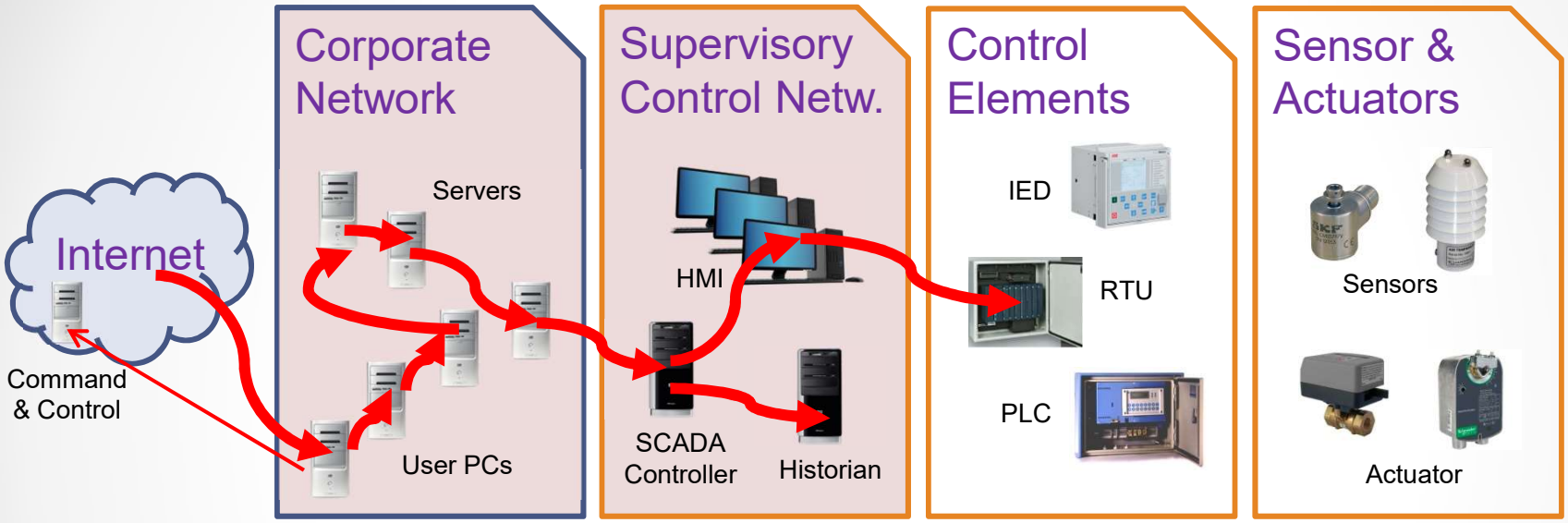
Ciências ULisboa

Stage 1: Intrusion



- **Exploit, Escalate and Ensure Persistent Access**
  - when the macros are enabled, the BlackEnergy malware is installed
  - malware connects to command & control machines, enabling remote control
  - credentials are harvested, privileges are escalated, and further machines are compromised allowing persistent access to the corporate network

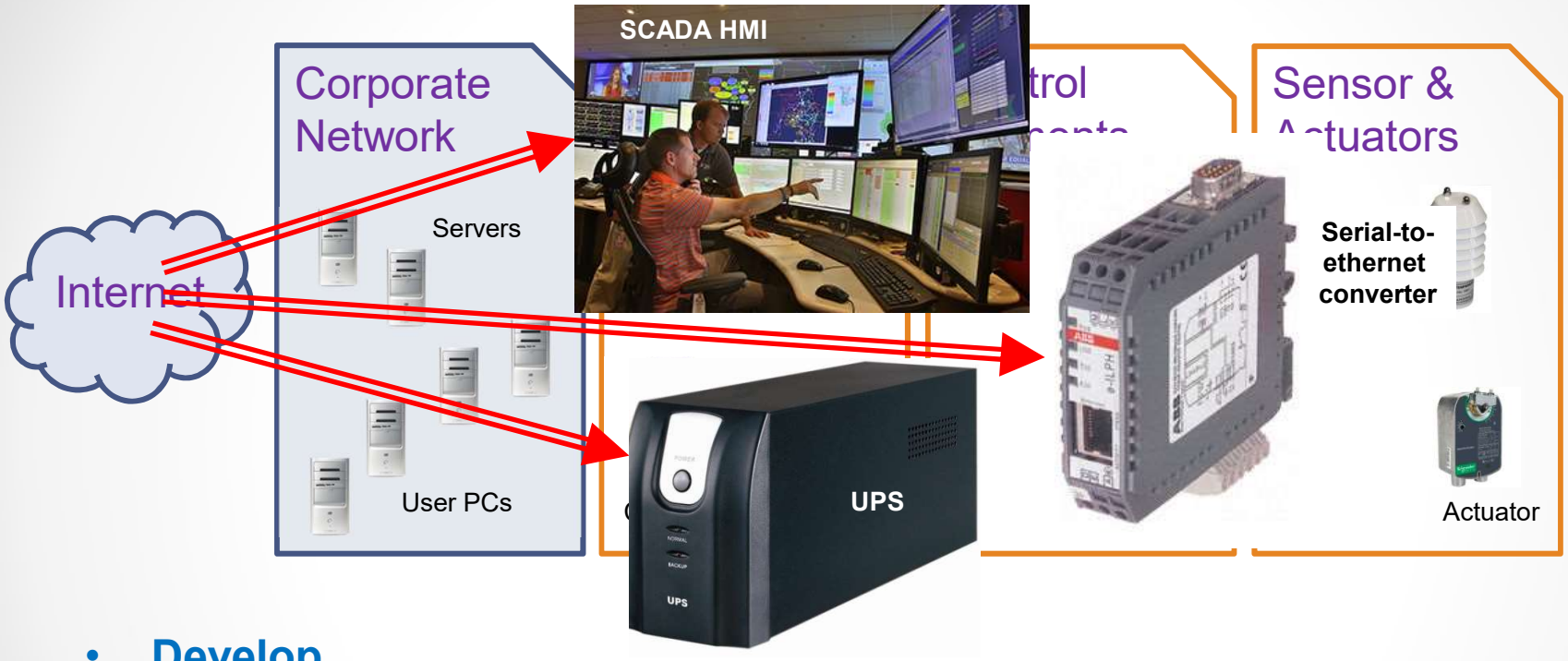
Stage 1: Intrusion



- **Expand to Supervisory Control Network**
  - identify VPN connections from the corporate to supervisory network
  - collect and extract information about control systems and other elements

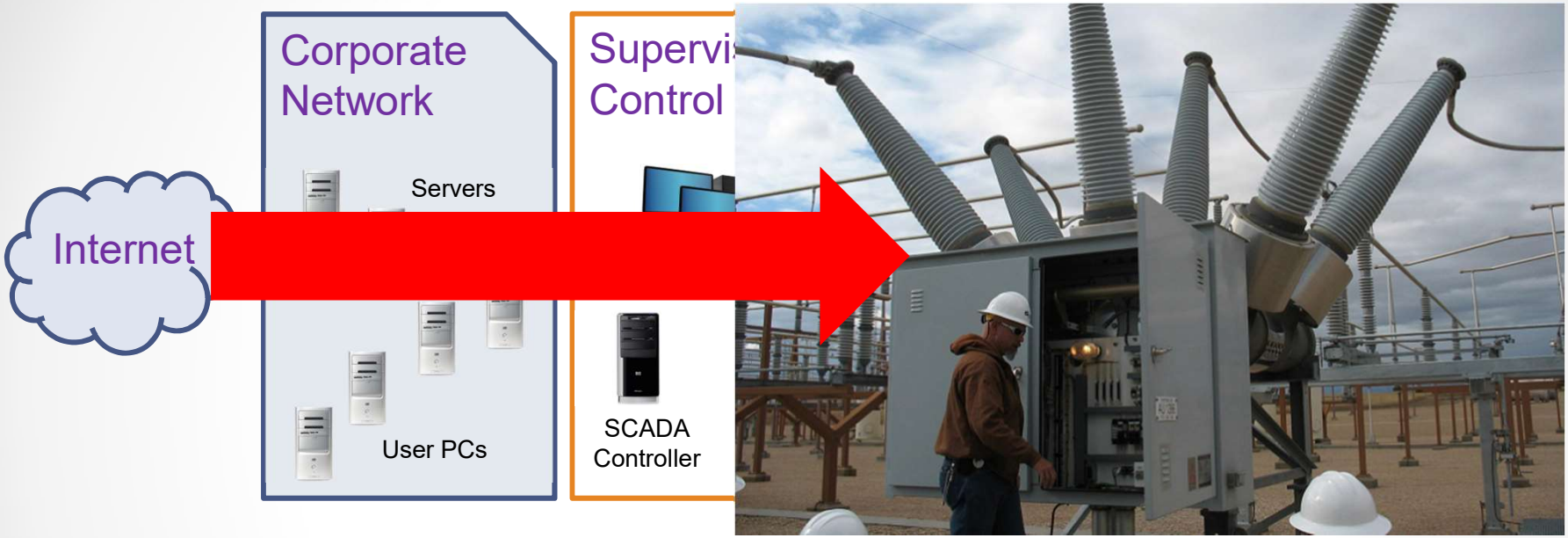
NOTE: 1) the various DSOs probably utilize different systems
2) the duration of Stage 1 can take more than 6 months

Stage 2: Cause Damage



- **Develop**
  - during the six months, the adversary developed capabilities to
    - use remote administration programs to interact with the SCADA controller
    - developed malicious firmware updates for the serial-to-ethernet devices
    - created or customized a KillDisk software for several machines
    - modified the software running in the UPS of the datacenter

Stage 2: Cause Damage



- **Damage**
  - Command the SCADA controller to open circuit breakers, causing substations to shutdown causing the loss of power at the customers
  - Delay recovery
    - upload malicious firmware to prevent communications to field devices
    - use KillDisk and disable UPS to preclude the restart of the machines
  - Perform a telephonic Denial-of-Service to the DSO call center
    - to frustrate customers and prevent the DSO from being informed about the outage

Ciências
ULisboa

Utopia or Reality?

Ciências ULisboa

Defense Capabilities

- Does Portugal have the necessary capabilities to prevent such sort of attack in **any** of its critical infrastructures?
  - CII: energy; telecommunications; transports; …
  - Expertise to build secure solutions, such as …
    - are infrastructures organized to increase the difficulty of credential theft?
    - are monitoring solutions in place to detect entrance in the most critical control networks?
    - if a successful attack occurs, can the systems be restored within an acceptable time frame?
  - Education is a fundamental area
    - are employees being taught about spear phishing?
    - do ICT departments include security experts? are they heard when relevant decisions are taken?
  - ***What about alternative attacks? Are they addressed?***

Ciências ULisboa

Offensive Capabilities

- Should Portugal have the capabilities to perform such sophisticated missions?
  - being able to conduct combat operations in cyberspace will be required in the future
    - will be equivalent to land / air / sea military missions
    - in short term, ability to do such actions will be needed for an effective participation in international organizations (ex. NATO)
  - interesting for a country with limited resources
    - less expensive than buying traditional military equipment
    - mostly related to training people
    - funds remain at least in part in Portugal
  - worrying to instruct people to become expert cyber attackers
    - if they leave the military, ***what will they do?***

Ciências ULisboa

U.S. Cyberattacks Target ISIS in a New Line of Combat

Defense Secretary Ashton B. Carter is among those who have publicly discussed the new mission, but only in broad terms, and this month the **deputy secretary of defense, Robert O. Work**, was more colorful in describing the effort.

"We are **dropping cyberbombs**," Mr. Work said. "We have **never** done that before."

The campaign has been conducted by a small number of "national mission teams," newly created **cyberunits** loosely modeled on Special Operations forces.

< . . . >

In an interview this month in Colorado Springs, where she talked to Air Force Academy cadets, Mr. Obama's **national security adviser, Susan E. Rice**, said that the fight against the Islamic State had to be thought of as a multifront war — and that **computers were just another weapon in the arsenal**.

Source: New York Times, 24 Abril 2016

Ciências ULisboa

Reality

- The attack was performed on the 23rd of December 2015
- Three DSOs were compromised in Ukraine
  - cyber attacks were performed 30 min apart from each other
  - at least 27 medium voltage substations were affected (< 110kV)
  - 225 000 customers were affected
  - restoration took several hours

- Recovery was achieved relatively quickly given the sophistication of the attack
  - DSOs moved to manual operations
  - engineers were deployed to the various substations
  - power was manually restored

Ciências
ULisboa

Thank you!

Nuno Neves (nuno@di.fc.ul.pt)
Web: **www.di.fc.ul.pt/~nuno** *and*
msi.di.fc.ul.pt