RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: **SPO3-T07**

Playing with Fire: How Cyber Physical Attacks Threaten Our Connected World

Sandra Joyce

Senior Vice President
FireEye Global Intelligence

Sandra Joyce, Senior VP, FireEye Global Intelligence

- 20 years in the U.S. Air Force Reserve
- U.S. Congress legislative aide
- Battelle Memorial Institute
- Faculty, National Intelligence University

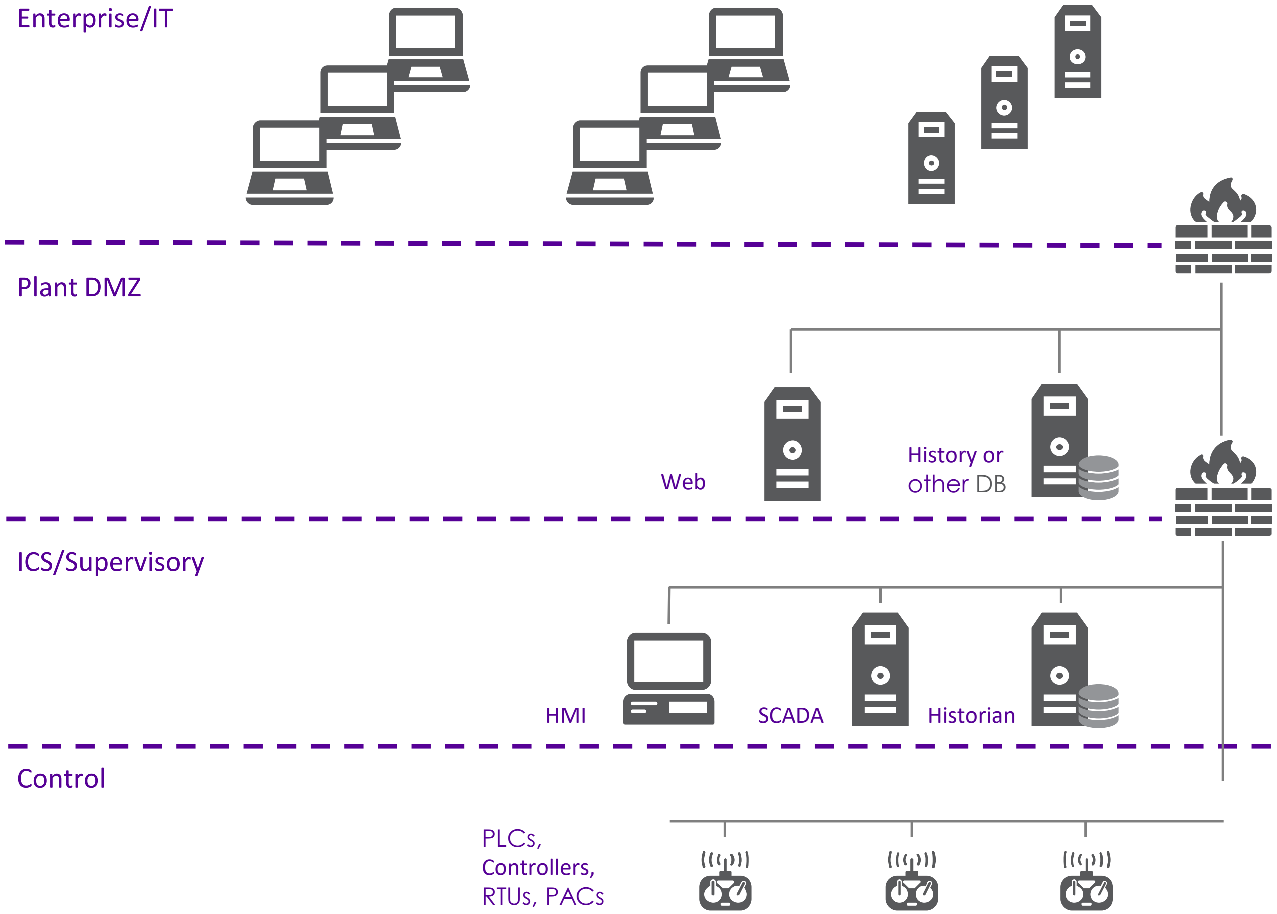
- M.A.LS. International Affairs, Georgetown University
- Master's of Military Art & Science, US Air Force
- Master's of Science and Technology Intelligence, NIU
- B.A. German, University of California, Irvine

RSA®Conference2019

Increasingly Destructive Cyber Attacks

Telangana

The Race to the Bottom



The Purdue Model

Ukrainian Attacks: Power Outage in Winter

Substation / ФСК ЕЭС

TRITON Attack Framework: Increased Sophistication

CNIIHM / Google Maps

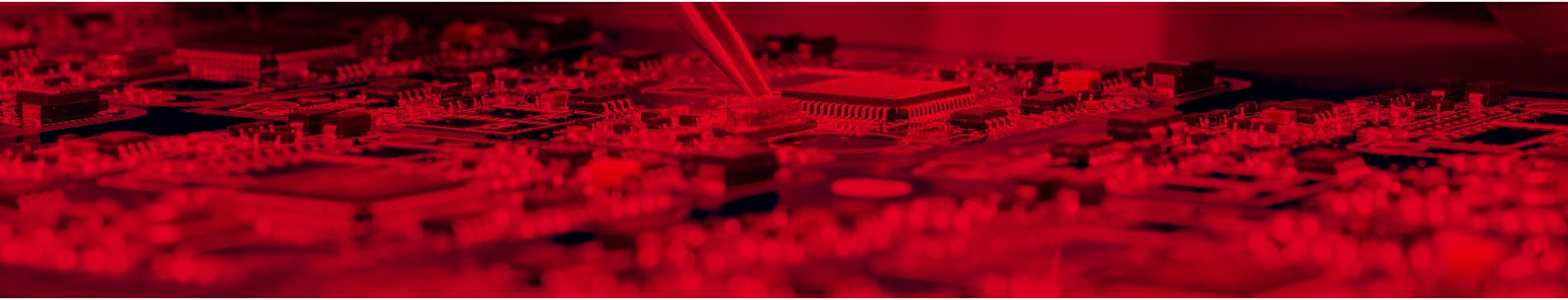
Russian NotPetya Ransomware

- Petya + supply chain compromise + wormable exploits
- Infected 65 countries, especially Ukraine
- Goal was destructive, not financial

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

North Korean WannaCry Ransomware

- Infected over 300,000 computers in 150 countries
- Cost hundreds of millions of dollars
- Attackers gained less than $150,000 from paid ransoms



RSA®Conference2019

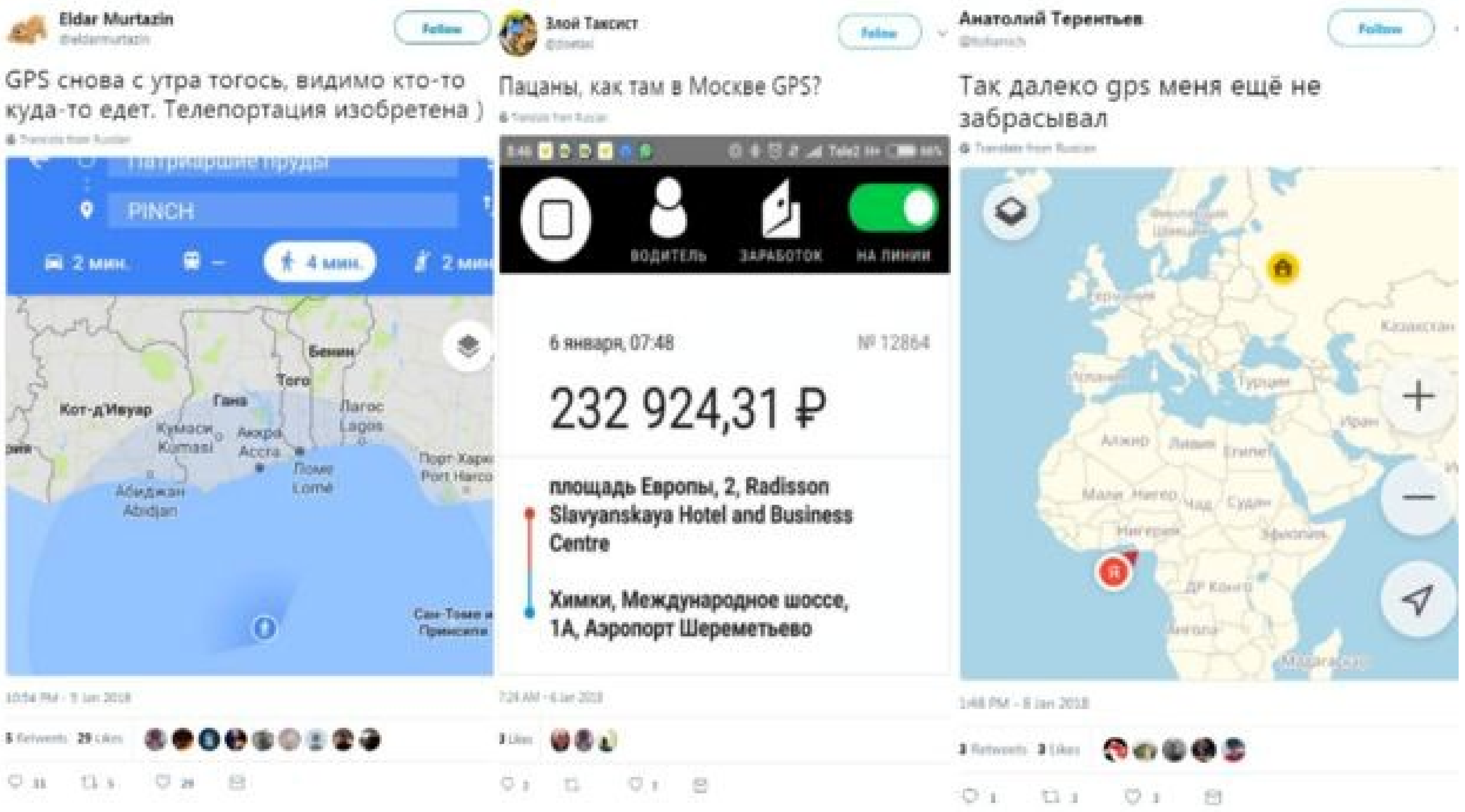
Collateral Damage

Definition

***Unintentional or incidental** injury or damage to persons or objects that would **not be lawful military targets** in the circumstances ruling at the time.*

(JP 3-60, US DoD)

$3,700 Taxi Ride Anyone?



Eldar Murtazin
@eldarmurtazin

GPS снова с утра тогось, видимо кто-то куда-то едет. Телепортация изобретена)

Translate from Russian

10:54 PM - 5 Jan 2018

5 Retweets 29 Likes

Злой Таксист

Пацаны, как там в Москве GPS?

Translate from Russian

6 января, 07:48 № 12864

232 924,31 ₽

площадь Европы, 2, Radisson Slavyanskaya Hotel and Business Centre

Химки, Международное шоссе, 1А, Аэропорт Шереметьево

7:24 AM - 6 Jan 2018

3 Likes

Анатолий Терентьев

Так далеко gps меня ещё не забрасывал

Translate from Russian

1:48 PM - 8 Jan 2018

3 Retweets 3 Likes

Screenshots depicting taxis in the wrong locations and exorbitant fares

A Week of Cold Showers

Cancer Treatment Unavailable

Darren McCollester / Getty

The Geneva Convention + LOAC Protects Civilians in Wartime

GRAVE BREACHES

- Taking of hostages
- Extensive destruction and appropriation of property
- Unlawful deportation, transfer, or confinement

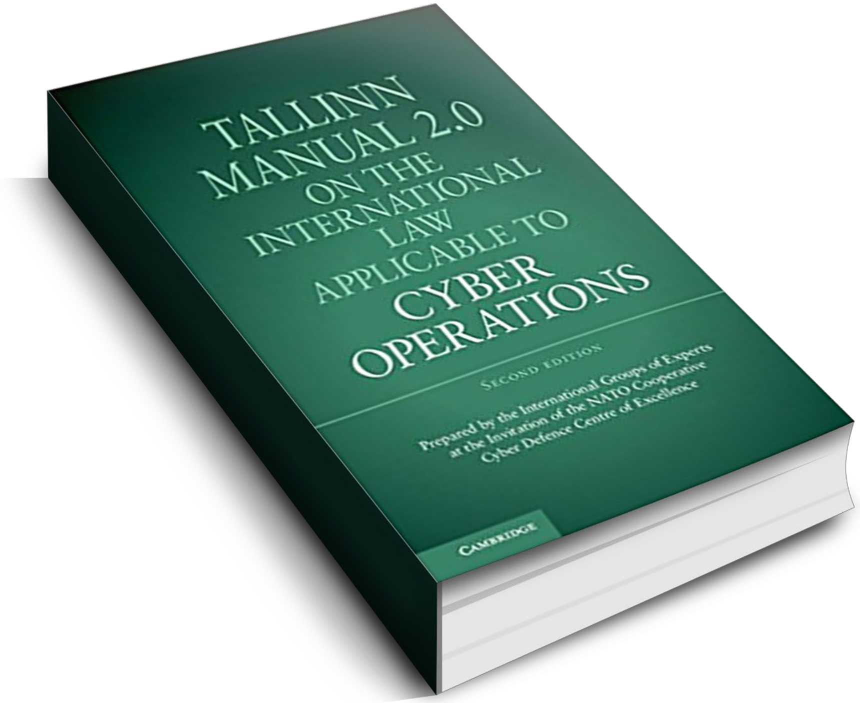
Law of Armed Conflict

- Humanity
- Military Necessity
- Proportionality

Diplomatic Conference of Geneva, 1949

Cyber Policy

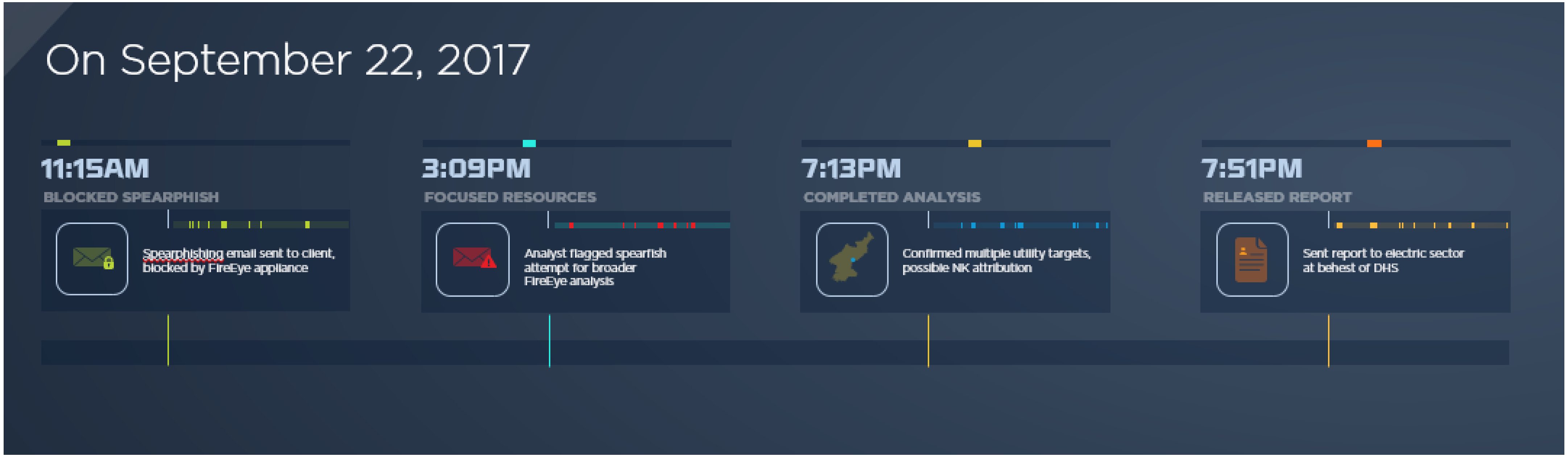
- International Law & Cyber Operations:
  - Tallinn Manual 2.0 enforceable?
- Attempts to establish norms and apply existing frameworks to the cyber domain


TALLINN MANUAL 2.0
ON THE INTERNATIONAL LAW APPLICABLE TO
CYBER OPERATIONS
SECOND EDITION
Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence
CAMBRIDGE

RSAConference2019

What Could Happen Next?

Capability, Opportunity, Intent: North Korea



On September 22, 2017

11:15AM
BLOCKED SPEARPHISH
Spearphishing email sent to client, blocked by FireEye appliance

3:09PM
FOCUSED RESOURCES
Analyst flagged spearfish attempt for broader FireEye analysis

7:13PM
COMPLETED ANALYSIS
Confirmed multiple utility targets, possible NK attribution

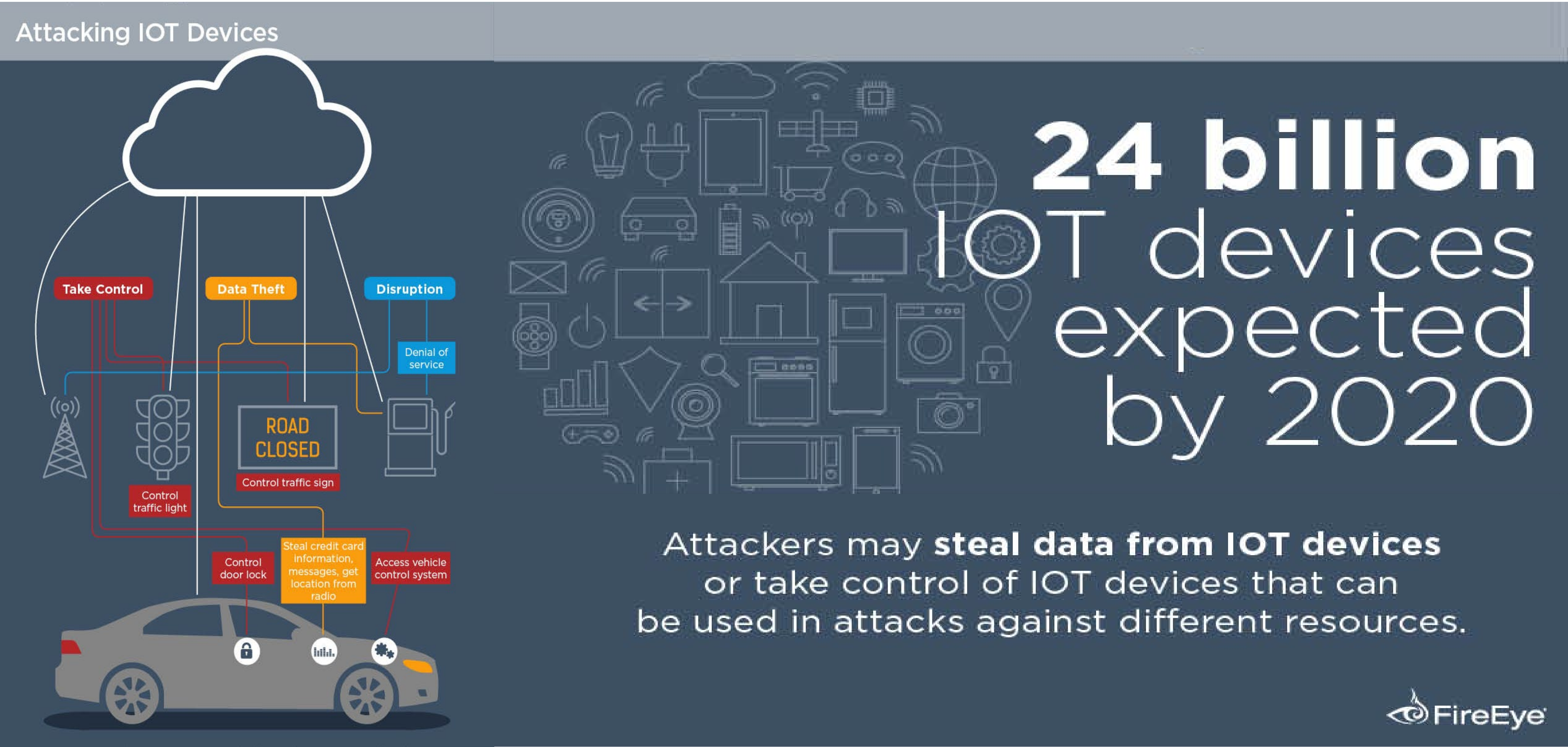
7:51PM
RELEASED REPORT
Sent report to electric sector at behest of DHS

Self-Propagating Worms

EternalBlue exploit leaked by the ShadowBrokers incorporated into:

- WannaCry
- NotPetya
- Metasploit modules

Internet of Things

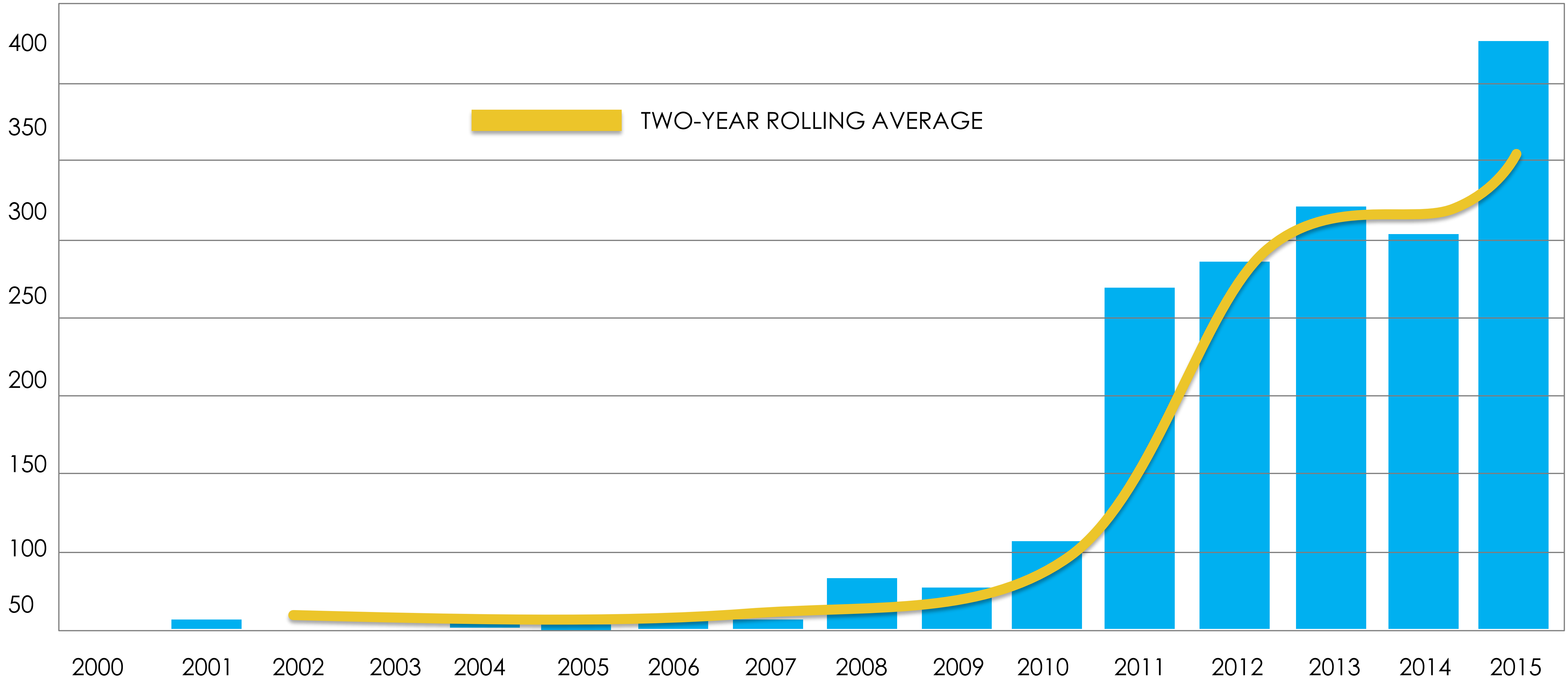


Attacking IOT Devices

24 billion IOT devices expected by 2020

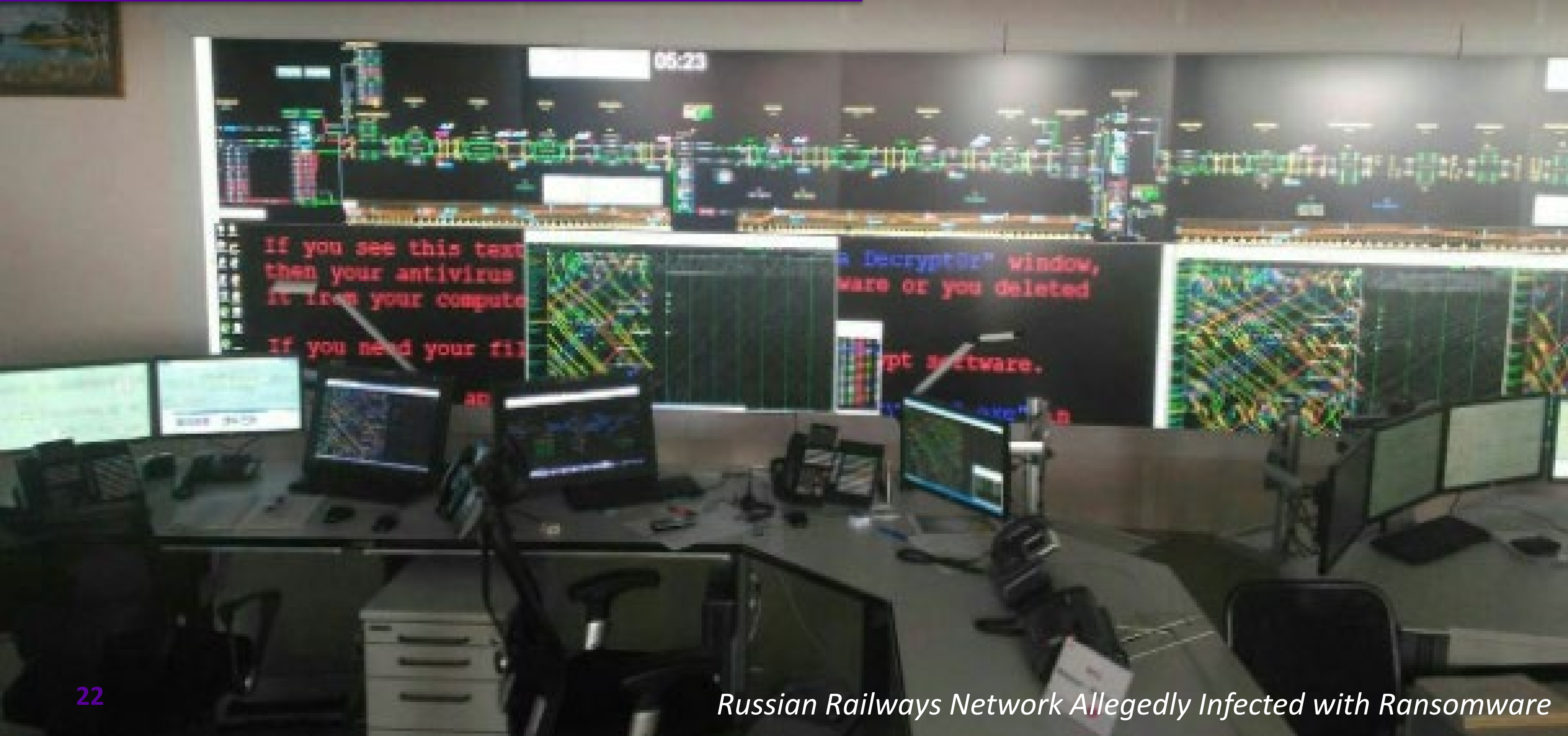
Attackers may **steal data from IOT devices** or take control of IOT devices that can be used in attacks against different resources.

Focus on ICS Vulnerabilities



ICS Vulnerability Disclosures by Year

What About Cyber Criminals?



Russian Railways Network Allegedly Infected with Ransomware

RSAConference2019

We are all on the front lines

RSA®Conference2019

Thank You