UKRAINE CYBER ATTACK, TRY #1

Guy Barnhart-Magen,

October 17, 2017

LEGAL NOTICES AND DISCLAIMERS

This presentation contains the general insights and opinions of its author, Guy Barnhart-Magen. I am speaking on behalf of myself only, and the views and opinions contained in this presentation should not be attributed to my employer.
The information in this presentation is provided for informational and educational purposes only and is not to be relied upon for any other purpose. Use at your own risk! I makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. I accept no duty to update this presentation based on more current information. I disclaim all liability for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of or reliance on the content of this presentation.
No computer system can be absolutely secure.
No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.
*Other names and brands may be claimed as the property of others.

WHO AM I?

- Guy Barnhart-Magen
- **Security Researcher**, Manager, Presenter
- Interests:

  Crypto, Embedded systems, System and product security
- iSTARE team
  - Intel Security Threat Analysis and Reverse Engineering
  - Leading the "AI Security Innovations" team
- "We break what we make"

We Are Hiring!

WHAT WILL WE COVER?

- Background
- Attack layout
- Anecdotes
- Then attack #2 happened (not covered in this talk)
- Then “WannaCry” and “Petya” happened
- There was much rejoicing

- https://revdrbrian.files.wordpress.com/2016/03/and-there-was-much-rejoicing.jpg

WHY IS THIS INTERESTING?

- First large scale attack on a utility, discussed in public
- Attack caused critical infrastructure to fail
- This could have been much worse that it was

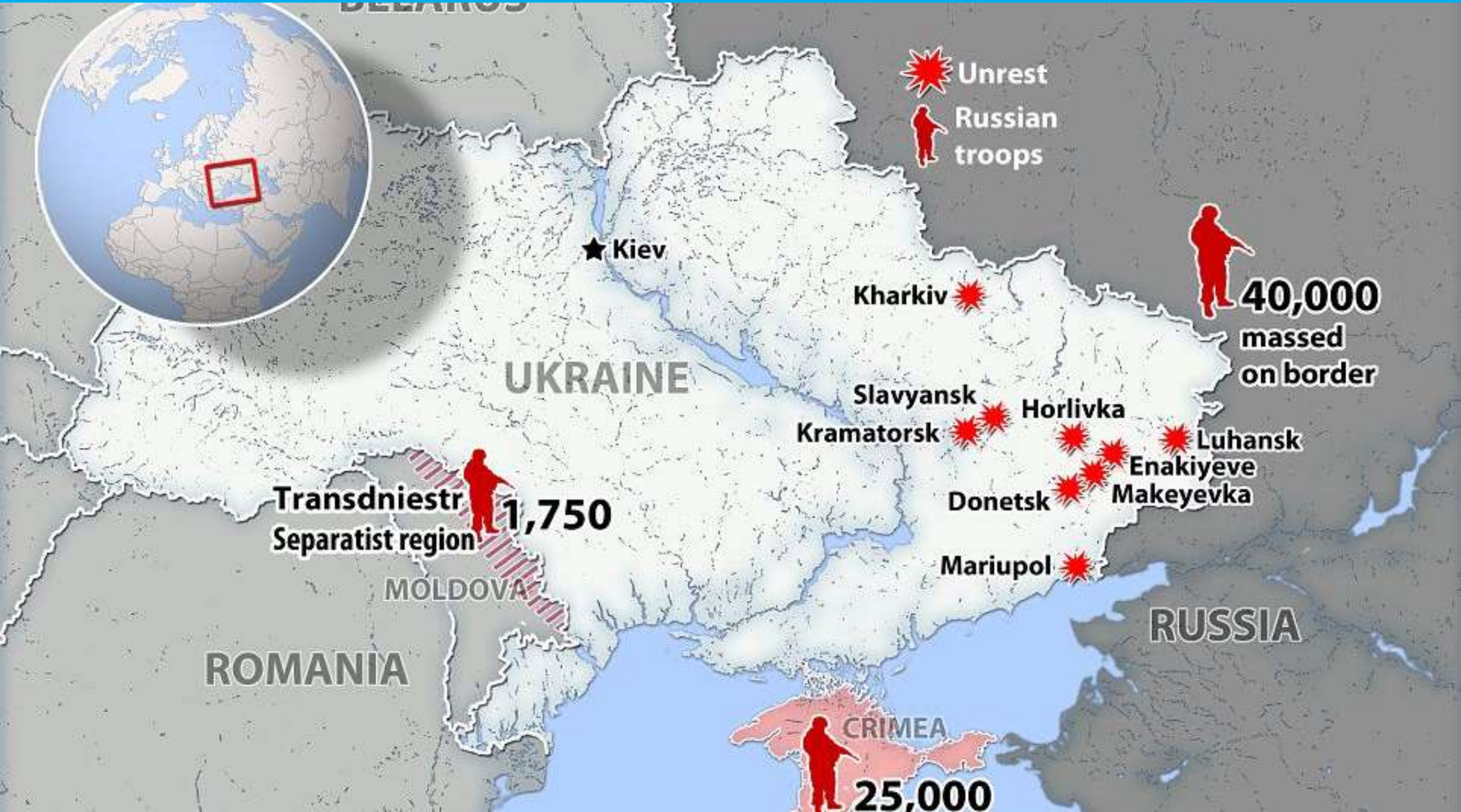
Probably a warning shot – not a full out attack

BACKGROUND

- The attack focused on 3 power utilities in the transport segment
- Over 250,000 people affected
- December 2015, winter, Ukraine
- Holiday – less people in the office
- Multi team/phased attack

- http://www.ukrainebusiness.com.ua/modules/news/images/topics/4e1bbcd2-d7a7-81e4.gif

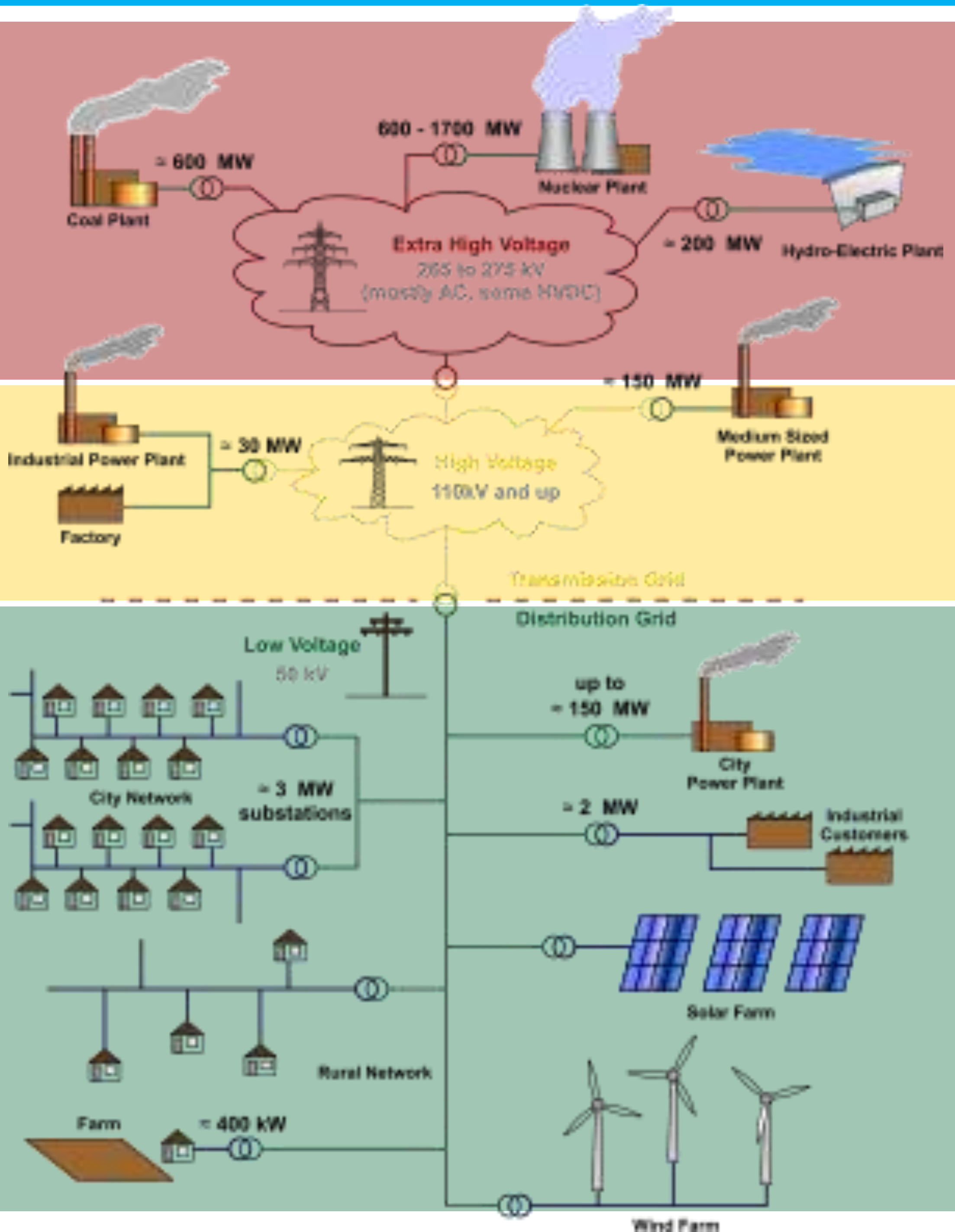
- https://ichef-1.bbci.co.uk/news/624/cpsprodpb/103C4/production/_88500566_cb3005b8-e157-4ee5-808c-cf00ae46effe.jpg


BELARUS
Unrest
Russian troops
Kiev
Kharkiv
40,000 massed on border
UKRAINE
Slavyansk
Horlivka
Kramatorsk
Luhansk
Enakiyeve
Makeyevka
Donetsk
Transdniestr
Separatist region
1,750
MOLDOVA
Mariupol
RUSSIA
ROMANIA
CRIMEA
25,000

Generation

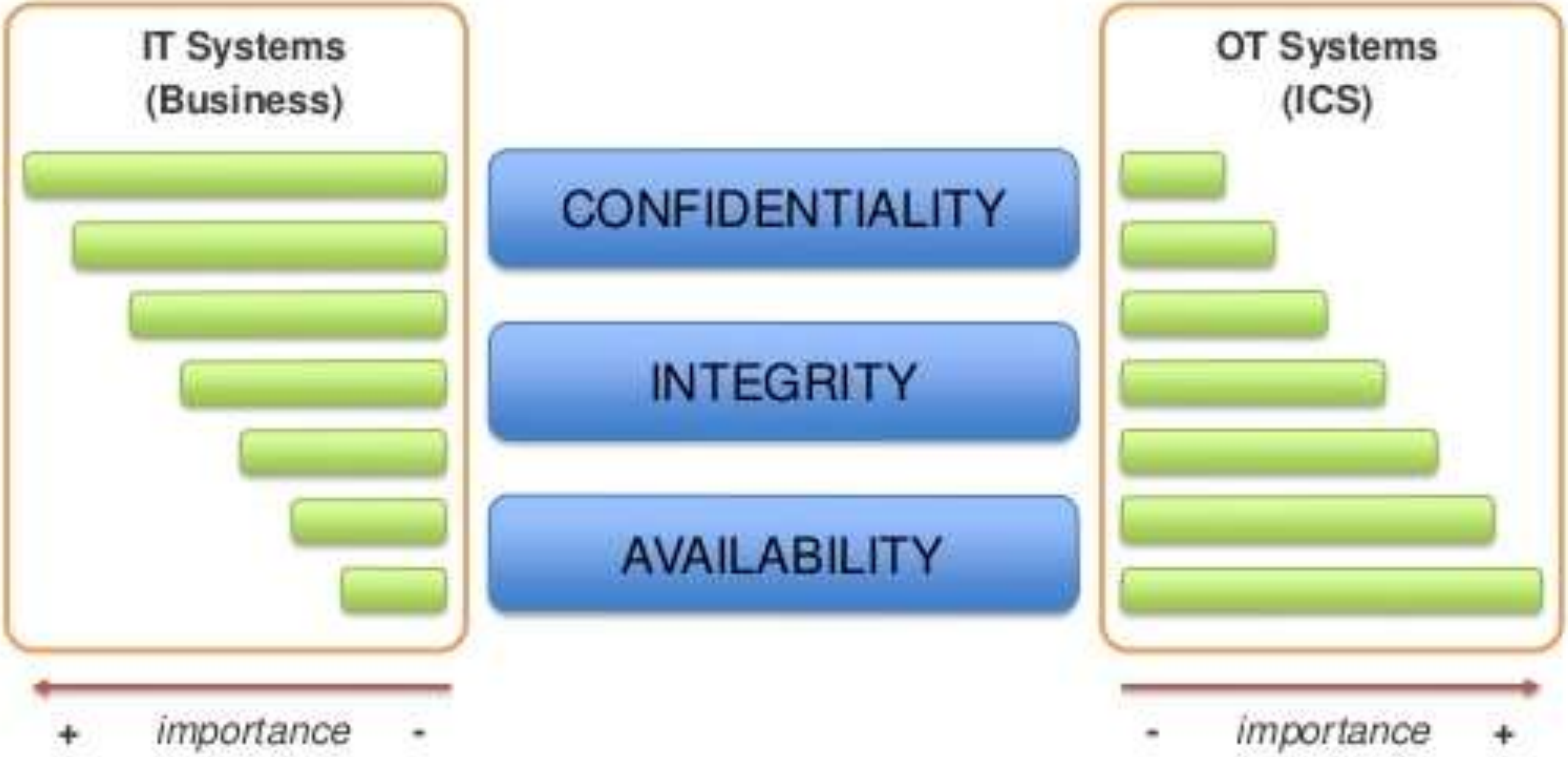
Transmission

Distribution



GROW YOUR **NETWORK.**
ENHANCE YOUR **KNOWLEDGE.**

SECURITY PRINCIPLES (IT *vs.* OT)



IT Systems
(Business)

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

OT Systems
(ICS)

+ *importance* -

- *importance* +

Did
Somebody Say
Shenanigans?
ICANHASCHEEZBURGER.COM

PHASE 1

- Before anything else, they placed the UPS to scheduled maintenance mode
- Timer for T0+4h

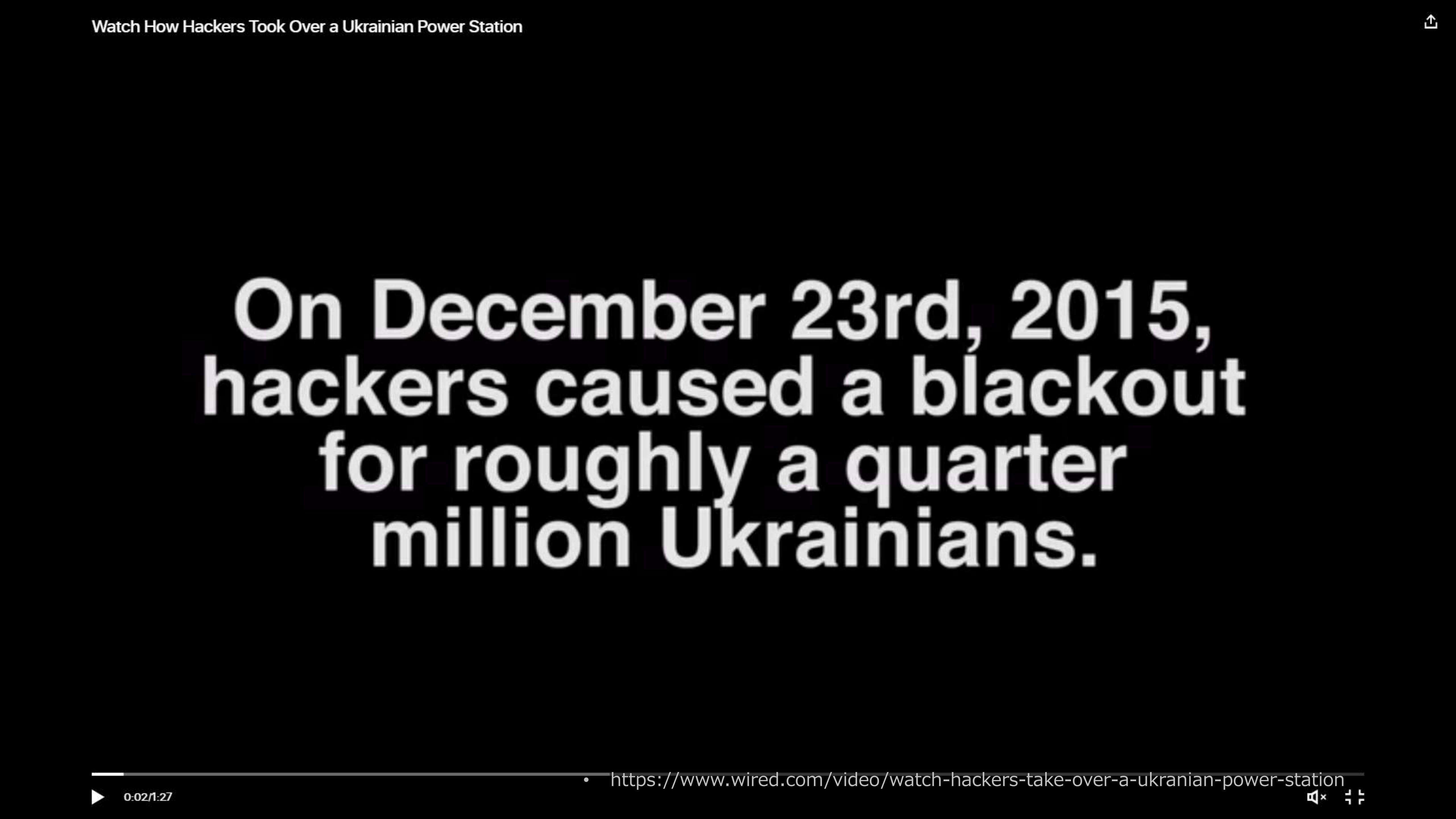
PHASE 1

- Used pre-harvested credentials to replace all relevant passwords
- Took over C&C stations
- VNC lockout

- https://cbsnews3.cbsistatic.com/hub/i/r/2016/12/22/bf532650-a9ec-49a4-8852-7d4afff7aab8/resize/620x/cba121689b9a066a7c9a862f8e2d41c1/williams-ukraine-grid-pkg-new-013.jpg

PHASE 2

- Turning off circuit breakers in sequence



Watch How Hackers Took Over a Ukrainian Power Station

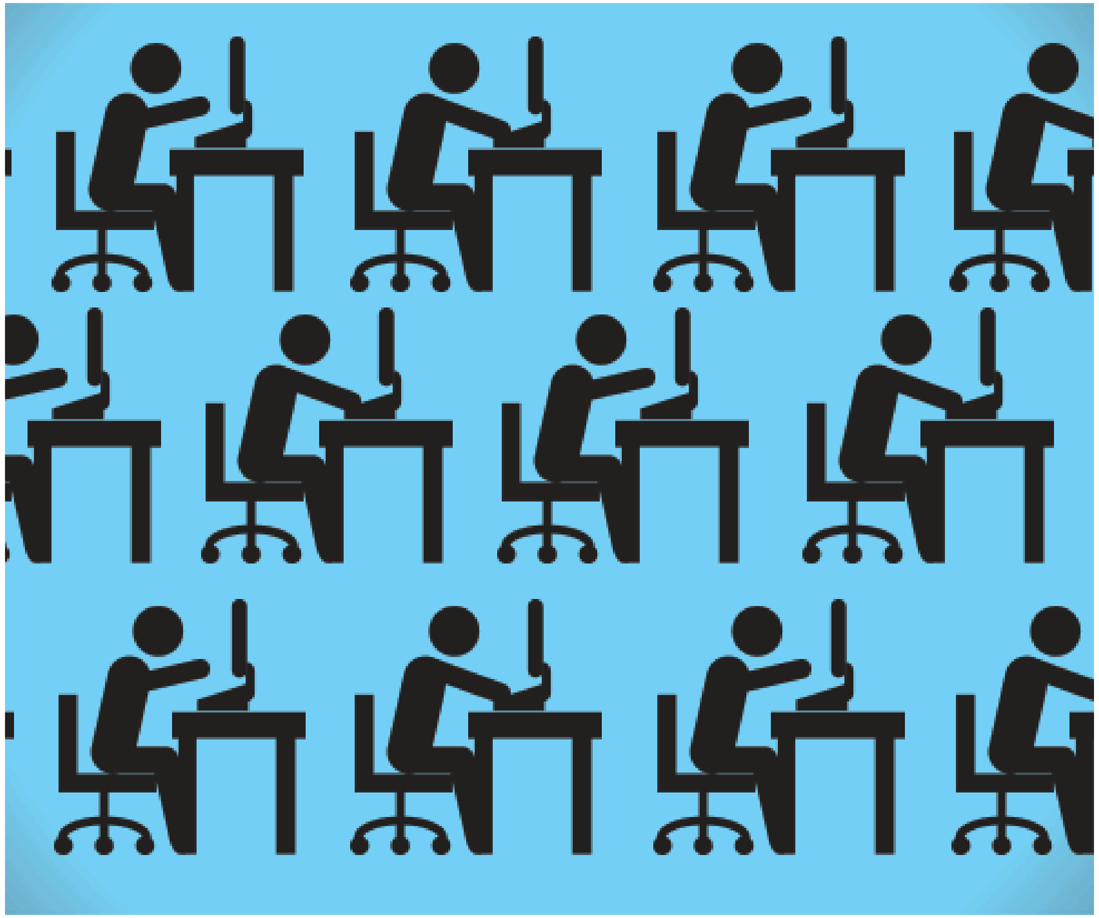
On December 23rd, 2015, hackers caused a blackout for roughly a quarter million Ukrainians.

- https://www.wired.com/video/watch-hackers-take-over-a-ukranian-power-station

Photography

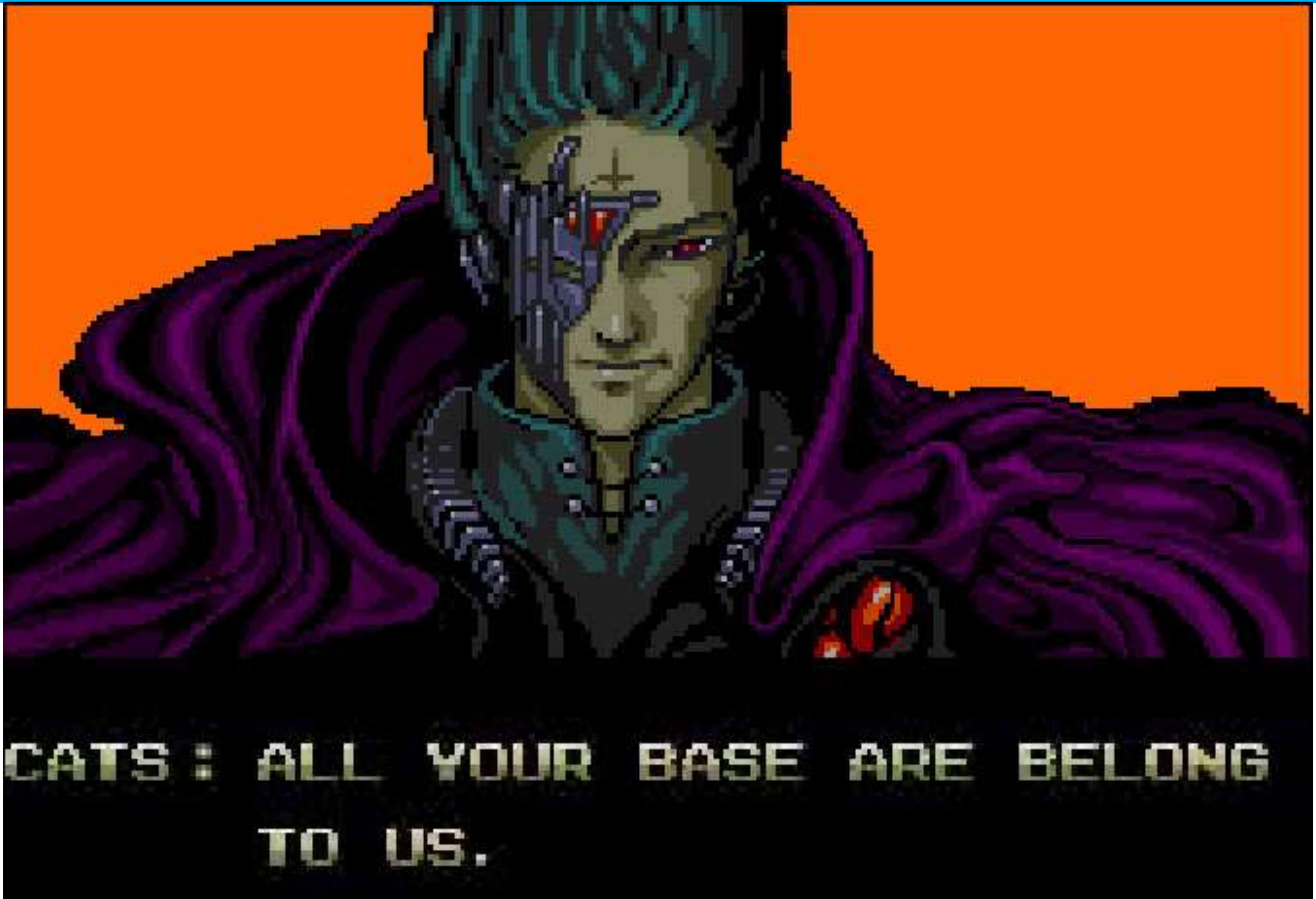
PHASE 3

- TDOS attack
- Not really against customers (as reported in the media)
- Break connection between central control (NOC) and operators at the sub-stations
- No coordinated response



- http://www.smh.com.au/cqstatic/12z7v7/oneOfmany.gif

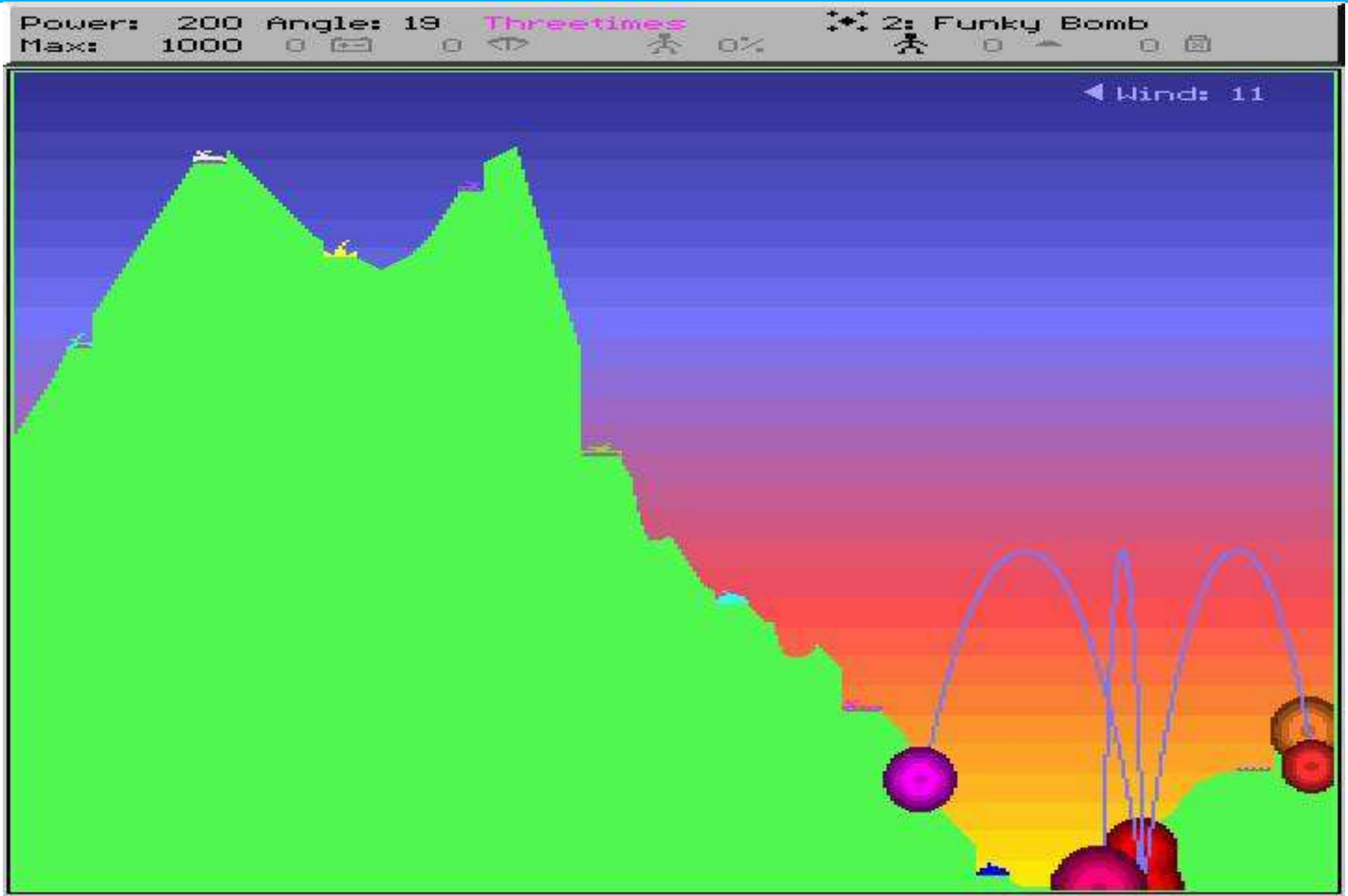
Why
Where
How
When
Where
Why
Who
?
Who
When
What
What
What
Why
When
Who
When
Where
Why
How



CATS: ALL YOUR BASE ARE BELONG TO US.

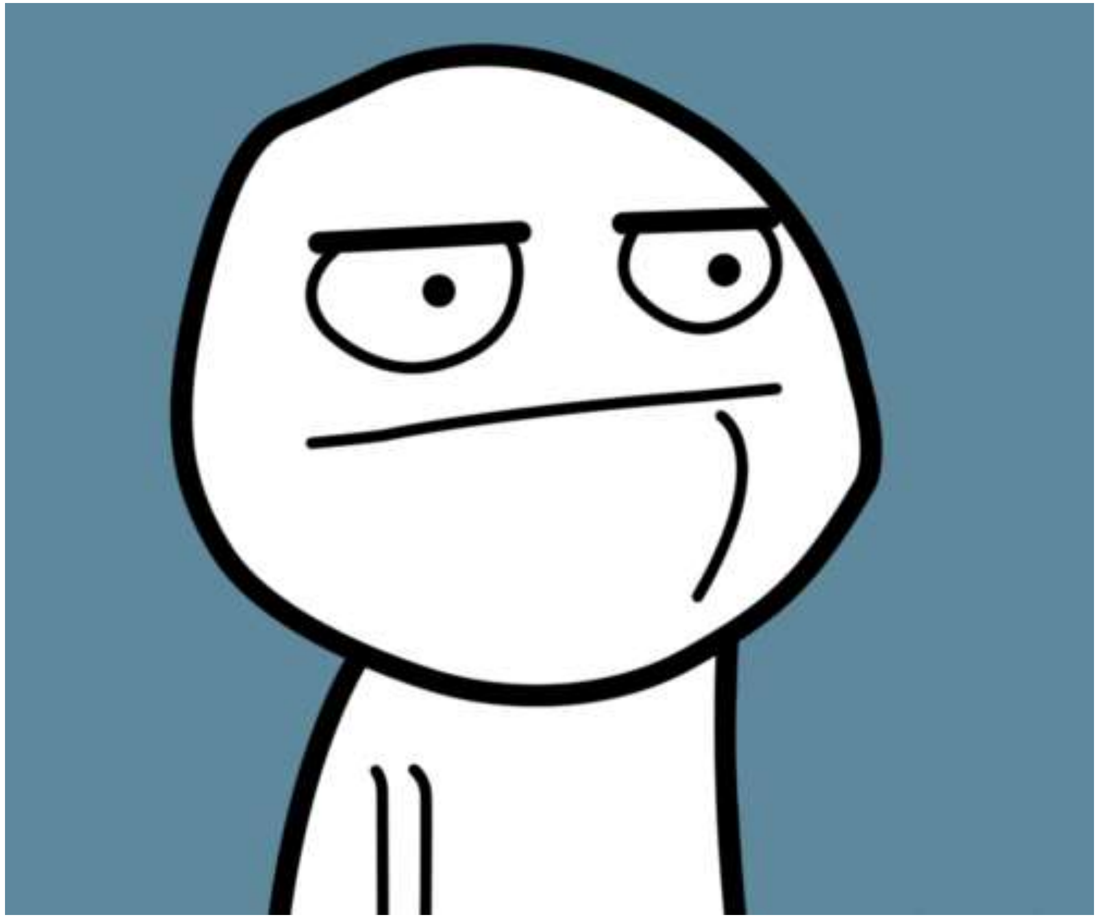
PHASE 4

- RS232/485 to Ethernet converters
  - Remote control units
- No password
- Remote firmware update


Power: 200 Angle: 19 Threetimes
Max: 1000 0 0 0% 0 0
2: Funky Bomb
Wind: 11

PHASE 5

- Remember the UPS?
- Now its turning off
- SOC has no more power
- ☺



- https://i.imgur.com/ZJD4hF8.gif

ANECDOTES

KILL SWITCH?

- The attackers knew their network better than them
- The SOC tried shutting down the routers (both of them)
- The attacker had a backup route through the ADSL backup
- The SOC didn’t know about the ADSL backup…

REGULATORS

- The Ukraine regulator was working hard on privatizing the power grid companies
- This was a major move that was supposed to happen early 2016

PHISHING, YES - PHISHING

- Around march 2015 the attackers used a government regulator mail server to phish the transmission company
- They got in through the email
- Scoped the network, hunted for credentials
- Stayed dormant for many months

REDUCED DAMAGE

- They didn’t understand the grid
- A lot of damage could have been done through deliberate shutdown of specific swtiches

STROKE OF LUCK

- The main reason the recovery was so fast was that they had a large number of skilled manual labor at hand
- Remember – they were all supposed to be fired and replaced with automation systems (yes, the pawned ones)
- Although power was recovered – the automation system was not
- The vendor didn’t have a hardened version – the best he could supply was hard coded passwords ☹

Any Questions?

@barnhartguy

- https://media.giphy.com/media/ejwFX1DPsfqec/giphy.gif