A Tale of Two Industroyers: It was the Season of Darkness

Luis Salazar, Sebastian R. Castro, Juan Lozano, Keerthi Koneru, Emmanuele Zambon, Bing Huang, Ross Baldick, Marina Krotofil, Alonso Rojas, and Alvaro A. Cardenas

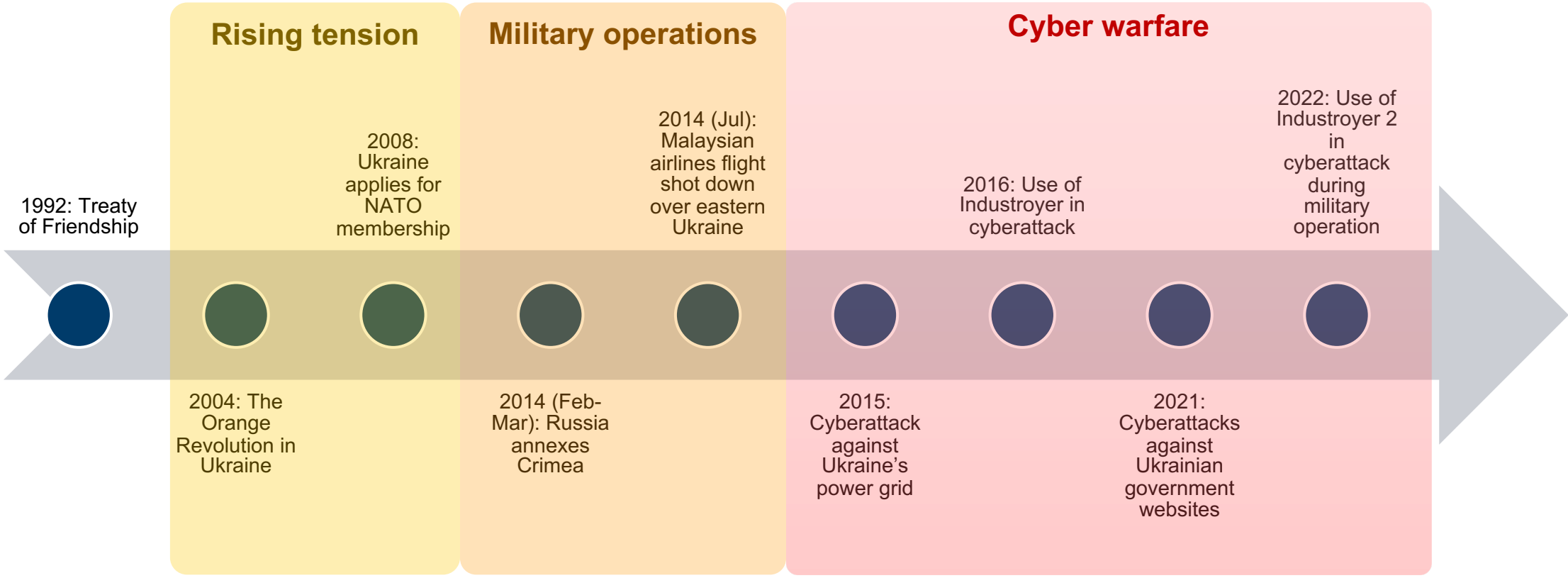
UC SANTA CRUZ

“By using terror and cold, the Russians want to break our spirit and unity. They believe that cold will become their most effective weapon of subjugation, so they are trying to destroy our power generation facilities. They are also trying to break up our national power grid by targeting substations so that even if there is power, it cannot be transferred from one part of the country to another”

- Yaroslav Demchenkov, Ukraine’s deputy energy minister

https://www.cnn.com/interactive/2023/02/europe/putin-ukraine-energy-infrastructure-attack/index.html

A timeline between Russia and Ukraine



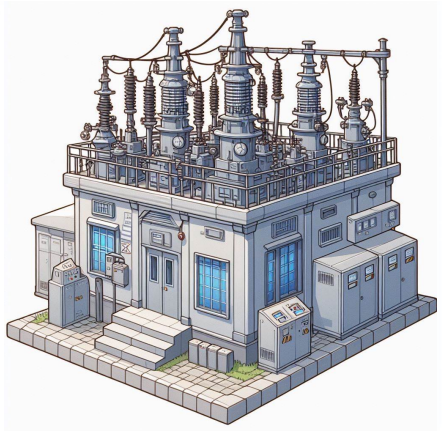
The power grid

Control Room

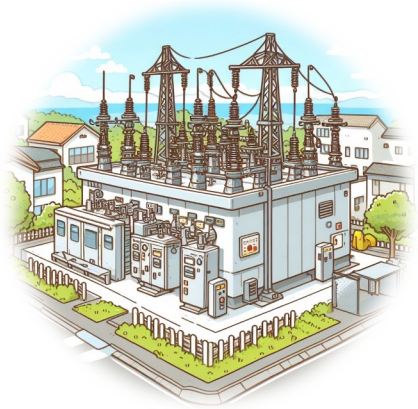
Two primary objectives:

- Synchronized generation
- Power transmission

Generation



Transmission Substation



Distribution Substation

Synchronization

Try to keep all the generated energy at the same frequency and voltage

60.1 Hz

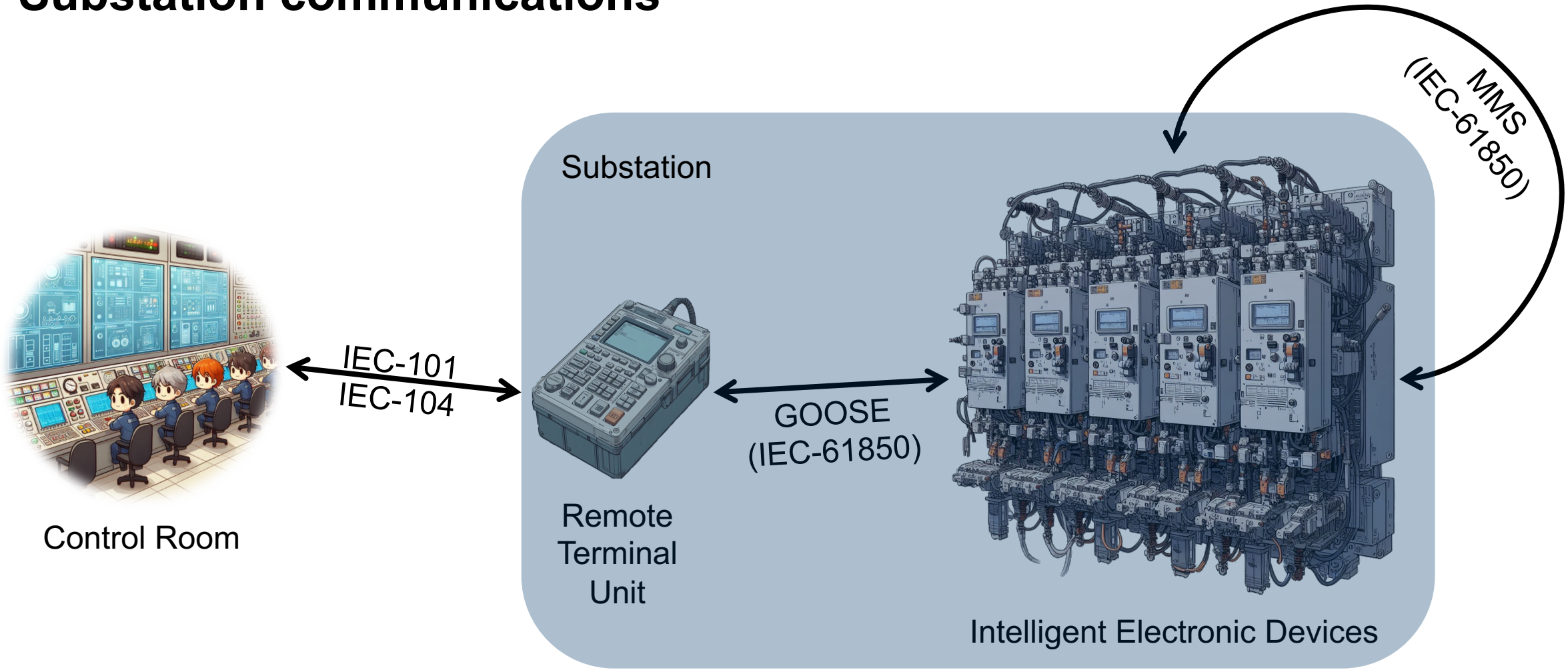
59.9 Hz

60.1 Hz

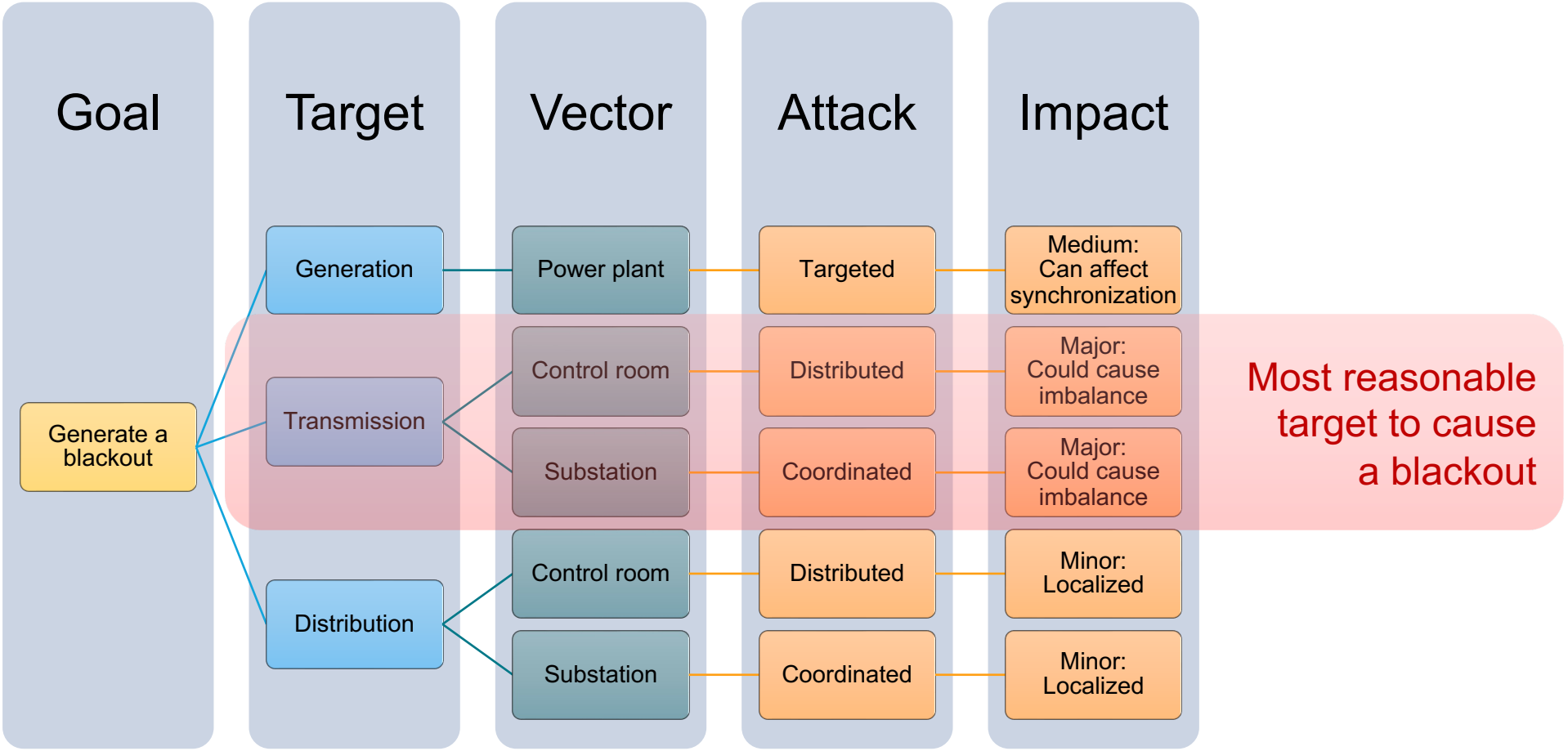
Power transmission

- Balance the produced energy with the consumption
- Send the energy where needed

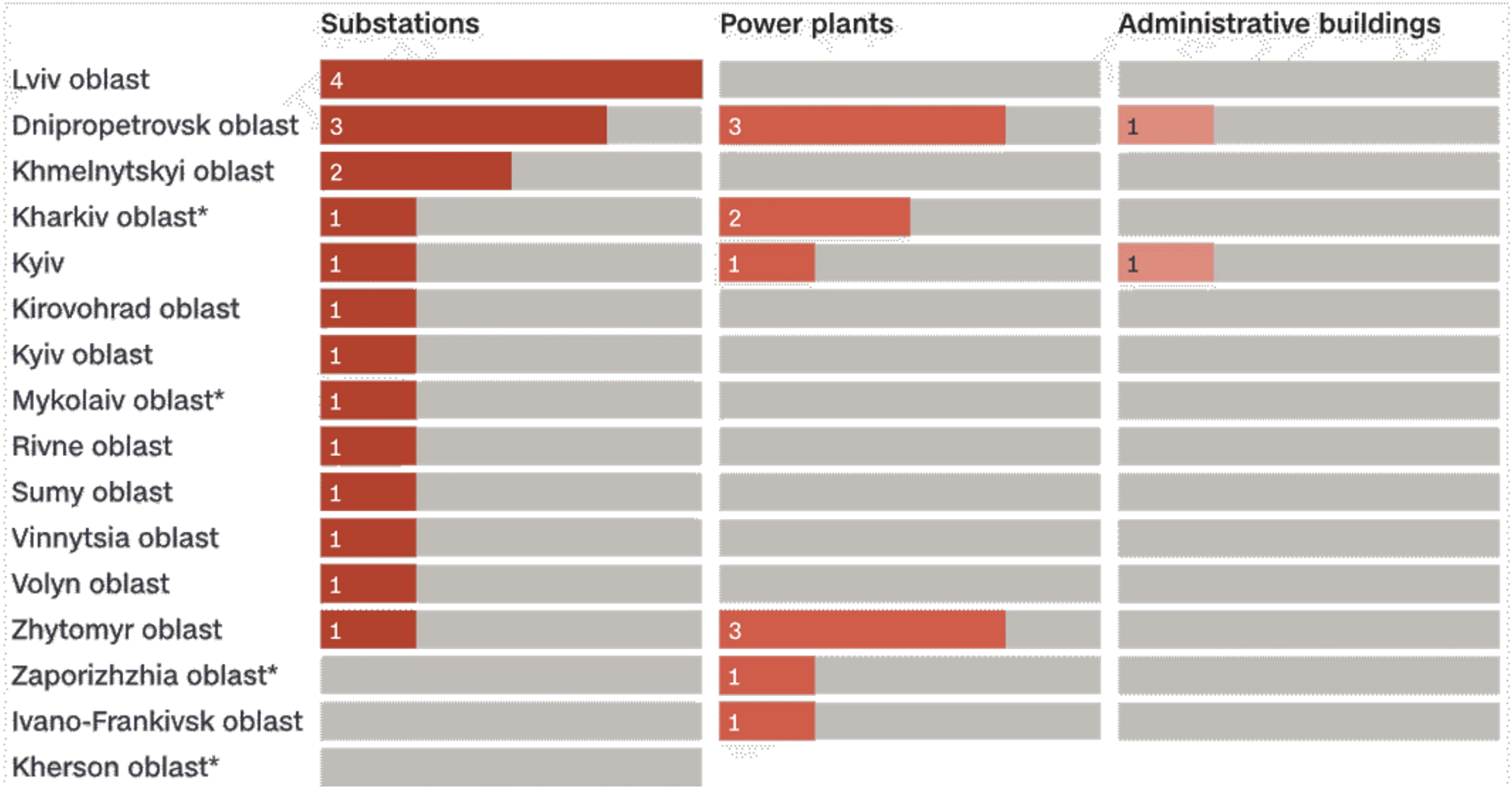
Substation communications



Target selection

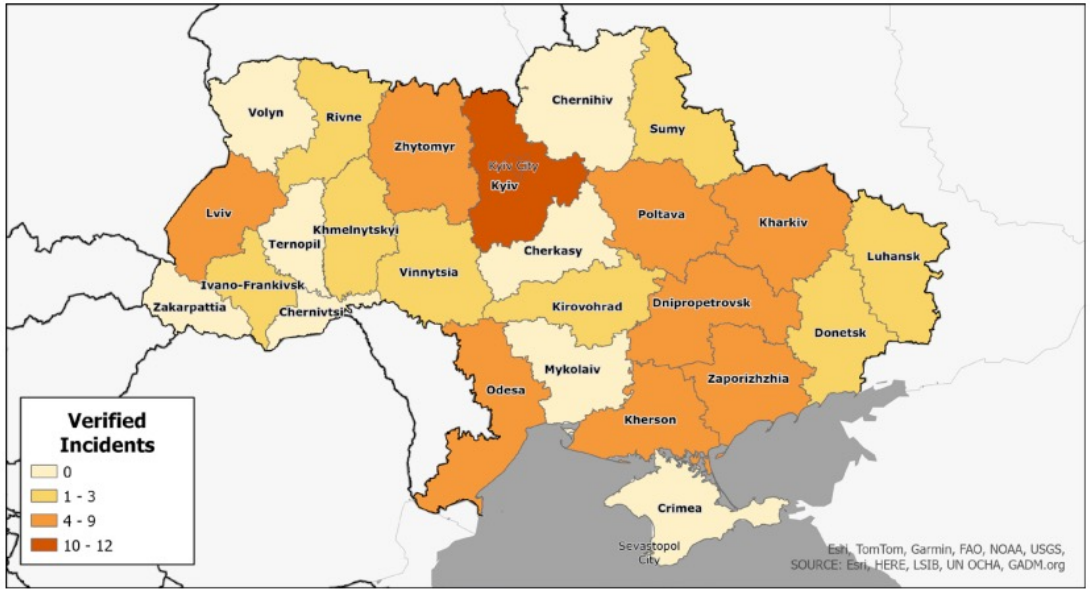


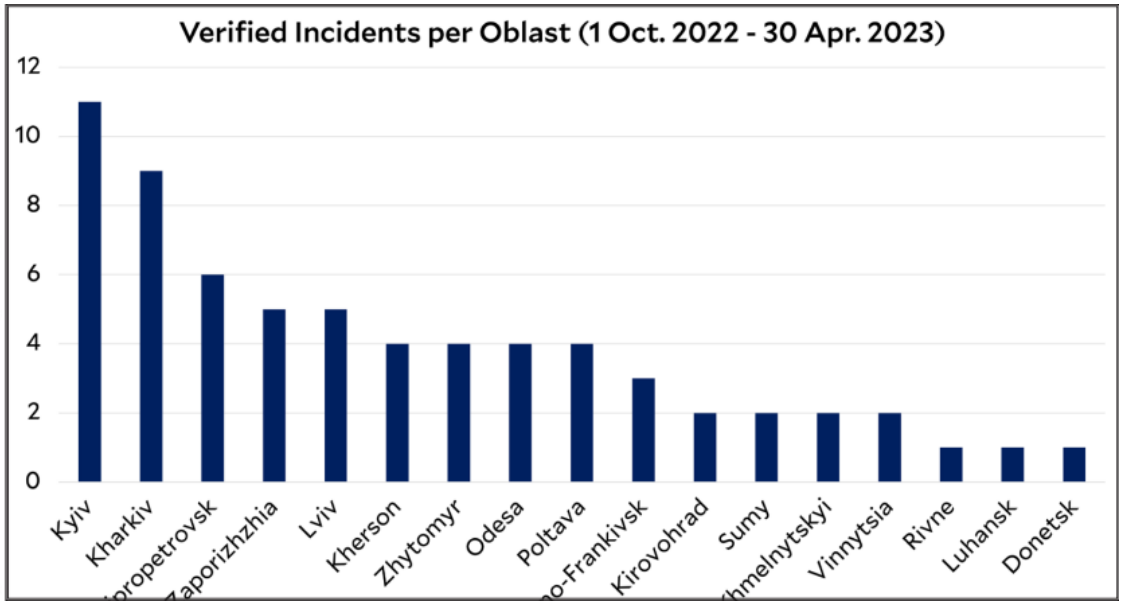
Military strikes against power facilities (Oct 2022)



https://www.cnn.com/interactive/2023/02/europe/putin-ukraine-energy-infrastructure-attack/index.html

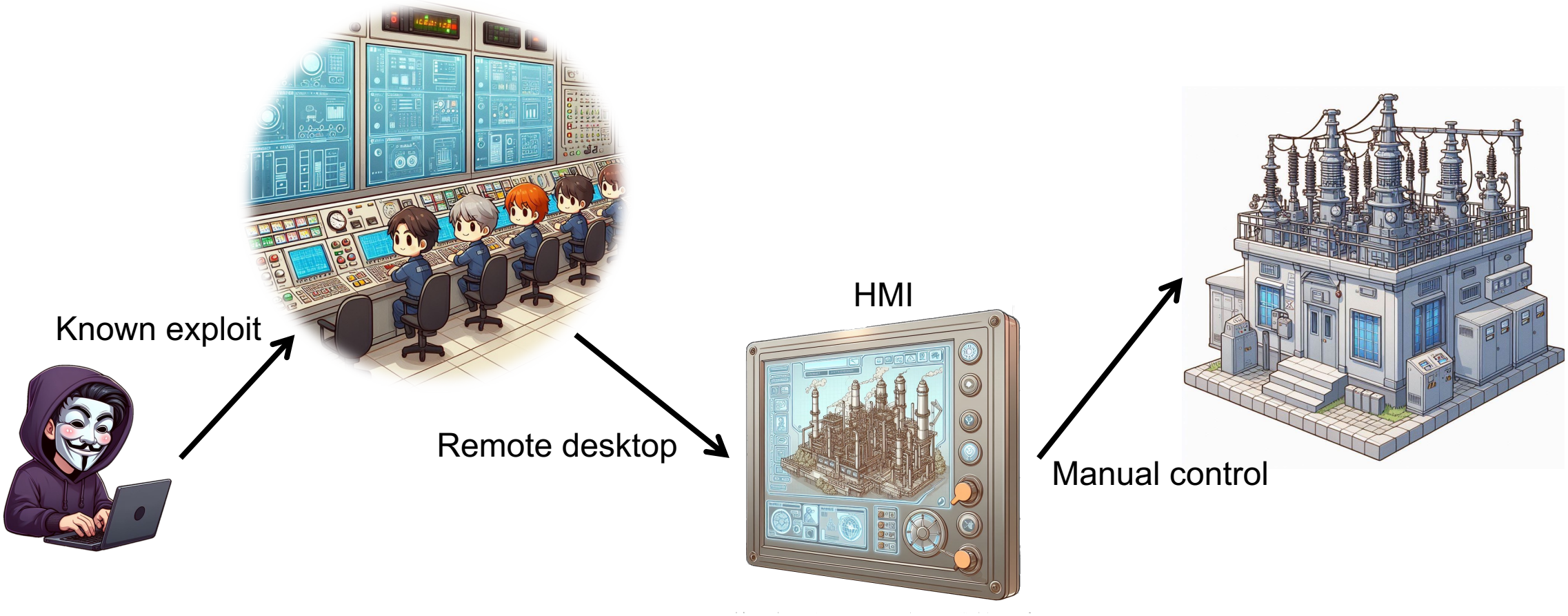
Verified incidents of damage by oblast (Oct/2022 – Apr/2023)





Hathaway, Oona A., Caitlin N. Howarth, Kaveh Khoshnood, Nathaniel A. Raymond et al., “Remote Assessment of Bombardment of Ukraine’s Power Generation and Transmission Infrastructure, 1 October 2022 to 30 April 2023.” 29 February 2024. Humanitarian Research Lab at Yale School of Public Health and Ukraine Digital Verification Lab: New Haven.

2015 Attack

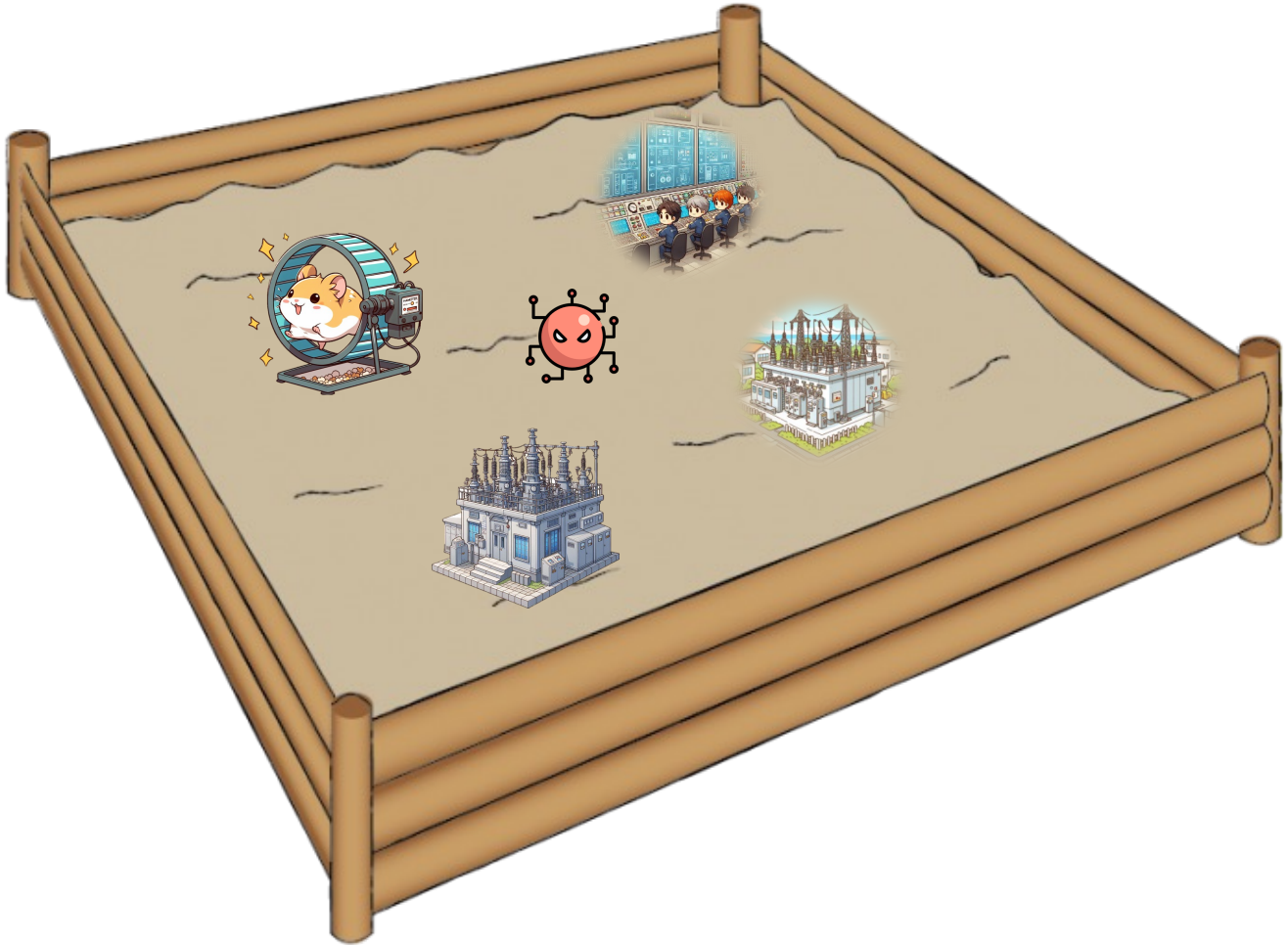


How to safely study a malware targeting a physical system?

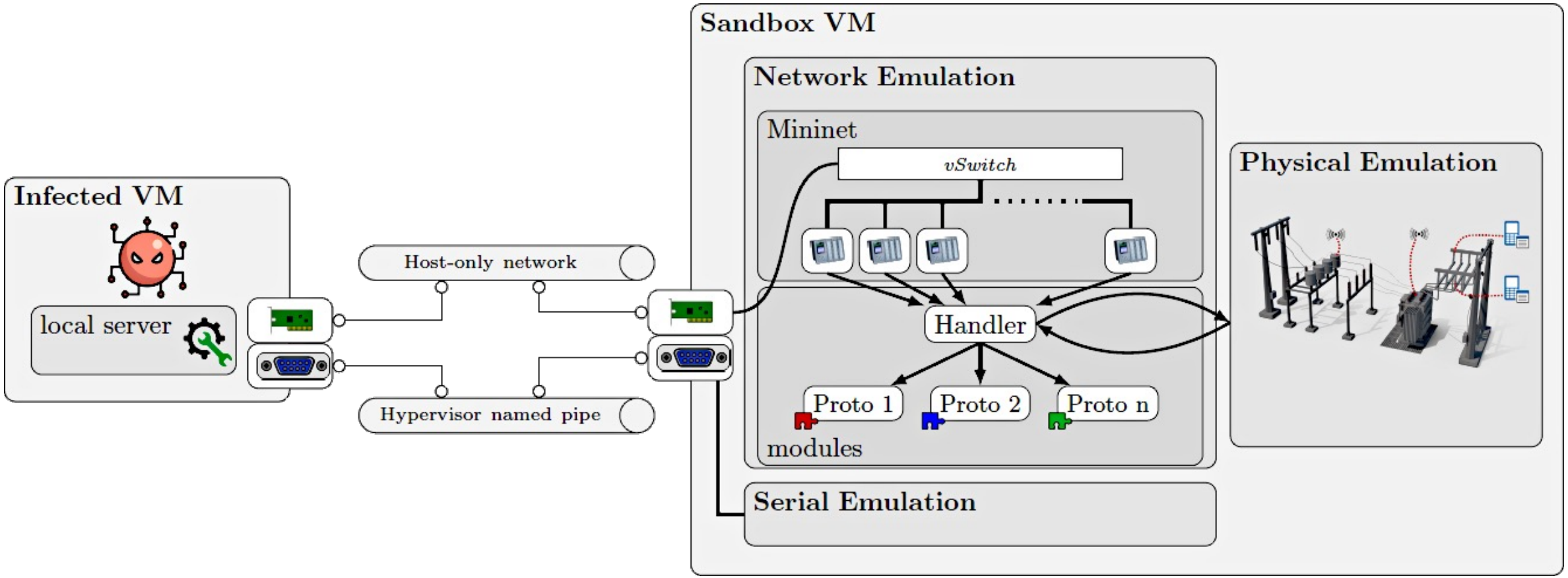
Previous efforts

- Binary analysis
  - (Encryption / Obfuscation techniques)
- Reverse engineering / Disassembly
- Identify system calls
- Execution in a sandbox
  - Execution analysis
  - Network analysis
    - Traffic / Protocol analysis
    - Behavioral analysis (Industrial Control - centered)

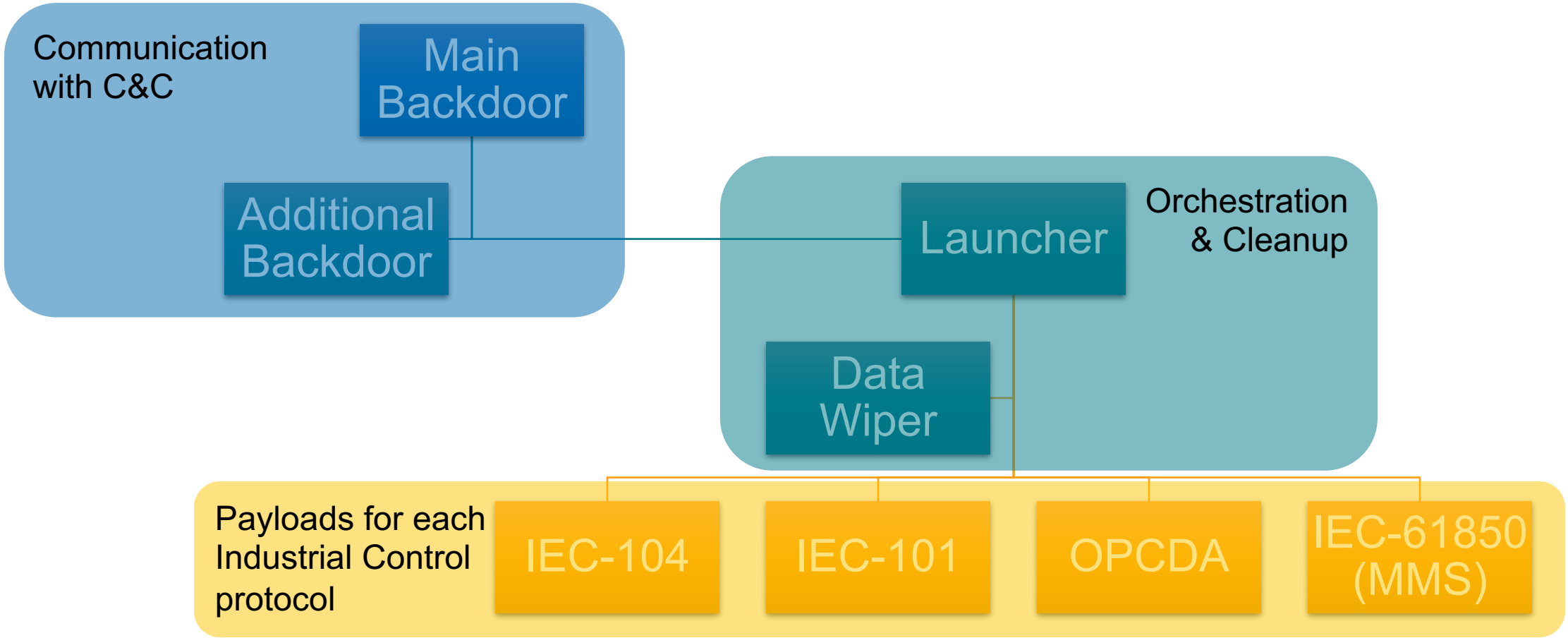
Safely testing the malware



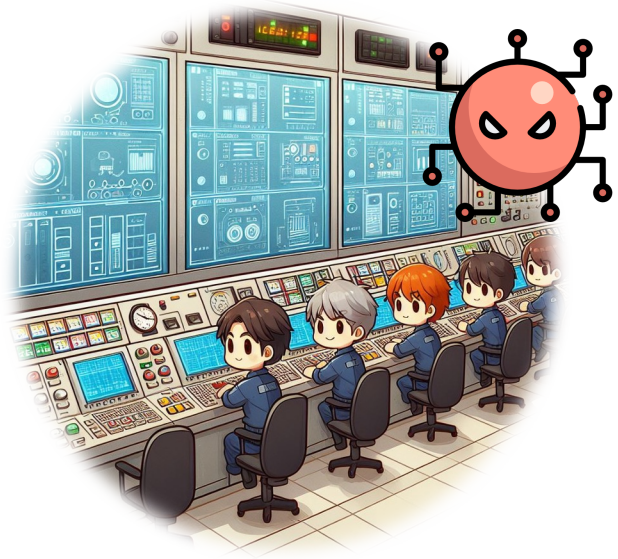
Sandbox architecture

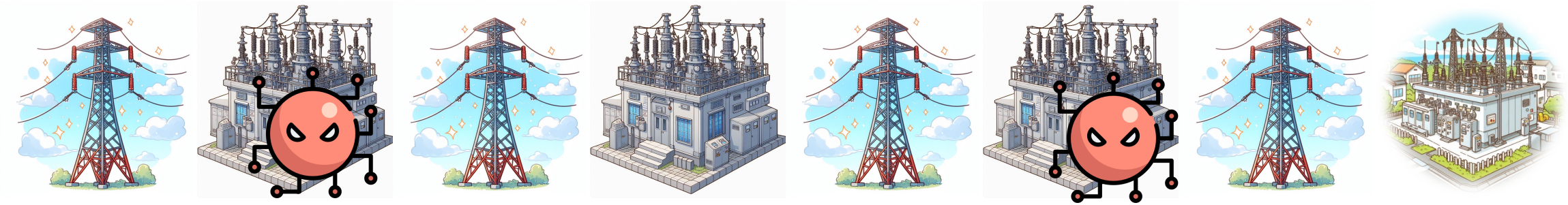


Industroyer 1 a.k.a. CrashOverride (2016)



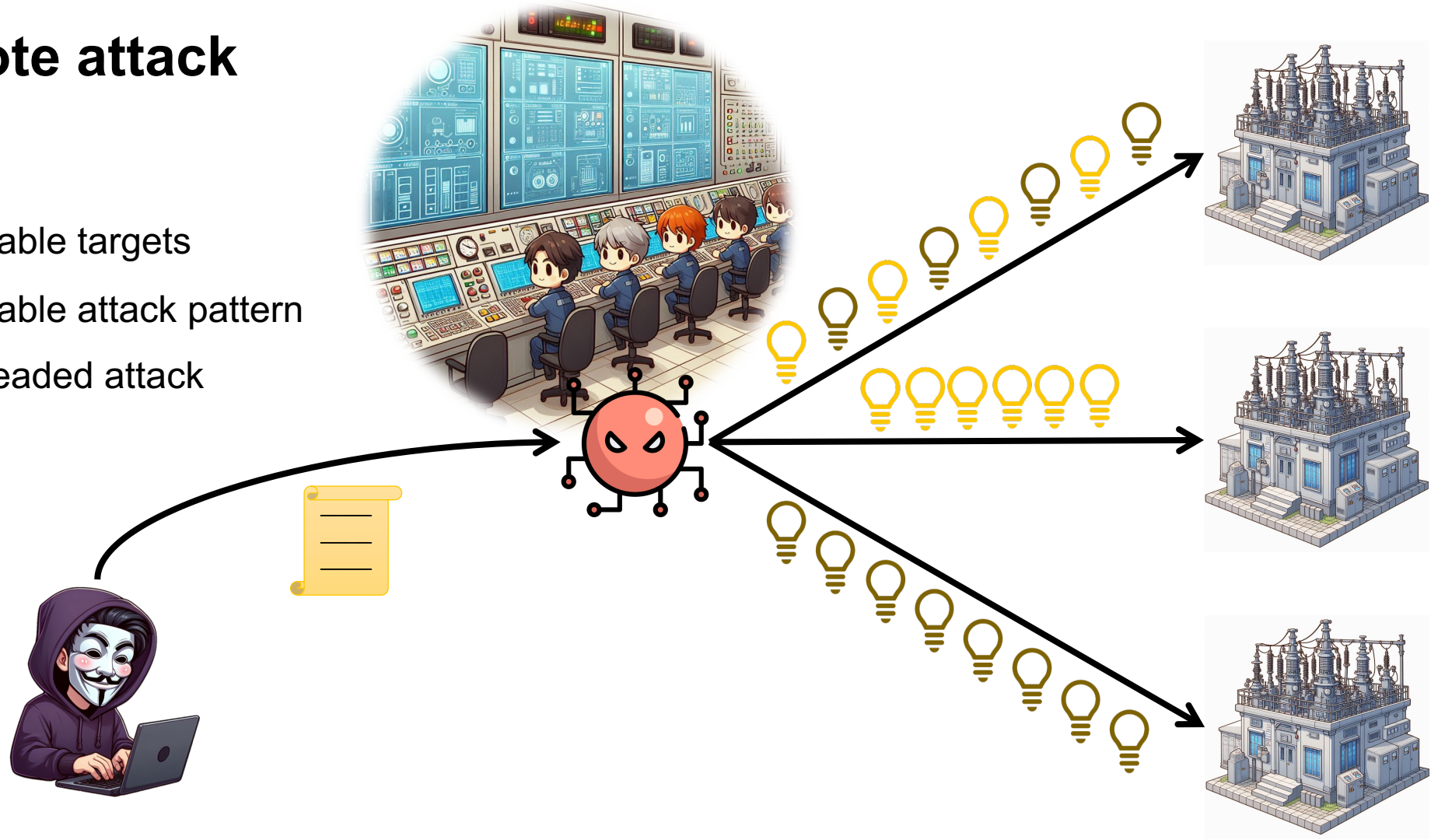
Deployment





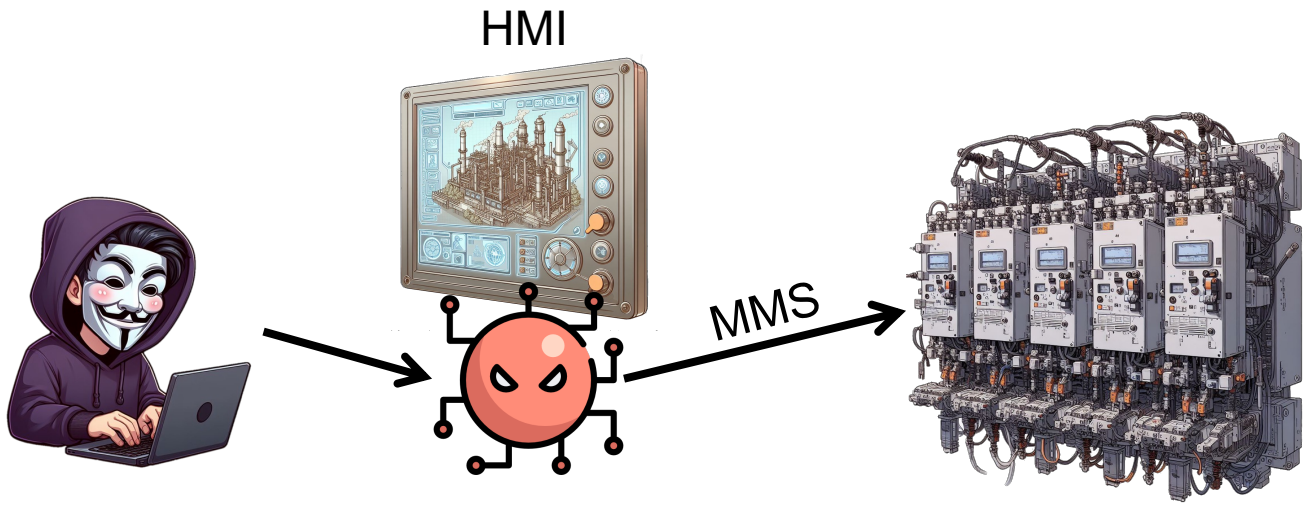
Remote attack

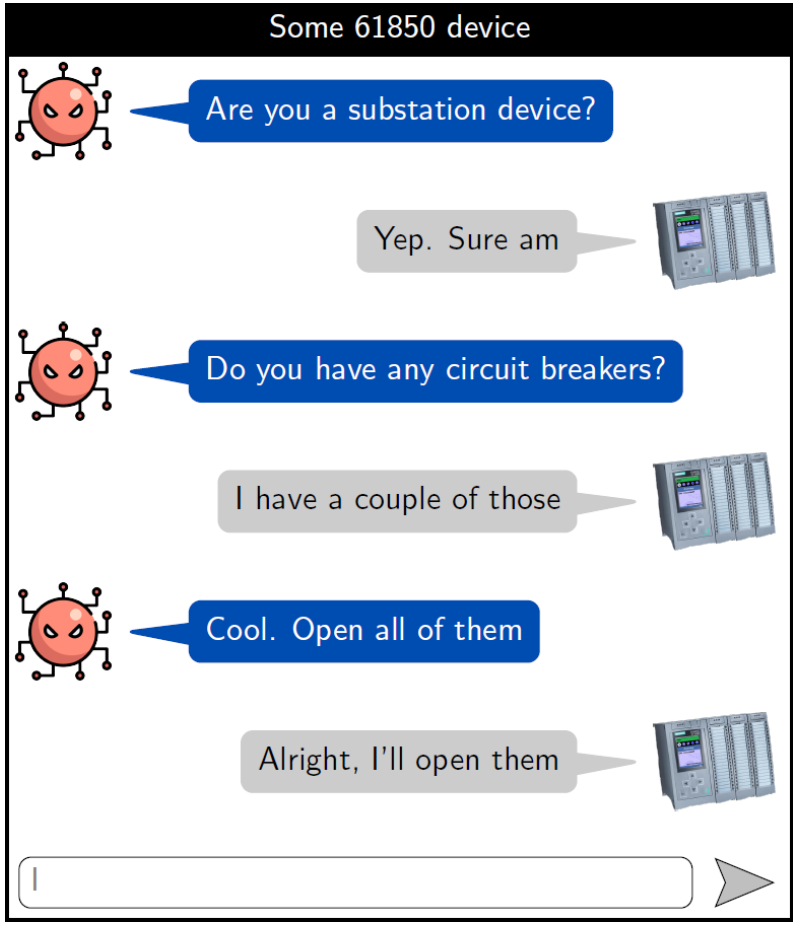
- Configurable targets
- Configurable attack pattern
- Multi-threaded attack



Local attack

- Semi-autonomous attack
- Scanning capabilities
- No configuration needed

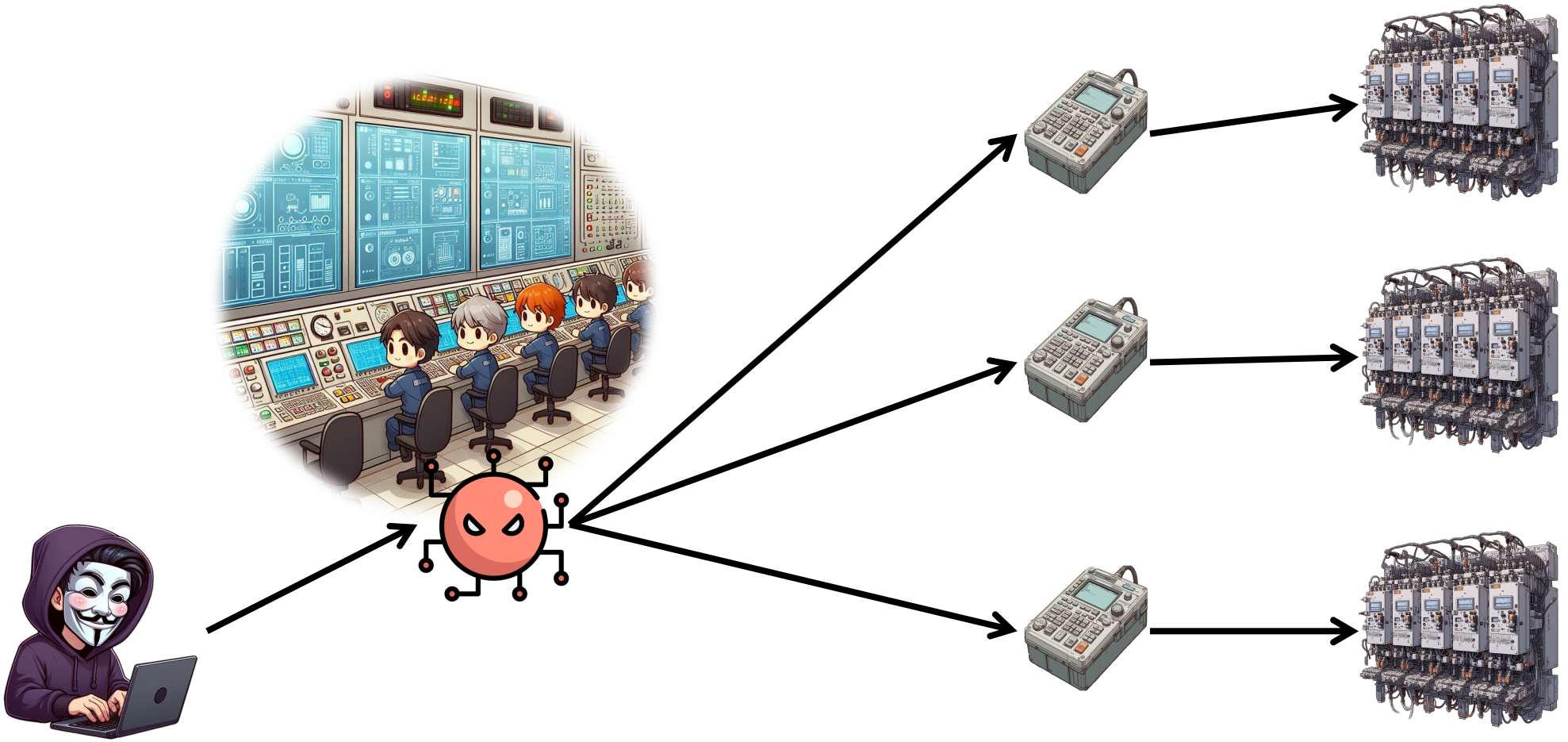




Industroyer 2 (2022)

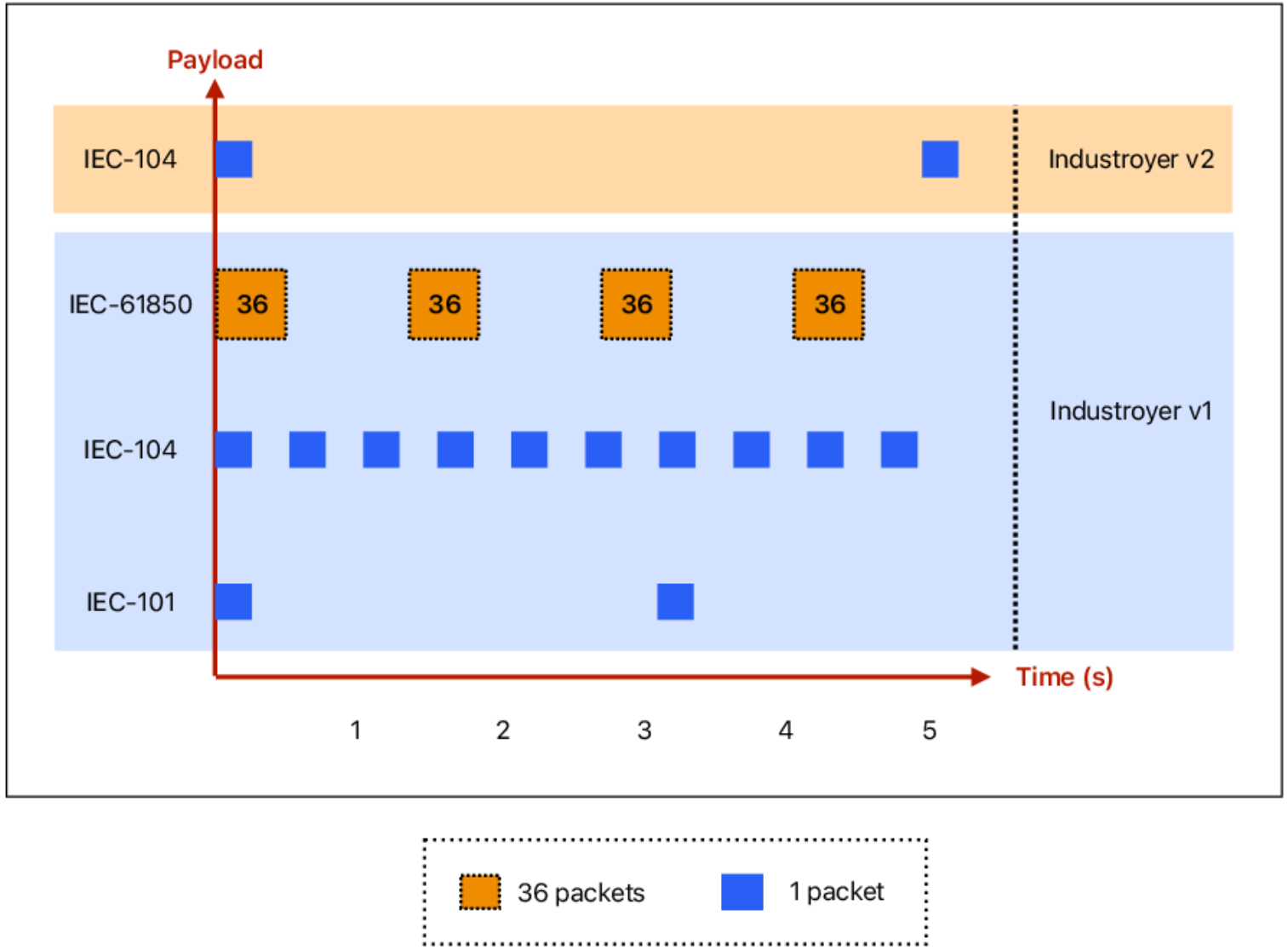
- Stand-alone executable
- Hard-coded configuration
- Single communication protocol (IEC-104)
- Single-shot attack (No infinite loop)

Industroyer 2 deployment

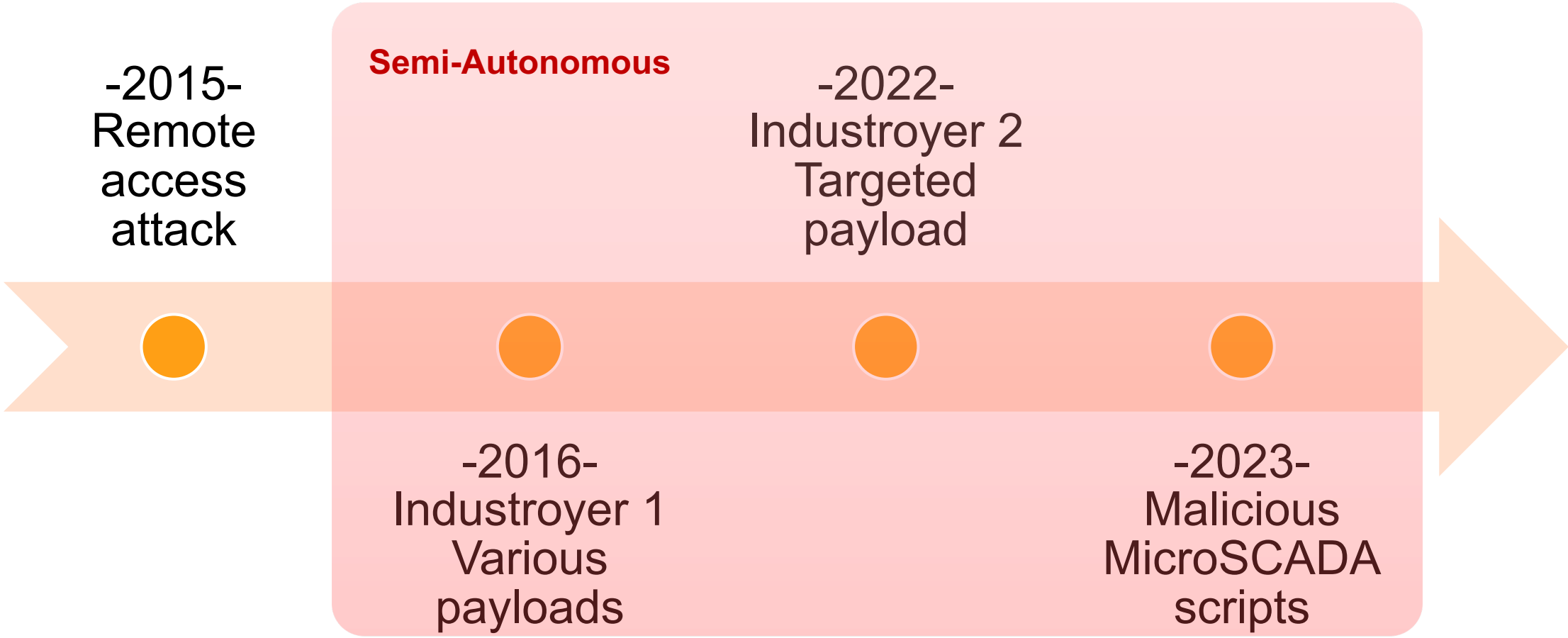


Timing

Each payload has a different timing and behavior.



Evolution of Russian cyber attacks



Questions?

UC SANTA CRUZ