Dutchpower

Hacking the grid

10-03-2026

BUREAU VERITAS

01 / INTRO

MONDAY, APRIL 28

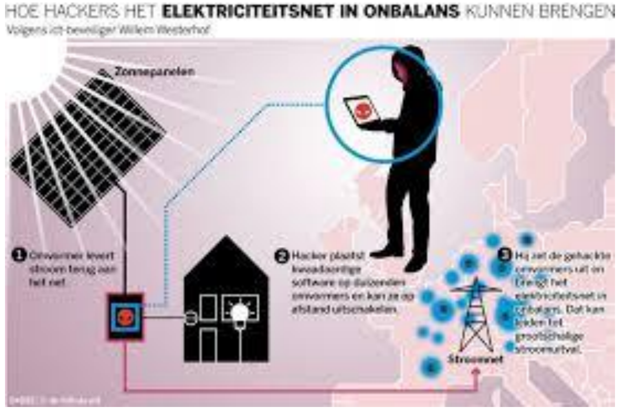
A short story

MONDAY, APRIL 28

A short story

- Reality for a lot of people
  - “Iberian peninsula blackout”
- Power is a necessity!
  - € 1 600 000 000 estimated damage
  - 8 deaths, 25+ injuries
  - Less than 16 hours for full recovery.

WHO AM I?


HOE HACKERS HET **ELEKTRICITEITSNET IN ONBALANS** KUNNEN BRENGEN

Volgens ict-beveiliger Willem Westerhof

1 Omvormer levert stroom terug aan het net

2 Hacker plaatst kwaadaardige software op duizenden omvormers en kan ze op afstand uitschakelen

3 Hij zet de gehackte omvormers uit en brengt het elektriciteitsnet in onbalans. Dat kan leiden tot grootschalige stroomuitval.

Secura

A BUREAU VERITAS COMPANY

RAPPORT

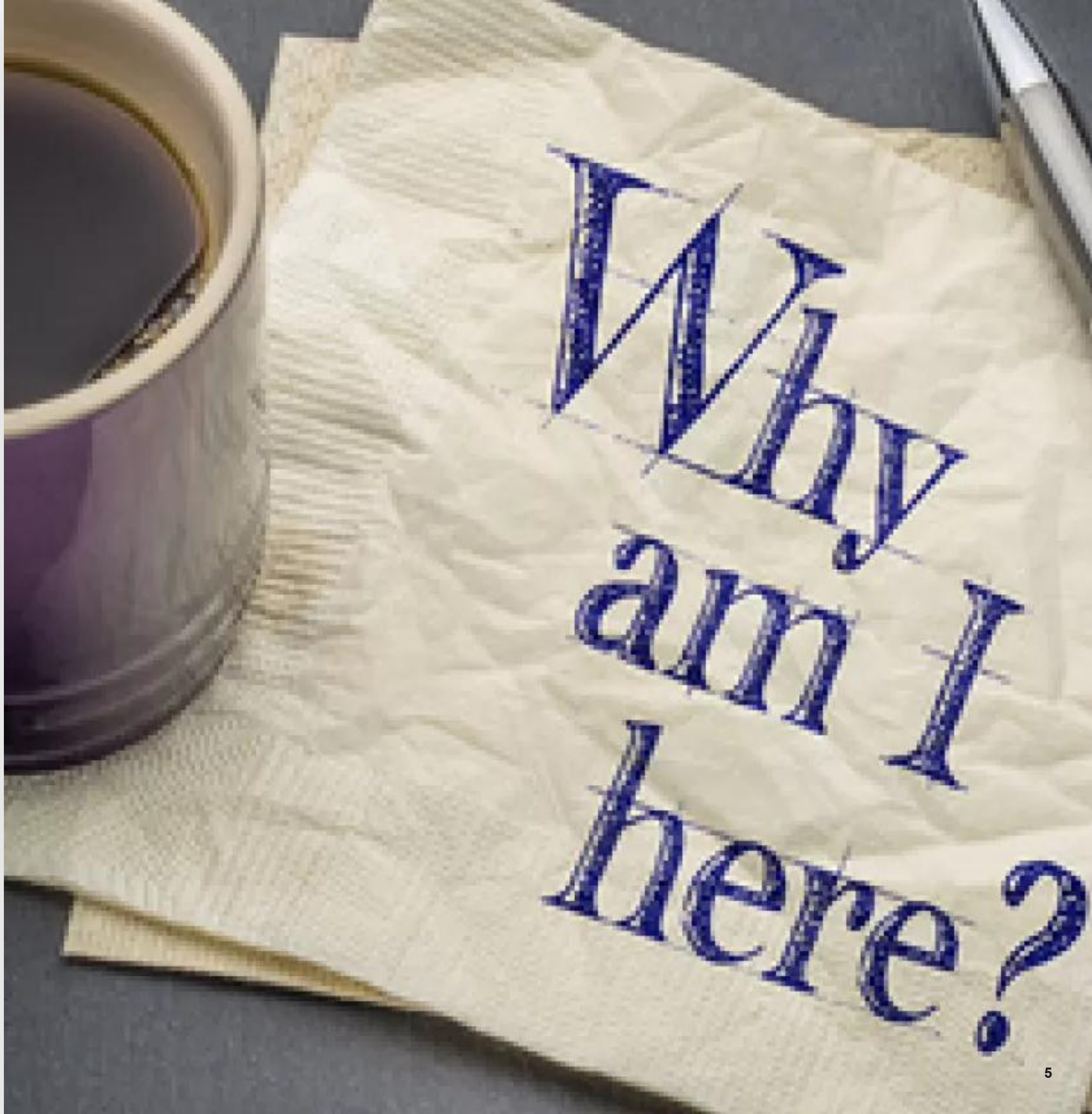
Scenario's en maatregelen voor cyberweerbare zonnestroominstallaties

Publicatieversie

WHY AM I HERE?

- We need the energy transition
  - Ideally without massive security gaps
  - Next-gen needs to be better
  - Solutions solve issues, BUT create new issues.

- Is it really that bad?
  - Yes, let me show you.



Timeline “potential” incidents

“Horus Scenario” (by Willem Westerhof) 21 vulnerabilities discovered in single brand, grid ending scenario.

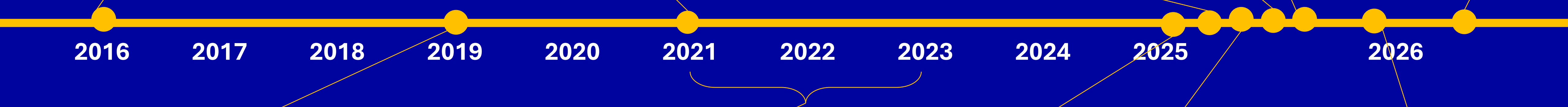
Master Password Cloud portal discovered (DIVD, Jelle Ursem) Access to management portal of ~1m inverters with superadmin rights.

Accounts webportals available on the “Dark web” (Secura) Accounts of users and installers, access to many portals.

API’s hacked of combined portals (Vangelis Stykas) Hundreds of gigawatts affected.

Forescout Sun:down project Multiple inverters tested, critical and scalable vulnerabilities found.

Ongoing disclosures



Trickle Down Vulnerabilities (By Jos Wetzels, Secura) Weaknesses in communicationmodules used by multiple inverters. Hardware supply chain issue.

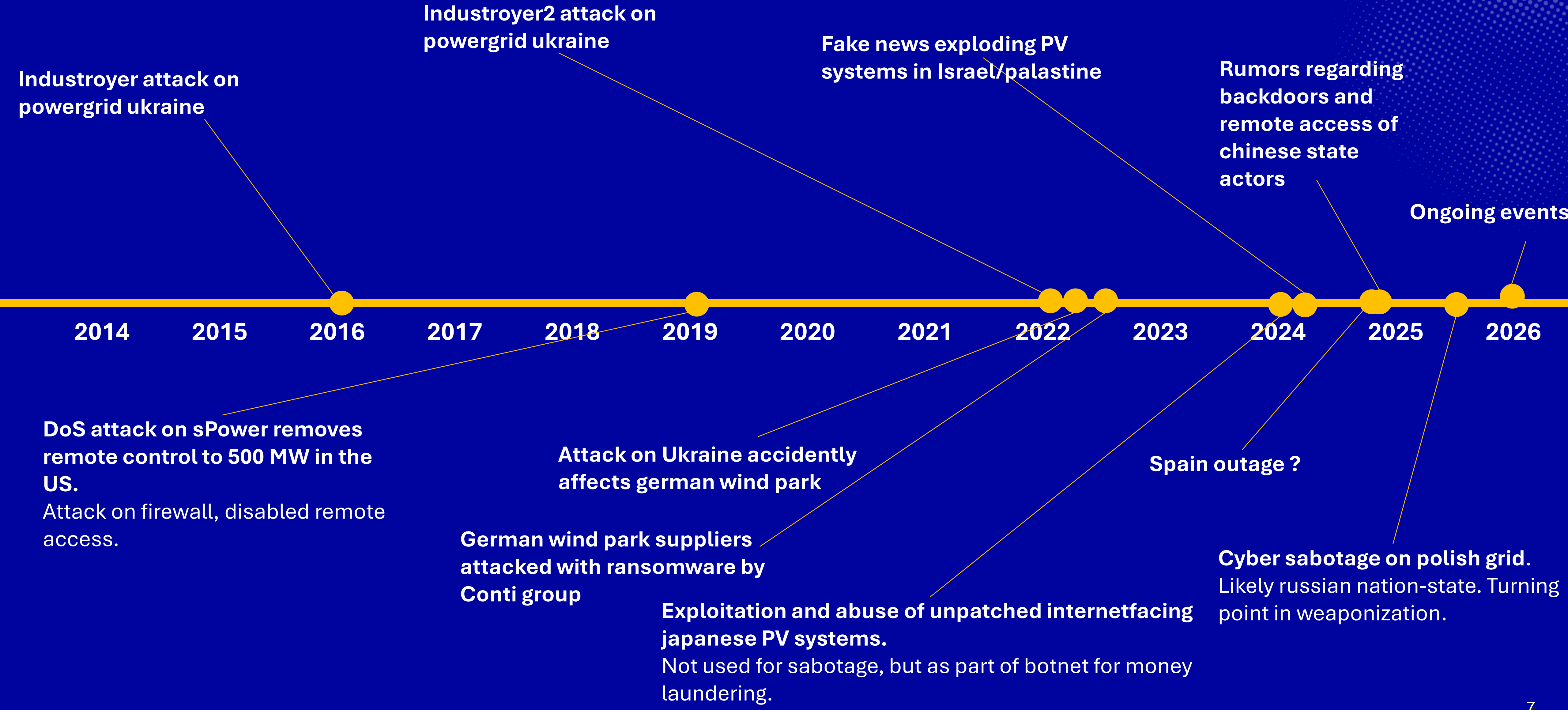
RDI, research inverters Important conclusion: None of the inverters meet basic cybersecurity requirements.

Vulnerabilities in API cloud mgt systems (Bitdefender) Vulnerability in API leads to full account takeover.

Vulnerabilities in solar gateways (DIVD, Wietse Boonstra, Hidde Smit) Combination of 6 vulns, enabling remote control.

Brian Foster: Harmonics and oscillations and boom, physics informed hacking indicates the true dangers once more.

Timeline “real world” incidents



Industroyer attack on powergrid ukraine

DoS attack on sPower removes remote control to 500 MW in the US.
Attack on firewall, disabled remote access.

Industroyer2 attack on powergrid ukraine

Attack on Ukraine accidently affects german wind park

German wind park suppliers attacked with ransomware by Conti group

Exploitation and abuse of unpatched internetfacing japanese PV systems.
Not used for sabotage, but as part of botnet for money laundering.

Fake news exploding PV systems in Israel/palastine

Rumors regarding backdoors and remote access of chinese state actors

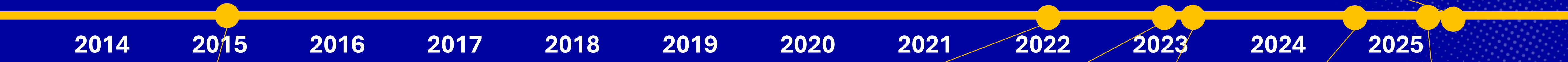
Spain outage ?

Cyber sabotage on polish grid.
Likely russian nation-state. Turning point in weaponization.

Ongoing events

Timeline of “oopsies”

Sigenergy emergency firmware patch, firmware update which enabled remote monitoring and control by vendor to prevent safety hazards.



800.000 Micro omvormers remotely updated
Hawaii, supplier updated everything to stabilize the grid and made it unstable by doing this.

LOG4J, software supply-chain incident
Weakness in common software library makes an insane amount of systems vulnerable.

TLStorm, weakness in UPS systems can lead to physical damage (Armis)
Cyber attack cause electrical fire in UPS and bricks attached systems.

600.000 network routers bricked after firmware update
(US) deliberate attack with malware to disable devices of a specific ISP.

Faulty software update crashes systems globally
Automatic updates in crowdstrike cause a windows crash and downs all sorts of critical businesses

Spain outage ?

CALL TO ACTION

PREVENT

MITIGATE

LESSEN IMPACT

Q&A

- Or ask me later

Willem.Westerhof@bureauveritas.com

BUREAU VERITAS

Shaping a World of Trust

THE BRIGHT SIDE

- Not all bad!

- Role ethical hackers
- Politics, “kamervragen” & lobby
- Knowledge in different layers
- Shift of interest and problem owners

- 10 years from now?