

# Cybersecurity: Attacks

1

**Paolo PRINETTO**

Director  
CINI Cybersecurity  
National Laboratory  
[Paolo.Prinetto@polito.it](mailto:Paolo.Prinetto@polito.it)  
Mob. +39 335 227529



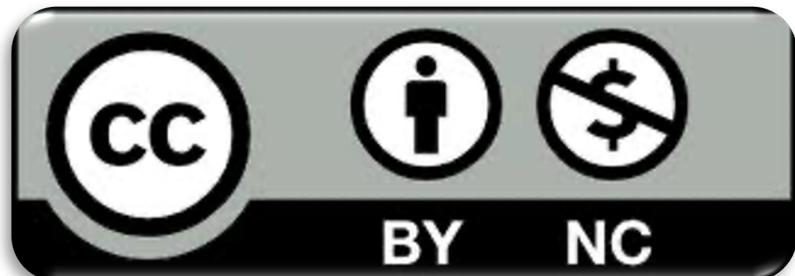
<https://cybersecnatlab.it>

# License & Disclaimer

2

## License Information

This presentation is licensed under the Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

## Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

# Acknowledgments

## Thanks

➤ The presentation includes material from several contributors, whose valuable help is here acknowledged and highly appreciated.

## Contributors

- CyberChallenge.IT
- Alessandro ARMANDO
- Roberto BALDONI
- Rocco DE NICOLA
- Arturo DI CORINTO
- Eugene KASPERSKY
- Rosario PUGLIESE
- Francesco VESTITO
- Stefano ZANERO

# Prerequisites

4

- Lecture:
  - *CS\_1.4 - Vulnerabilities*

# Goal

5

- Presenting an overview of some significant attacks to cybersecurity and a possible clusterization.

# Outline

6

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# Outline

7

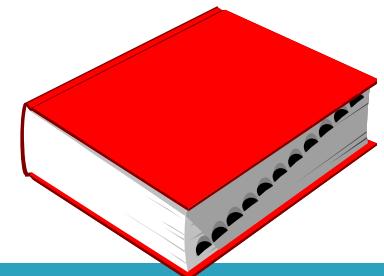
- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# Vulnerability



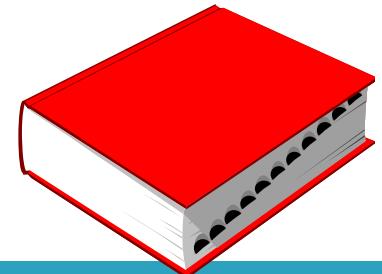
- *Particular* weakness present in a *specific* component of a system that can be *exploited* to carry out unauthorized actions to one's advantage against the Confidentiality, the Integrity or the Availability of the system assets.
- A vulnerability is such iff it is *exploitable*

# Exploit



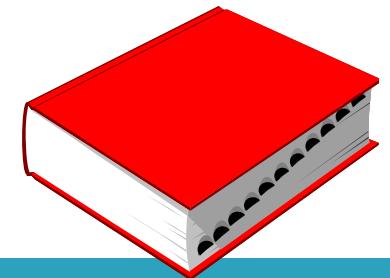
- The mean or method of taking advantage of a vulnerability for malicious purposes.

# Attack



- The act of taking advantage of a vulnerability through an exploit.

# Attack



- Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

[RFC 2828, Internet Security Glossary, May 2000]

# Caveat

12

*“Anything”  
connected to the Internet  
can be attacked ...*

*... and it will  
definitiely be ...*

*“Anything”  
connected to the Internet  
can be attacked ...*

de

Not IF,  
But WHEN ...

“ything”  
to the Internet  
attacked ...

# Everything is under attack

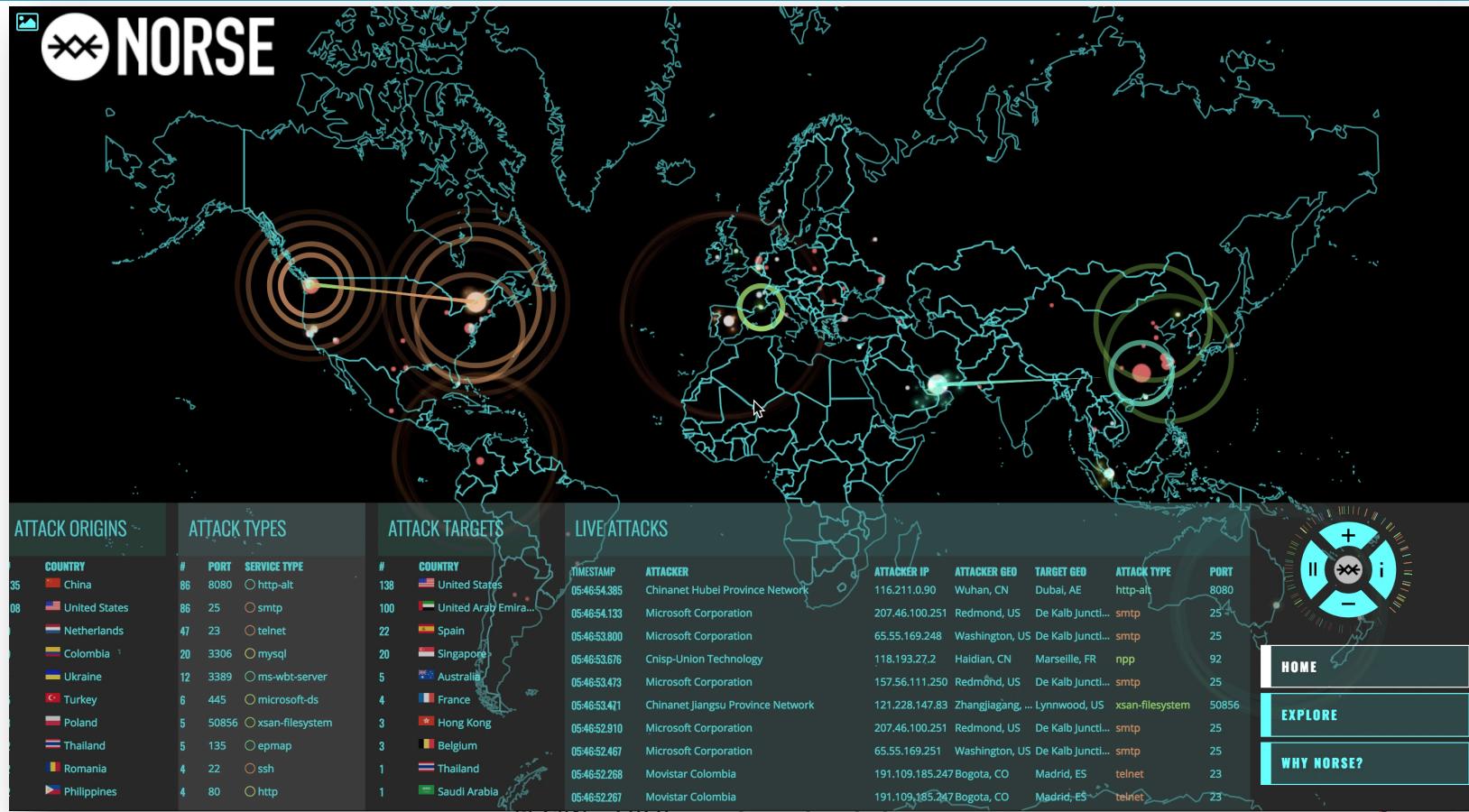
15



# ... always ...

<http://map.norsecorp.com/#/>

16



# Attack Goals

*Attacks* aim to:

# Attack Goals

*Attacks* aim to:

- Steal:
  - Data:
    - Personal, Company, State
    - Money
    - Objects
    - Identity
    - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

# Attack Goals & Clustering

*Attacks* aim to:

- Steal:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# Outline

20

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# Attack Goals & Clustering

*Attacks* aim to:

- Steal:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# Cybercrime

22

Cybercrime has been defined as such for the first time by the Committee of Ministers of the Council of Europe at the *Budapest Convention on Cybercrime* in November 2001.

# Budapest Convention on Cybercrime

23

- It states the cybercrime includes:
  - Unauthorized access
  - Unauthorized interceptions
  - Alteration of data and systems
  - Counterfeiting
  - Fraud
  - Child pornography
  - Copyright Infringement
  - ...

# Caveat

24

- Attacking a vulnerable system is considered a *criminal act*
- *Would you enter a house just because its door is open?*

# Cybercrime: where it stems from?

25

# Cyberspace: nobody's land ...

---

- In the cyberspace, social paradigms are completely different
- It is often considered *nobody's land* for the lack of clear
  - borders
  - laws

# Consequences (1)

- Great asymmetry between attack and defense (*in favor of the attack*)

# Consequences (1)

- Great asymmetry between attack and defense (*in favor of the attack*)
- Attackers share information among them in the deep web
- Defenders tend to hide attacks and to not disclose info's

# Consequences (2)

- Continuous increase in the cost / benefit ratio for the attackers:
  - it is easier and easier for them to reach the desired target, regardless of its location

# Consequences (3)

- Criminals and terrorists can do much more damage with:
  - Marginal efforts
  - relatively low risks
  - poor technological knowledges
- *Crime-as-a-Service*

# Consequences (4)

- Many new ways to:
  - Perform crimes
  - Launch attacks
  - Damage
  - Fight wars
  - Perpetrate hostile acts
  - ...

# Outline

32

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# Cybercrime: Examples

*Attacks* aim to:

- Steal:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

*JUST THE FAX, MA'AM —*

# Equifax breach exposed millions of driver's licenses, phone numbers, emails

17.6 million driver's license numbers, thousands of ID images stolen in breach.

SEAN GALLAGHER - 5/8/2018, 5:13 PM

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motori | Tutte le sezioni ▾ D Rep tv

f 5 | Twitter | g+ | in | Email

# Hackerata la catena di hotel Marriott: a rischio i dati di 500 milioni di clienti



(reuters)

*La compagnia ha annunciato di aver subito un attacco informatico ai suoi database. Potenzialmente coinvolti mezzo miliardo di utenti che hanno soggiornato negli alberghi del gruppo dal 2014 a oggi*



THE INTERNET OF HACKABLE THINGS

# Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings



LORENZO FRANCESCHI-BICCHIERAI  
Feb 27 2017, 10:00pm

A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

**UPDATE, Feb. 28, 12:25 p.m. ET:** After this story was published, a security researcher revealed that the stuffed animals themselves could easily be hacked

The image shows a composite of two screenshots. On the left, a screenshot of the Ashley Madison website homepage is displayed. The site features a black header with the text "ASHLEY MADISON" in large white letters, followed by the tagline "Life is short. Have an affair." Below this is a search bar with placeholder text "Get started by telling us your interests now!" and a pink button labeled "SEE MATCHES". A banner at the bottom of the page states "Over 37,000,000 anonymous members". On the right side of the composite, there is a close-up photograph of a woman's face. She has her finger to her lips, suggesting silence or a secret. She has long dark hair and is wearing a ring on her finger.

**READ MORE**

## Ashley Madison hack reveals its 37 million users sexual fantasies

# Rubate le mail a 1,4 milioni di utenti Libero e Virgilio

Il cybercriminale, uno studente di 24 anni, si è intrufolato nella rete Wi-Fi del gestore (Italiaonline) operando da un bar vicino alla sede dell'azienda (Assago, Milano). I carabinieri l'hanno fermato dopo che aveva già spedito il pacchetto di credenziali mail al committente

# Cybercrime: Examples

*Attacks* aim to:

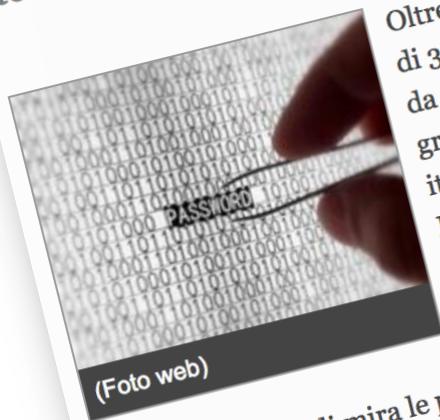
- Steal:
  - Data:
    - Personal, Company, State
    - Money
    - Objects
    - Identity
    - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

SICUREZZA INFORMATICA

# Hacker rubano 36 milioni di euro sui conti di 30 banche europee via sms

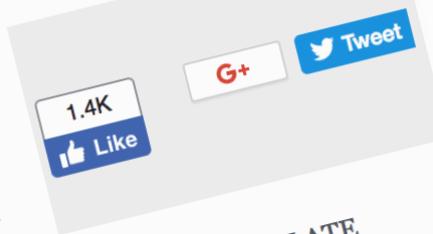
Colpiti anche clienti italiani. L'attacco attraverso un trojan dormiente sui Pc che si è trasferito sugli smartphone



Oltre 36 milioni di euro, sui conti di 30 banche europee. Una cifra da capogiro. Rubata da un gruppo di hacker anche di clienti italiani. A darne notizia è stato il Financial Times nell'edizione online, rilevando che si tratterebbe del primo caso di furto che ha preso

sui servizi

specificatamente di mira le procedure di sicurezza sui servizi



## NOTIZIE CORRELATE

- L'attacco di Apple: «Android è a rischio» (22/01/2014)

## 4 Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

"Sposta subito mezzo milione su questo conto estero". Ma la mail era di un hacker. E i soldi sono spariti. Il finto ordine a firma della direttrice Panucci: "Esegui e non mi chiamare che sto fuori col presidente"

di ROBERTO MANIA

Lo leggo dopo | 30 settembre 2017



Gianfranco Dell'Alba

contraffatte (mail spoofing, le chiamano gli esperti del settore) da cui partono ordini per spostare denaro in ogni parte del mondo.

ROMA - Ci sono circa cinquecentomila euro che da un conto della Confindustria sono finiti in un conto estero di cui ancora non si conosce l'intestatario. Soldi evaporati, per ora. C'è una mail falsa da cui è cominciato tutto. C'è un dirigente dell'associazione degli industriali licenziato in tronco per un bonifico che non avrebbe dovuto fare. È successo in Confindustria ma sono centinaia le aziende colpite ogni giorno da frodi finanziarie e milioni le mail

## Hacker truffa con una mail falsa un dirigente di Confindustria: spariti 500mila euro

"Sposta subito mezzo milione su questo conto estero". Il finto ordine a firma della direttrice Marcella Panucci, ad eseguire il bonifico il dirigente livornese Gianfranco Dell'Alba

TRUFFE CONFININDUSTRIA HACKER

30 settembre 2017

# ADVANCED CROSS-BORDER FINANCIAL CYBERCRIME

## CARBANAK – THE \$1 BILLION BANK HEIST

Infecting bank clerks' computers

Harvesting intelligence

Controlling admin computers

Stealing money

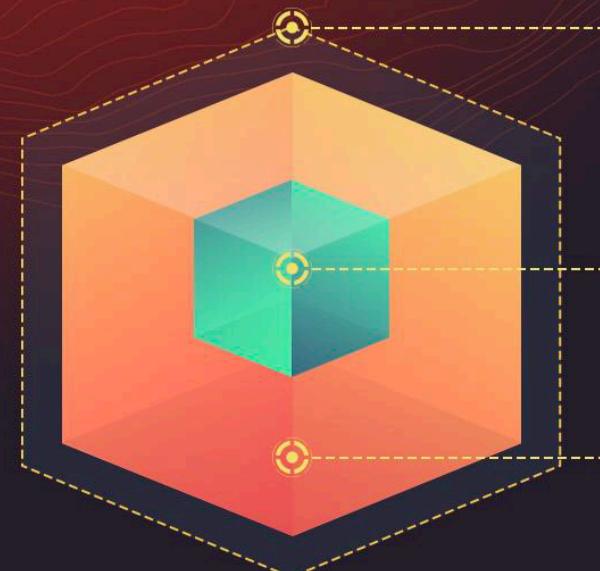


## BANGLADESH CENTRAL BANK HEIST

35 transfer orders to the New York Federal Reserve

Four orders, \$81M Stolen, still missing

31 orders, \$870M Blocked because of word 'Fandation'



[E. Kaspersky, 2018]

# Cybercrime: Examples

*Attacks* aim to:

- Steal:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# Crime-as-a-Service

44

TRADITIONAL AND ONLINE  
CRIME GROUPS ARE NOW WORKING TOGETHER



[E. Kaspersky, 2018] mal Lab

# Surveillance Camera Attack

- A massive Distributed Denial of Service (DDoS) attack slowed down major websites
  - Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, and The New York Times
- Target: Dyn (a major DNS host)
- Attack: a weakness in surveillance cameras, that allowed installing malicious software in more than 25,000 cameras!



# Automotive attacks

Upstream

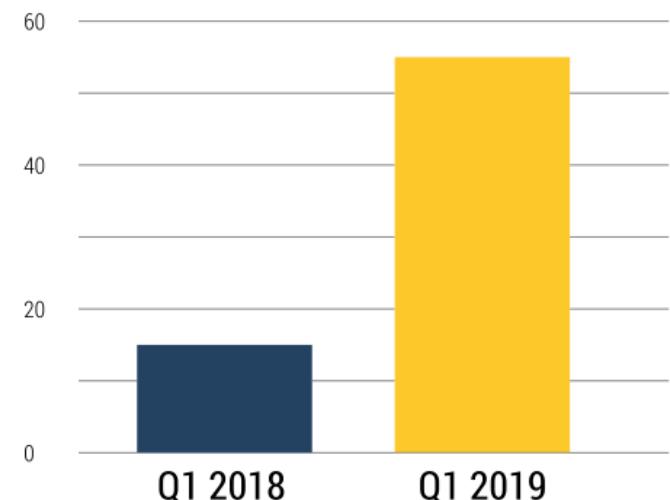
Q1 2019 SEES RAPID GROWTH OF  
AUTOMOTIVE CYBER INCIDENTS

# Automotive attacks

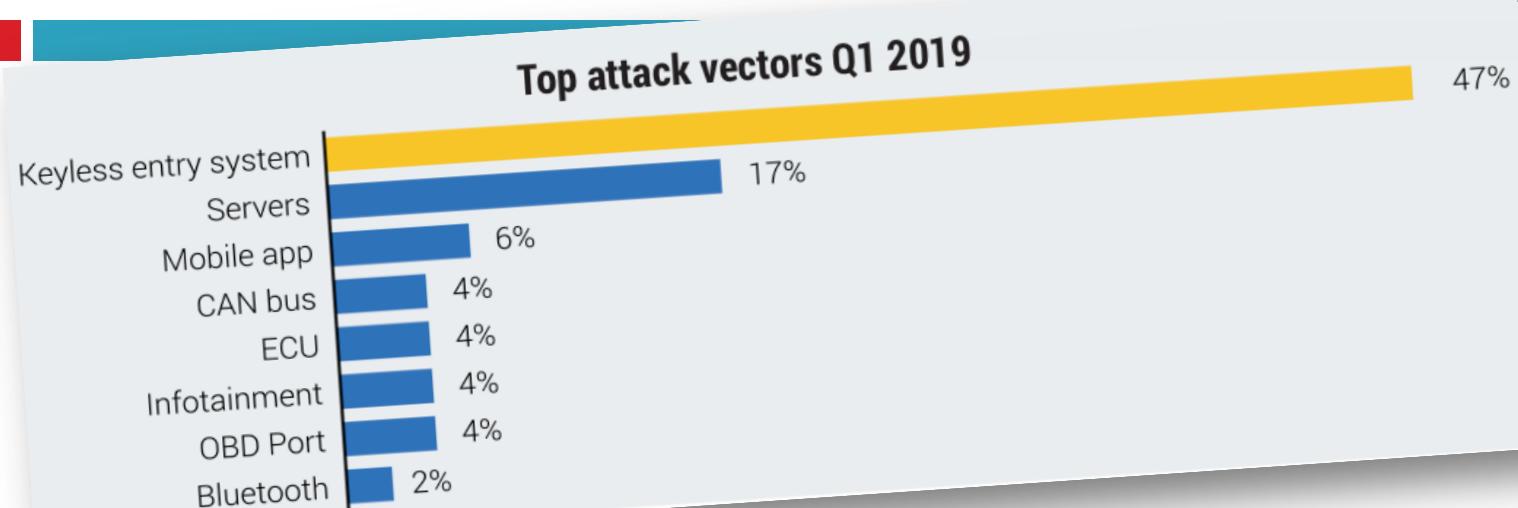
Upstream

Q1 2019 SEES RAPID GROWTH OF  
AUTOMOTIVE CYBER INCIDENTS

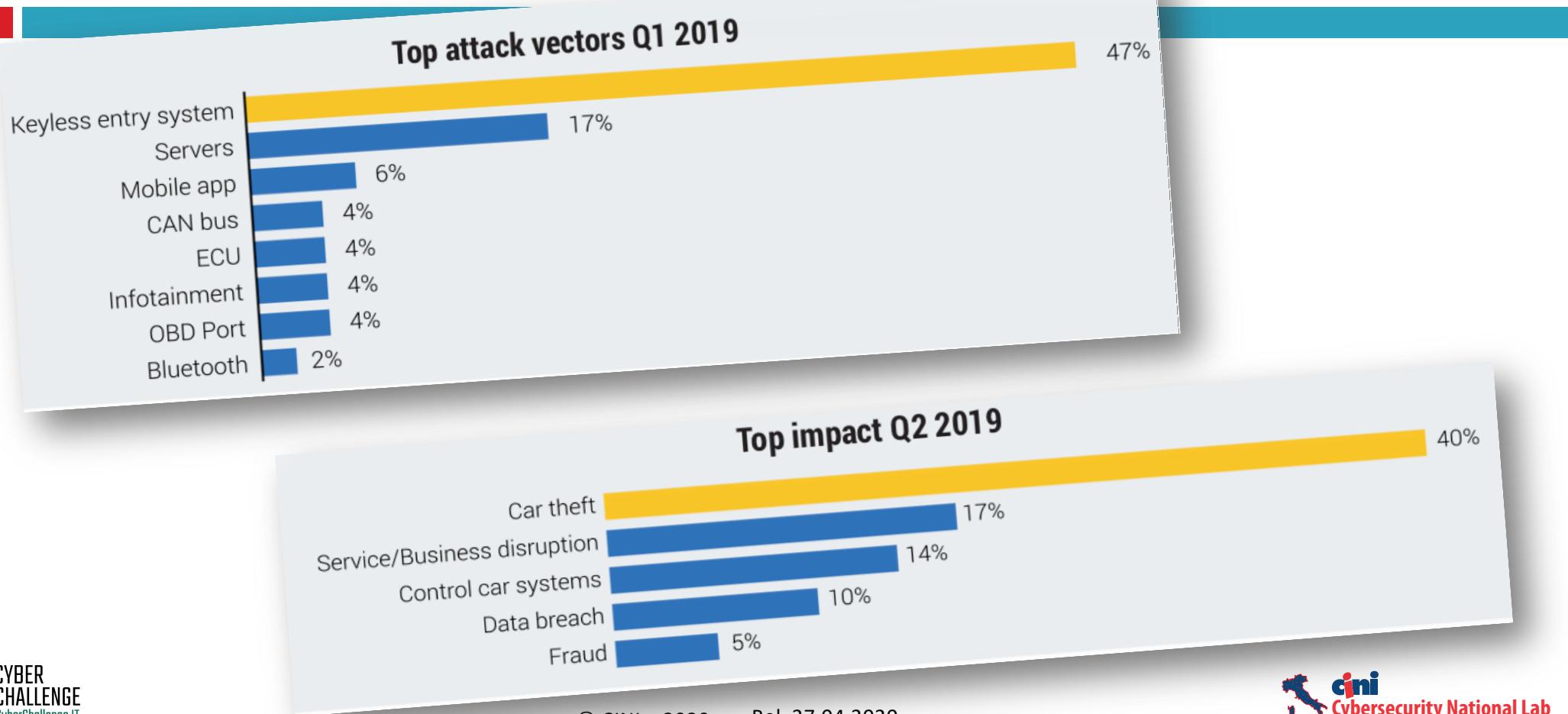
Total incidents Q1 18 vs Q1 19



# Automotive attacks



# Automotive attacks



# Cybercrime: Examples

*Attacks* aim to:

- Steal:
  - Data:
    - Personal, Company, State
    - Money
    - Objects
    - Identity
    - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# Attacco DDoS Contro Dyn DNS, giù twitter, spotify, github, heroku e altri.

I Cyber attacchi si fanno sempre più frequenti e rappresentano giorno per giorno una grave minaccia per le compagnie IT.





## PRIVACY AND SECURITY FANATIC

By Ms. Smith, Network World | FEB 12, 2017 8:15 AM PT

# University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.

### About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

## Hacking link to USS McCain warship collision? Expert says 'I don't believe in coincidence'

THE collision of a second US warship this year that has left 10 sailors missing points to an expert has warned.



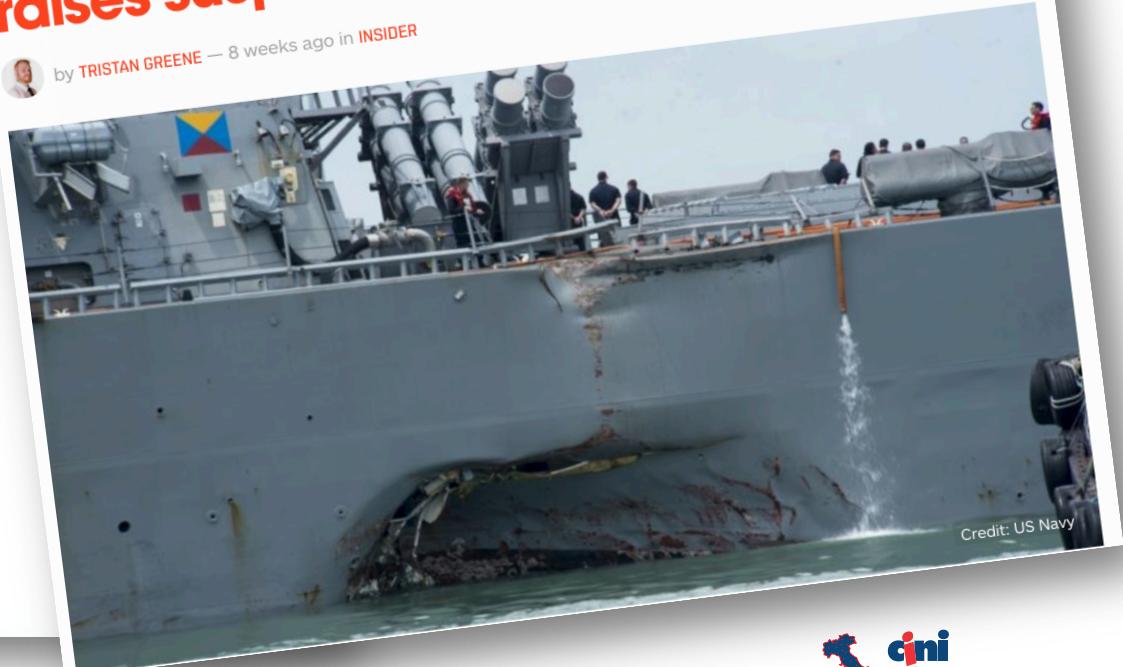
Charis Chang [@CharisChang2](#)



**Fourth US Navy collision this year raises suspicion of cyber-attacks**



by TRISTAN GREENE — 8 weeks ago in INSIDER



LA COMUNICAZIONE

Ascolta

# IoT security, 350 mila pacemaker a rischio attacchi informatici negli USA

*Intervento della Food and drug administration: batterie scarse e bassi livelli di cybersecurity. Solo l'anno passato sono state individuate oltre 8.000 vulnerabilità su sette diversi apparecchi.*

di Flavio Fabbri | @FabbriFlav2 | 8 maggio 2018, ore 12:21

# Outline

55

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# Cybercrime costs

56

The image shows a news article from CNBC. At the top, there's a navigation bar with categories: CYBERSECURITY (in large letters), TECH, MOBILE, SOCIAL MEDIA, ENTERPRISE, CYBERSECURITY (in red), and TECH GU. Below the navigation bar, the main headline reads "Cybercrime costs the global economy \$450 billion". Underneath the headline, the author is listed as "Luke Graham | @LukeWGraham" and the publication date is "Published 10:00 AM ET Tue, 7 Feb 2017". The NBC logo (CNBC) is visible at the bottom left of the article area.

CYBERSECURITY

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GU

## Cybercrime costs the global economy \$450 billion

Luke Graham | @LukeWGraham  
Published 10:00 AM ET Tue, 7 Feb 2017

CNBC

# Cybercrime costs

57

CYBERSECURITY

TECH | MOBILE

SOCIAL MEDIA

ENTERPRISE

CYBERSECURITY

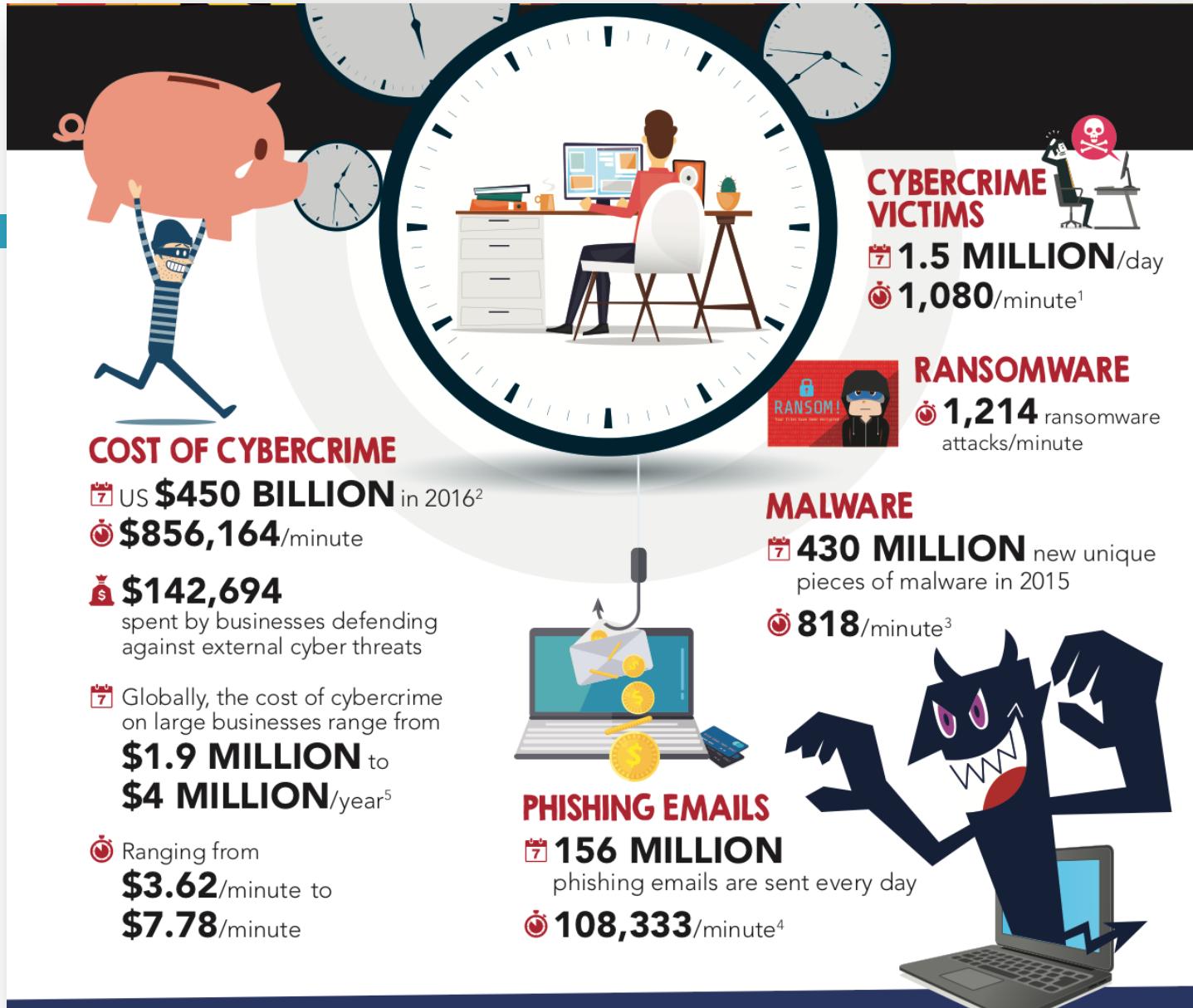
TECH GU

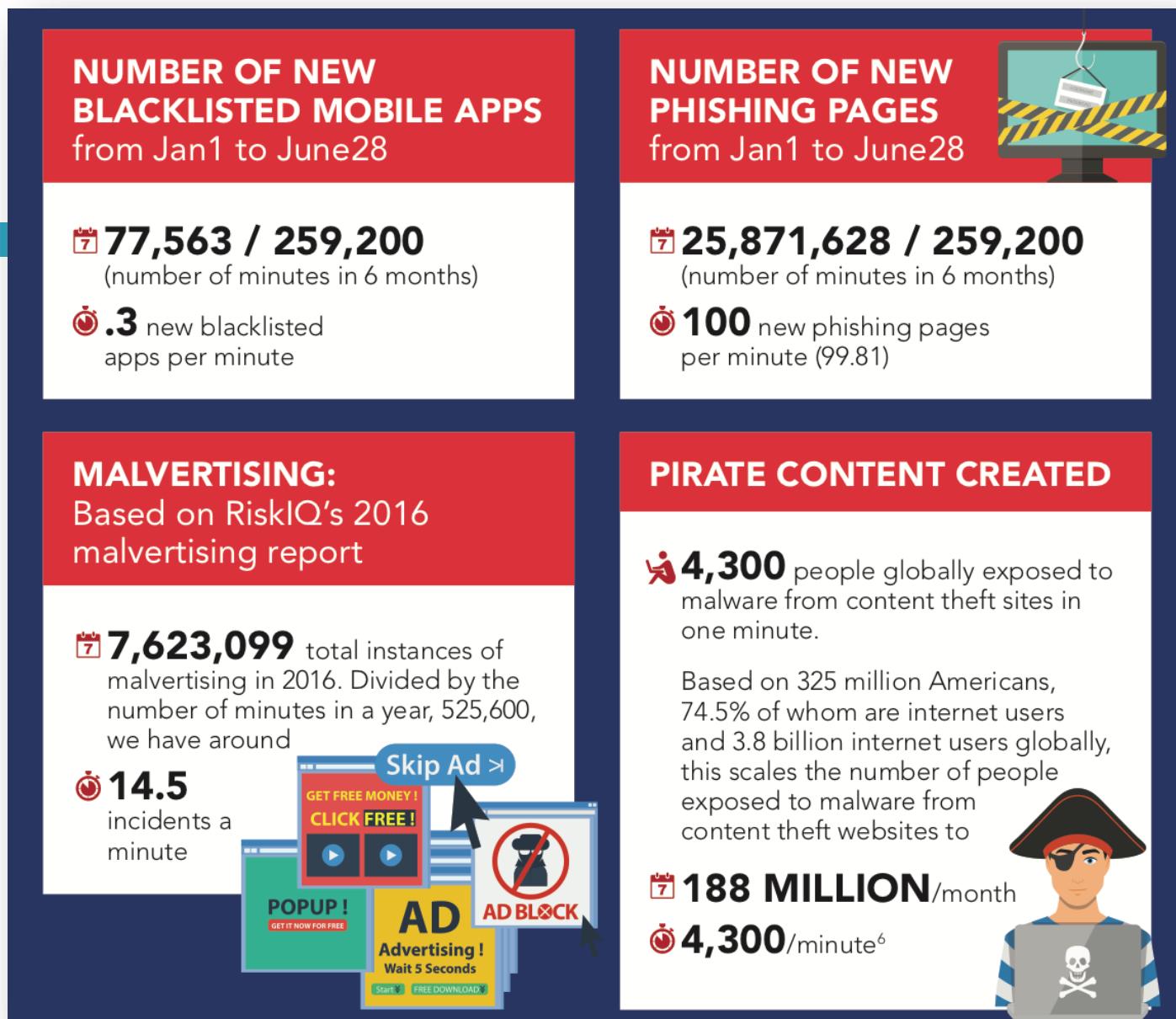
Cybercrime costs the global economy \$450 billion

Luke Graham | @LukeWGraham  
Published 10:00 AM ET Tue, 7 Feb 2017



Austria GDP (Gross Domestic Product) in 2017:  
\$434 billion





# Cybercrime vs. space

60



[E. Kaspersky, 2018] tional Lab

# Cybercrime vs. space

61



# Outline

62

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# Cyber-espionage

*Attacks* aim to:

- Get:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# Cyber-espionage ??



# Cyber-espionage ??



Liaoning CV 16



USS TRUMAN

# Outline

66

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

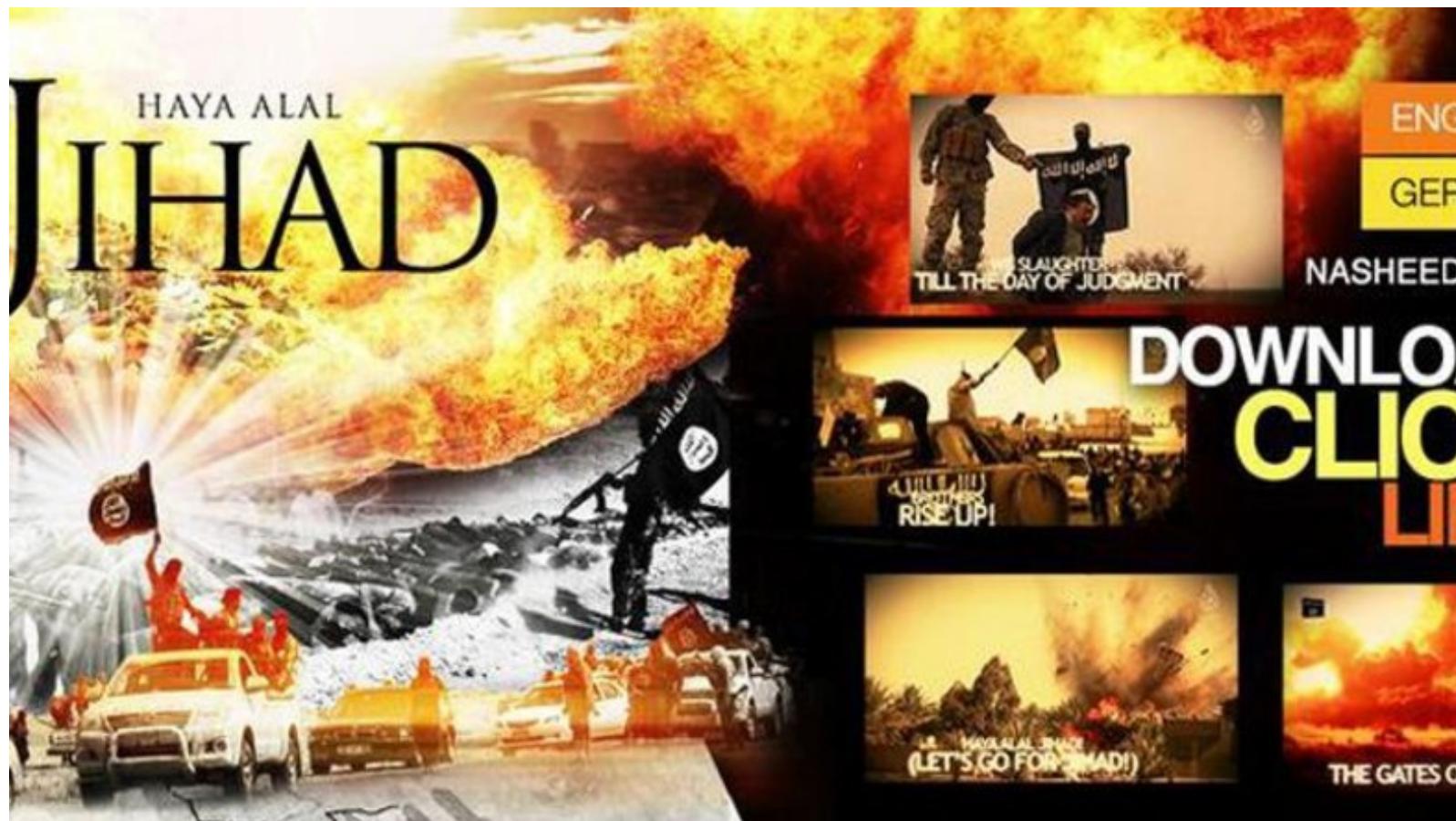
# Cyber-terrorism

*Attacks* aim to:

- Get:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# CYBER-JIHAD



# Outline

69

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- **Cyber-warfare**
- Conclusions

# Cyber-warfare

*Attacks* aim to:

- Get:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

# The 4<sup>th</sup> domain

71

- In 2016, during the Warsaw summit, NATO officially elevated cyberspace to the rank of “*operations domain*” together with *land*, *sea*, and *air*

# CEMA (Cyber ElectroMagnetic Activities)

- Use the electromagnetic spectrum to have cyber effects
- Example:
  - how to inoculate malware in radars not through networks but waves (software-defined radio)
  - attackers can turn off or spy on radar not with viruses in systems, but through electromagnetism

- It is no longer the world where the vulnerability of networks is the result above all of the ingenuity of human beings.
- The so-called *air-gap* to get into the networks without entering the networks themselves is overcome.
- There will be military aircraft with ISR platforms capable of doing all this remotely, analyzing the information that passes via Wi-Fi

[Francesco Vestito - comandante del CIOC - Comando Interforze per le Operazioni Cibernetiche]

# Cyber-warfare: Examples

*Attacks* aim to:

- Get:
  - Data:
    - Personal, Company, State
  - Money
  - Objects
  - Identity
  - Roles
- Damage
- Control in a malicious way:
  - Structures
  - Services
  - Whole nations

- Depending on authors and goals, threat is classified in:
  - *Cybercrime* (es: fraud, identity theft, etc.)
  - *Cyber-espionage* (unauthorized data acquisition)
  - *Cyber-terrorism* (with ideological connotation)
  - *Cyber-warfare* (operation planning and conducting)

New: Security researchers say Triton, a powerful malware that once tried to blow up a Saudi chemical plant, has been found in a second facility.



#### A powerful malware that tried to blow up a Saudi plant strikes again

A highly capable malware reportedly used in a failed plot to blow up a Saudi petrochemical plant has now been linked to a second compromised facility. FireEy...

[techcrunch.com](https://techcrunch.com)

## 6 SEPTEMBER 2007: ORCHARD OPERATION



weapon called *Suter*.

*Suter* it is a computer system that, through sensors, can identify the source of electromagnetic waves, for example a radar, understand what type of transmitter it has in front of it and send signals that can confuse the transmitter or even infect it with viruses.

*Suter* according to various sources, it is an American system developed by BAE Systems and integrated on some unmanned aircraft.

There are several versions of *Suter*, the most basic allows you to understand what they see the opposing radars, the second version allows you to take control of the enemy network and control the sensors, the third version allows you to take control of sensors and actuators connected, or weapon systems . All this is achieved "simply" by injecting the ad hoc built code.

These systems are used by the US at least from the 2006 and have been deployed in Iraq, Syria and Afghanistan.

What Israel has used *Suter* or something similar created by its laboratories does not matter, what is interesting to note is that very probably for at least ten years there are technologies capable of reducing the radar to impotence.

(To Alessandro Rugolo) 09/09/18 - In the 2007 in Italy we just heard of *cyber*. Someone dared to write their thesis trying to illustrate the meaning of terms like *cyberspace*, *cyberdefence*, *cyberattack*, but without proving great public success. Yet the rest of the world went on.

Israel in the meantime hit a nuclear installation in Syria with the use of the Air Force ...

The night of the 6 September at least 4 F-16I *Sufa* and 4 F-15I *Ra'am* they crossed the border with Syria towards the nuclear installation near the city of Deir ez-Zor.

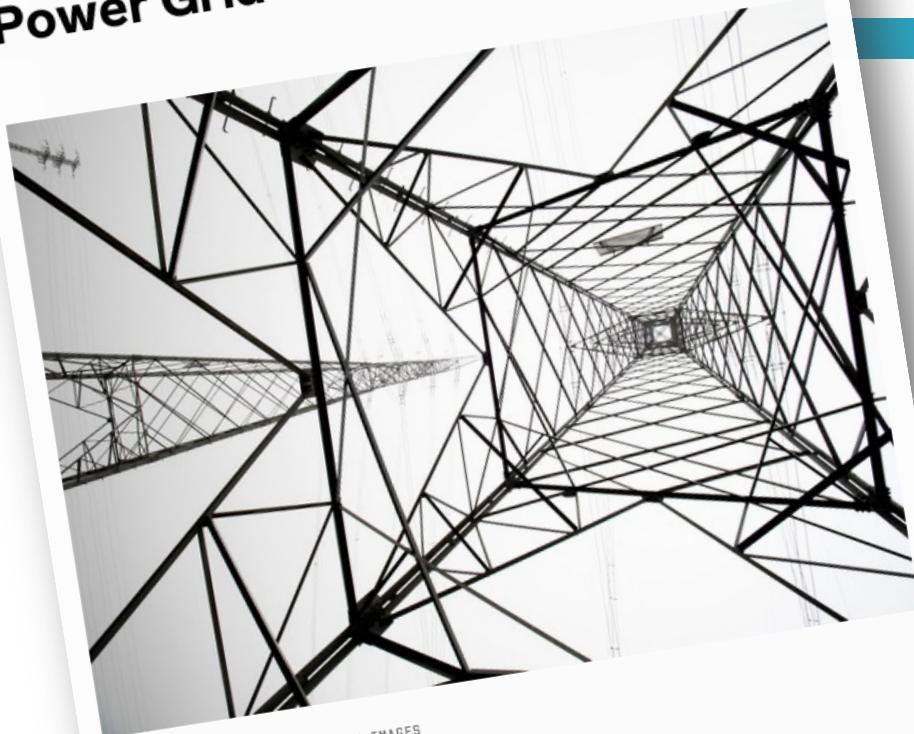
The aircraft carried out their mission and all returned to the base without the Syrian anti-aircraft defenses noticing: the radars were blind and the anti-aircraft defenses did not come into operation, although they were very advanced Russian systems (Pantsir S1).

The success of the mission has always been attributed to the great skill of the Israeli pilots and to the great work of the Israeli electronic war, and yet with time the truth has emerged: the mission has succeeded thanks to the use of a cyber

# 2015, Dec. 23<sup>rd</sup>

77

## Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



© JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their

# La rete elettrica in Ucraina è stata attaccata da degli hacker

Gli hacker hanno attaccato anche i centri telefonici cercando di impedire ai clienti di notificare alle compagnie le interruzioni di corrente.

Booz | Allen | Hamilton

# WHEN THE LIGHTS WENT OUT

A COMPREHENSIVE REVIEW OF THE 2015 ATTACKS  
ON UKRAINIAN CRITICAL INFRASTRUCTURE

CONSULTING | ANALYTICS | SYSTEMS DELIVERY | ENGINEERING | CYBER



Industrial  
Control  
Systems



**E-ISAC**  
ELECTRICITY  
INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

## Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

1325 G Street NW  
Suite 600

Washington, DC 20005

404-446-9780 #2 | [www.eisac.com](http://www.eisac.com)

**e-gazette.it**  
Notiziario ambiente energia on-line dal 1999

## CYBERATTACCO, UN VIRUS INFORMATICO PROVOCÀ BLACKOUT IN UCRAINA

KIEV (UCRAINA) LUN, 11/01/2016

✉️ 📧 ★ f t in + 1

Grazie a un documento Excel infetto, il 23 dicembre scorso 700mila persone sono rimaste al buio per diverse ore

Il tanto temuto blackout provocato da attacco informatico alle centrali elettriche è arrivato. Il primo vero salto di qualità nelle minacce hacker ad impianti elettrici è avvenuto il 23 dicembre scorso, ai danni della rete elettrica ucraina nel Nord-Ovest del Paese: lo ha reso noto l'azienda di sicurezza informatica Eset, sottolineando come si tratti del primo caso del genere al mondo. Secondo Eset, il virus responsabile dell'attacco è stato infiltrato nel sistema grazie a un documento Excel infetto: si tratta di un programma denominato "BlackEnergy", contenente a sua volta un eseguibile, "KillDisk", in grado di sabotare le funzionalità dei sistemi industriali, spesso assai vulnerabili.

Nel capoluogo della regione Ivano/Frankivsk sono rimasti senza luce circa 700mila persone. L'interruzione della corrente - leggiamo su International Business Time - è durata circa sei ore. "Se questo è veramente il primo attacco riuscito contro impianti elettrici, credo che un sacco di persone lo interpreteranno come il passaggio del Rubicone" ha detto Jason Healy, esperto di conflitti informatici e ricercatore senior presso la Columbia University's School of International and Public Affairs di New York. "Non c'è dubbio che il rischio aumenta ogni anno e che tali attacchi saranno sempre più comuni."

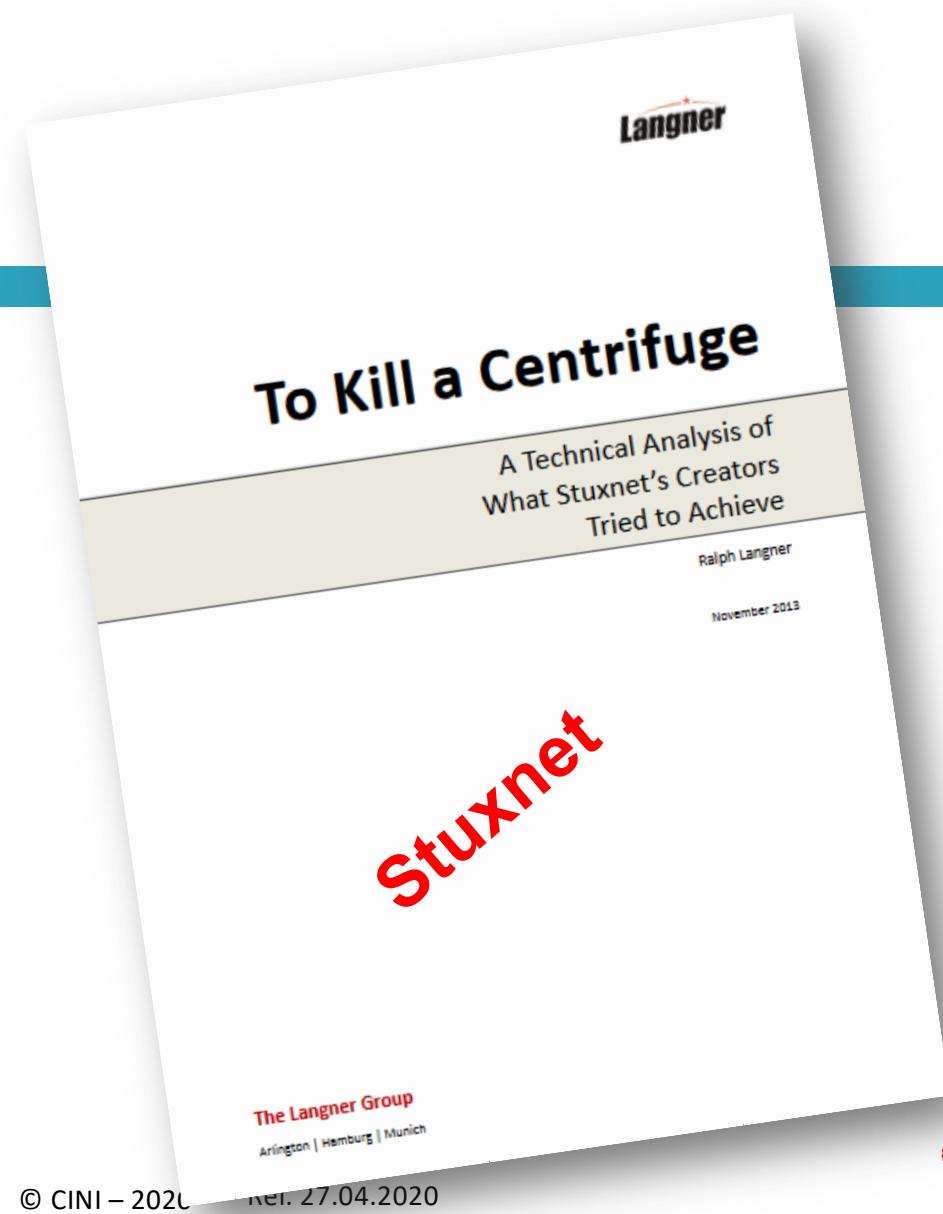
I funzionari ucraini hanno aperto un'inchiesta su quell'evento ed alcuni studi recenti sottolineano che l'attacco avrebbe colpito almeno altre due utility in Ucraina occidentale. Secondo le spiegazioni fornite dai tecnici, BlackEnergy esiste da circa un decennio e in passato è stato utilizzato per attacchi hacker da parte del gruppo Sandworm, con sede a Mosca e vicino al governo russo.

Nonostante l'esistenza di responsabilità provate e circostanziate c'è una certa titubanza nell'attribuire la colpa a un partito politico. Un istruttore certificato di sicurezza informatica sostiene che occorrono più analisi per poter giungere ad una conclusione, soprattutto perché si tratta di infrastrutture civili fuori dalle zone del conflitto. Tuttavia, come alcuni stati utilizzano l'informatica per spiarsi l'un l'altro, gli stessi potrebbero arrivare a trovarsi in posizioni scomode nell'ammettere le azioni di spionaggio.



# Stuxnet

81



# Stuxnet

- In an article in The New York Times of June 1, 2012, White House policy expert David E. Sanger writes an article in which he anticipates the news that President Obama has ordered a cyber-attack on Iran.
- According to Sanger's reconstruction, some European states and some Israeli officers were also involved in the operation, the weapon used is Stuxnet



[<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>]

# From cyber to physical

- The attack was carried out with the **Stuxnet worm** which went from a Windows system to the **SCADA** controllers (Supervisory Control And Data Acquisition) used for the electronic monitoring of an Iranian nuclear power plant.
- The worm managed to change **the speed of the rotors** in a centrifuge of the Iranian plant used to enrich uranium.
- The compromise was possible thanks to **social engineering** activities and other techniques so as not to be discovered (when the rotor had warmed up the malware continued to send messages to the operations center confirming that everything was ok)

# Trump secretly ordered cyber attacks against Iran missile systems

June 23, 2019 By [Pierluigi Paganini](#)

The United States launched a series of cyber attacks on Iran after the Iranian military has downed an American surveillance drone.

The military response to Iran, after the Iranian army has downed an American surveillance drone, started from the cyberspace.

US President Donald Trump first approved military strikes against Iran in retaliation for downing a surveillance drone, [but pulled back from launching them](#) on Thursday night after a day of escalating tensions.

# State-sponsored cyberattacks

85

CYBERSECURITY

## Today's enterprises face increasing risk of state-sponsored cyberattacks

Brian Ulicny Vice President, Thomson Reuters Labs

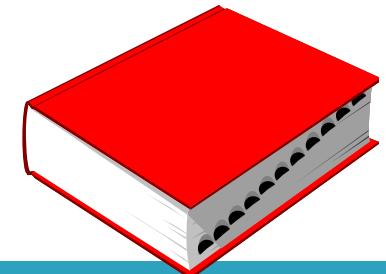
14 Jan 2019

© CINI – 2020 Rel. 27.04.2020

[Share](#)

**cini**  
Cybersecurity National Lab

# Hybrid warfare



86

- *Hybrid warfare* is a military strategy which employs political warfare and blends conventional warfare, irregular warfare and *cyberwarfare* with other influencing methods, such as fake news, diplomacy, lawfare and foreign electoral intervention.

# Cyber attacks in *Hybrid warfare*

87

- Why Cyber attacks in *Hybrid warfares*:
  - favorable cost-effectiveness ratio;
  - "below the threshold" of military response;
  - absence of geographical boundaries and attribution difficulties.

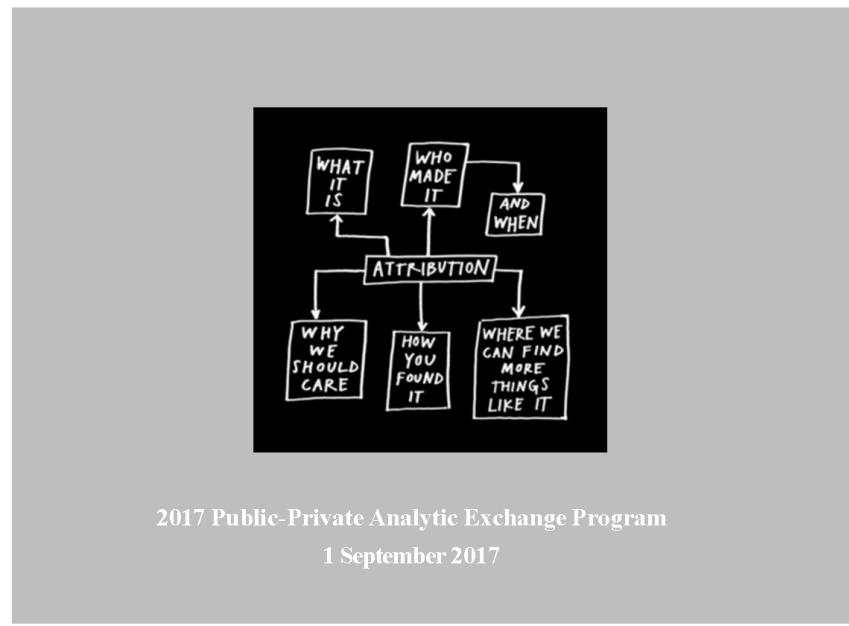
# The issue of attribution

88

- “Most sophisticated and exhaustive approaches to attribution are often outside the means of most companies, and from the perspective of the government or its intelligence organizations, is usually classified or sensitive.”



## PHASE II - CYBER ATTRIBUTION USING UNCLASSIFIED DATA



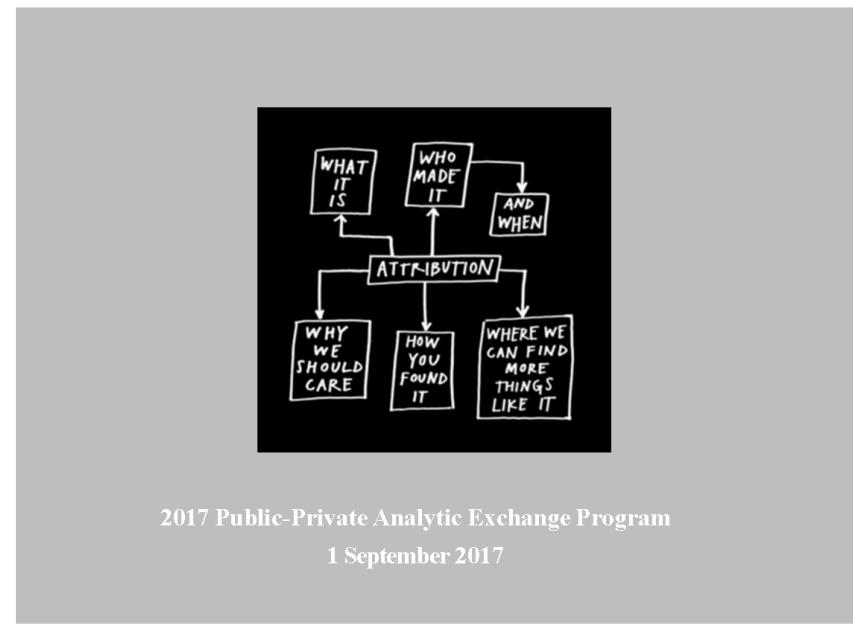
# The issue of attribution

89

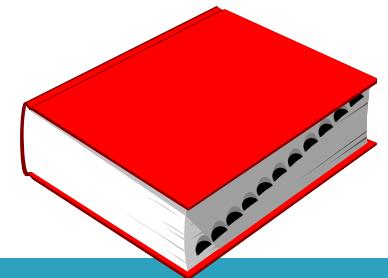
- This leaves private enterprise in a difficult position when it is targeted by state actors. They may fail to anticipate being targeted and lack the ability to respond when they are.



## PHASE II - CYBER ATTRIBUTION USING UNCLASSIFIED DATA



# Deterrence



- Prevention of an action through a credible threat of retaliation with consequences of unacceptable size for the attacker and/or through operations that lead to the belief that the cost of the action exceeds the perceived benefits.

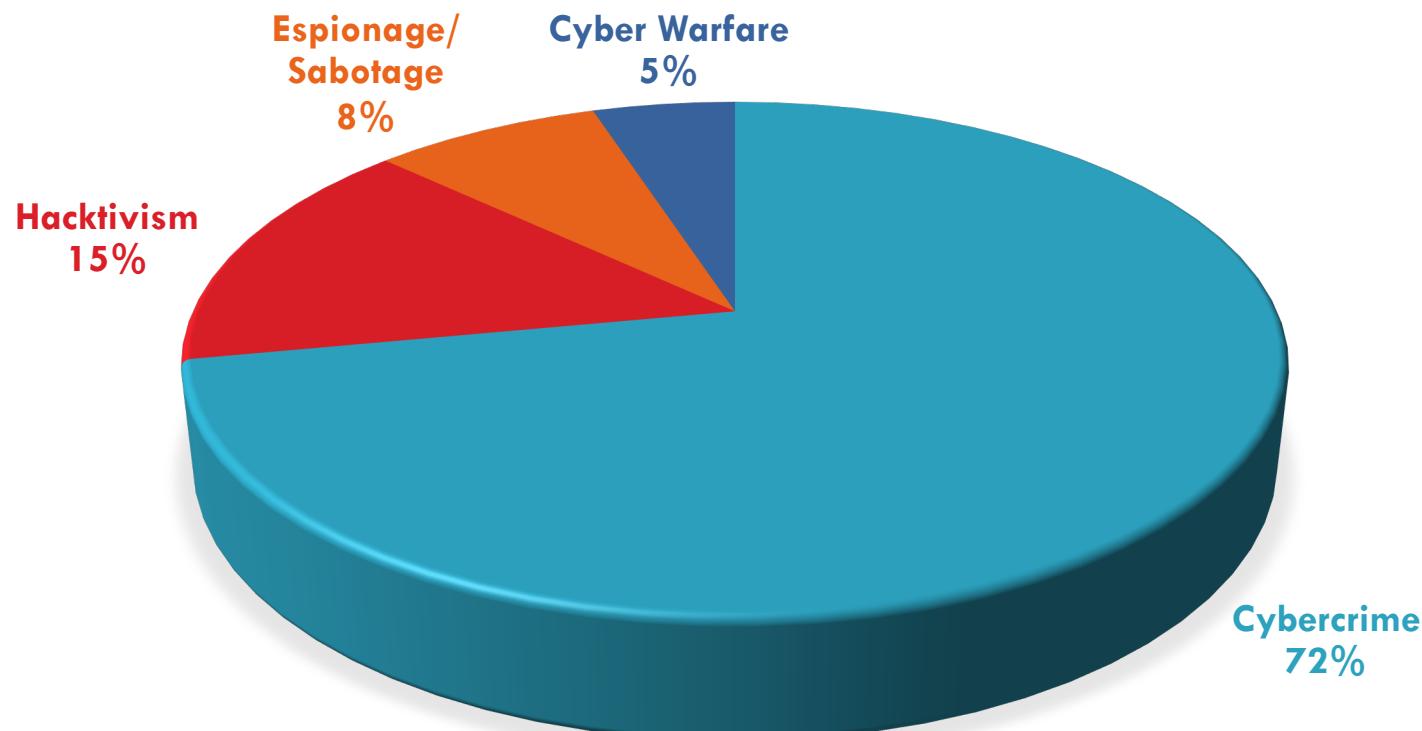
# Outline

91

- Attacks
- Cybercrime:
  - Motivations
  - Examples
  - Costs
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusions

# THREAT ANALYSIS

## TYPES AND DISTRIBUTION OF ATTACKERS - 2016



[Francesco Vestito - comandante del CIOC - Comando Interforze per le Operazioni Cibernetiche]

# Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*

# Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*
- Insufficient knowledge of system
- Not highly sophisticated equipment
- Look for existing weaknesses

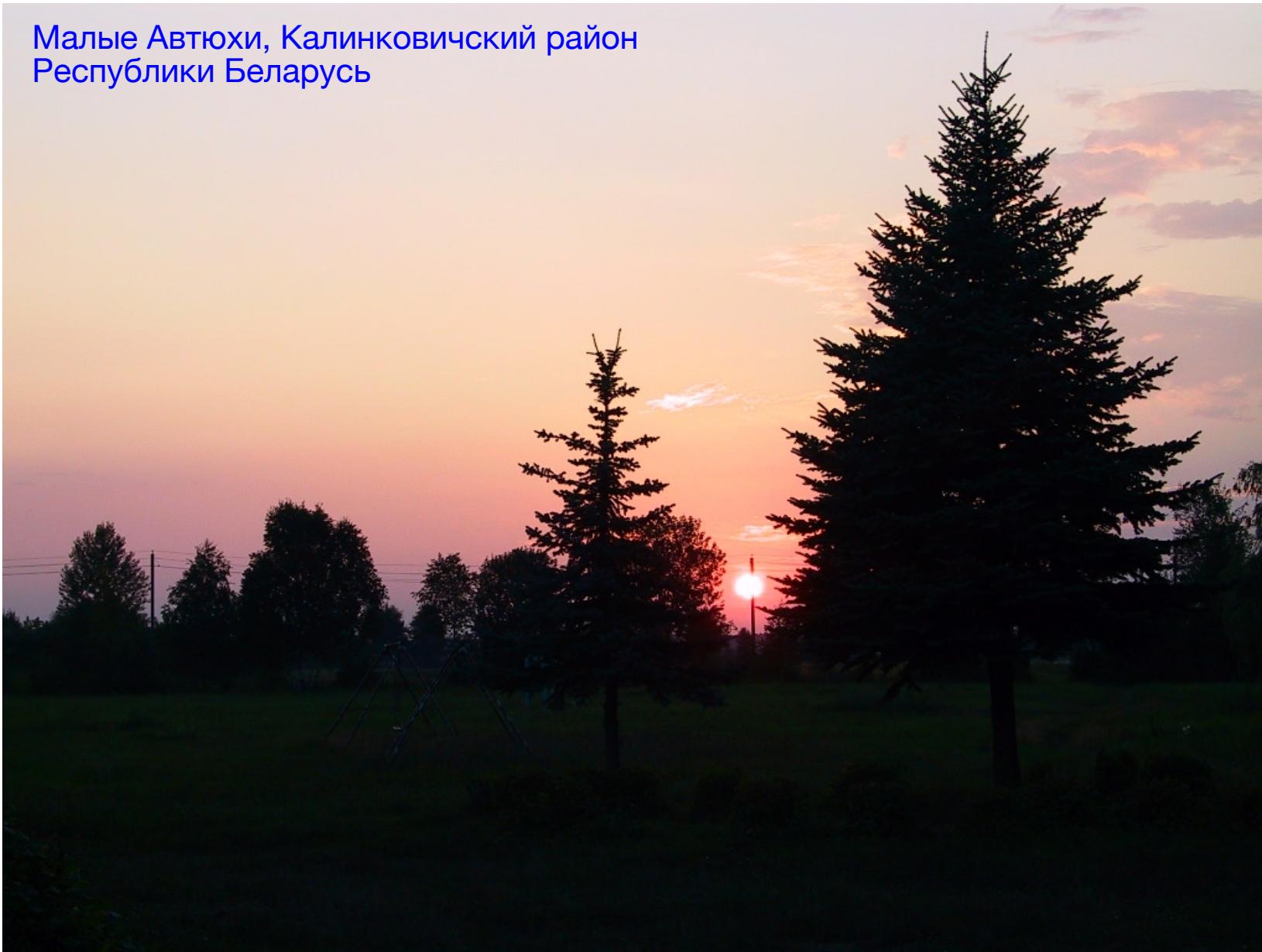
# Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*
- Have potential access to
  - most parts of the system
  - highly sophisticated tools

# Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*
- Governments, terrorists, mafia
- They resort to
  - teams of experts
  - big budgets
  - most advanced tools

Малые Автюхи, Калинковичский район  
Республики Беларусь



## Paolo PRINETTO

Director  
CINI Cybersecurity  
National Laboratory  
[Paolo.Prinetto@polito.it](mailto:Paolo.Prinetto@polito.it)  
Mob. +39 335 227529



<https://cybersecnatlab.it>