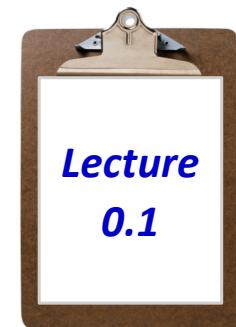


# Relevance & Costs

1

**Paolo PRINETTO**

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



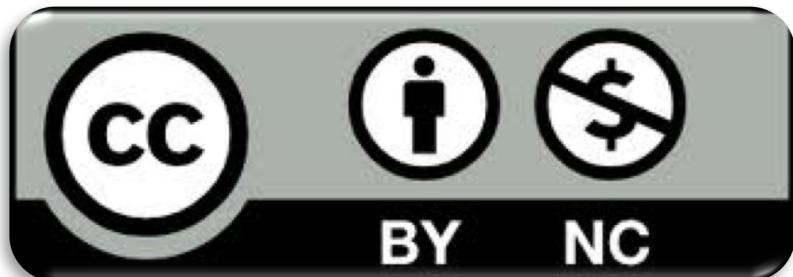
[www.consorzio-cini.it](http://www.consorzio-cini.it)

# 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

3

## Thanks

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

## Contributors

- CyberChallenge.IT
- Giuseppe AIRO' FARULLA
- Jean ARLAT
- Alessandro ARMANDO
- Roberto BALDONI
- Rocco DE NICOLA
- Arturo DI CORINTO
- Giorgio DI NATALE
- Eugene KASPERSKY
- Rosario PUGLIESE
- Francesco VESTITO
- Stefano ZANERO

# Outline

4

- Rilevanza
- Costi

# Outline

5

- Rilevanza
- Costi

# Cybersecurity

6

- *Non è un problema che mi riguarda*

# Cybersecurity

7

- *Non è un problema che mi riguarda ... e, in ogni caso, con la mia vita e con la mia professione c'entra come i cavoli a merenda!!*

# Ma ne siete proprio sicuri?

8

# L'appello di Mattarella per la cybersicurezza: "Gli Stati hanno l'obbligo di difendere dagli attacchi web"



*Il presidente della Repubblica Sergio Mattarella a Riga (Lettonia), in occasione del vertice Arraiolos (ansa)*

*"Non dobbiamo cadere nella trappola di pensare di potere irreggimentare i nostri concittadini orientandoli, ma stimolare la loro libertà e il loro spirito critico", così il capo dello Stato durante il meeting in Lettonia*

13 Settembre 2018

*"Le conseguenze di attacchi informatici possono essere disastrose: sui sistemi informatici pubblici, sulle banche, sui sistemi elettorali, sui sistemi sociali e sanitari. E la possibilità che grandi gruppi criminali, o anche Stati con atteggiamento ostile, possa provocare questi danni disastrosi è davvero allarmante per tutti".*



RELAZIONE DEGLI 007

# L'appello di Conte ai cittadini: 'La cybersecurity diventi interesse di tutti'

di Luigi Garofalo | 28 Febbraio 2019, ore 13:31

CYBERSECURITY



*Alla presentazione della Relazione sulla politica dell'informazione per la sicurezza 2018, Giuseppe Conte: 'La minaccia cibernetica può danneggiare le infrastrutture critiche e strategiche. La cultura della cybersecurity diventi interesse dei cittadini per incrementare il livello complessivo di sicurezza, anche se l'Intelligence è il custode della cybersecurity nazionale'.*



# Ue, Jean-Claude Juncker: "L'Europa non è pronta contro i cyberattacchi"



Jean-Claude Juncker, presidente della Commissione europea (ansa)

*Nel suo discorso sullo Stato dell'Unione il presidente della Commissione europea mette la cybersecurity tra le priorità dell'agenda e propone un'Agenzia europea per la sicurezza*

di ARTURO DI CORINTO

# Ue, Jean-Claude Juncker: "L'Europa non è pronta contro i cyberattacchi"



Jean-Claude Juncker, presidente della Commissione europea (ansa)

*Nel suo discorso sullo Stato dell'Unione il presidente della Commissione europea mette la cybersecurity priorità dell'agenda e propone un'Agenzia europea per la sicurezza*

di ARTURO DI CORINTO

Priorità:

1. Agenda commerciale
2. Competitività
3. Clima
4. Cybersecurity
5. Immigrazione

# Ue, Jean-Claude Juncker: "L'Europa non è pronta contro i cyberattacchi"



Jean-Claude Juncker, presidente della Commissione europea (ansa)

*Nel suo discorso sullo Stato dell'Unione il presidente della Commissione europea mette la cybersecurity priorità dell'agenda e propone un'Agenzia europea per la sicurezza*

di ARTURO DI CORINTO

Rel. 03.06.2019

- Priorità:
1. Agenda commerciale
  2. Competitività
  3. Climat
  4. Cybersecurity
  5. Immigrazione

# ITALIA SOTTO ATTACCO



Baldoni, in una sala piccola ma splendida, con il soffitto completamente affrescato, di Palazzo Verospi in via dell'Impresa a Roma.

(di Alessandro Rugolo) 20/11/18 - Da tempo l'Italia risulta essere nel mirino degli hacker, eppure, fino a ieri sembrava che nessuno fosse interessato. Ma questa volta è diverso.

Già da qualche giorno circolano voci su un attacco cyber che avrebbe colpito gli uffici giudiziari. Questa volta però alle voci seguono i fatti, e i fatti consistono nella **prima conferenza stampa tenuta dal professor Roberto Baldoni, vice direttore generale Cyber del Dipartimento delle informazioni per la Sicurezza**.

Questa volta l'attacco è andato a segno e sembra che siano in tanti ad essere preoccupati.

*Difesa Online* è invitata alla conferenza stampa, come le principali testate giornalistiche. Ci si trova tutti assieme ad aspettare l'arrivo del professor

# Perché occuparsene

16

- L'informatizzazione della società e la digitalizzazione di beni, merci e servizi, pubblici e privati, ci obbliga ad avere una grande attenzione verso la sicurezza degli asset informatici.

# Perché occuparsene

17

Infrastrutture  
Critiche

# Cybersecurity e infrastrutture critiche

18

- In un mondo sempre più digitalizzato gli attacchi informatici che suscitano allarme nella popolazione e causano danni ingenti all'economia mettono in pericolo la stessa incolumità dei cittadini quando colpiscono le reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti; cioè le infrastrutture critiche delle società moderne.

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)

Rel. 03.06.2019

# Perché occuparsene

20

Infrastrutture  
Critiche

Imprese

# Cybersecurity e imprese

21

- Un attacco informatico di successo potrebbe anche rappresentare un momento di non ritorno per la credibilità di un'azienda, lo sviluppo del suo business, la capacità di vendere prodotti utili in un regime di sana concorrenza.

# Average Enterprise Is Hit by a Cyber Attack Every 1.5 Seconds

Stu Sjouwerman



FireEye released its yearly Advanced Threat Report, and they did some interesting math. Enterprises are hit by cyber attacks on average once every 1.5 seconds, which is double from the year before, which was once every three seconds for an attack of some kind.

In the first six months, Java was the most common attack vector for hackers, but FireEye observed a surge in watering hole attacks using IE zero-days in the second half of the year.



# Status

23

[Claudia Biancotti:  
“The price of cyber  
(in)security: evidence  
from the Italian private  
sector”.  
*Questioni di Economia e  
Finanza* 407,  
Banca d’Italia,  
Dicembre 2017]

Tabella 1.1: Attacchi subiti da imprese italiane, settembre 2015–2016

<b>Area geografica</b>	
Nord Ovest	44,2
Nord Est	47,3
Centro	52,3
Sud e Isole	35,9
<b>Numero di addetti</b>	
20 – 49	42,7
50 – 199	48,4
200 – 499	56,0
500 e oltre	62,8
<b>Intensità tecnologica</b>	
Alta e medio-alta	48,8
Bassa e medio-bassa	43,8
<b>Incidenza delle esportazioni sul fatturato</b>	
Meno di 1/3	43,0
Tra 1/3 e 2/3	51,8
Più di 2/3	48,5
<b>Percentuale sul totale delle aziende</b>	<b>45,2</b>

## Le aziende nel mirino degli hacker

Nord Ovest

**44,2%**

Centro

**52,3%**

% di aziende che  
hanno dichiarato  
di aver subito  
**un attacco tra**  
**il 2015 e il 2016**

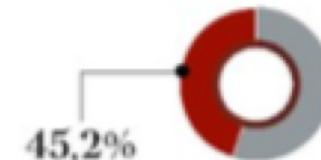


Nord Est

**47,3%**

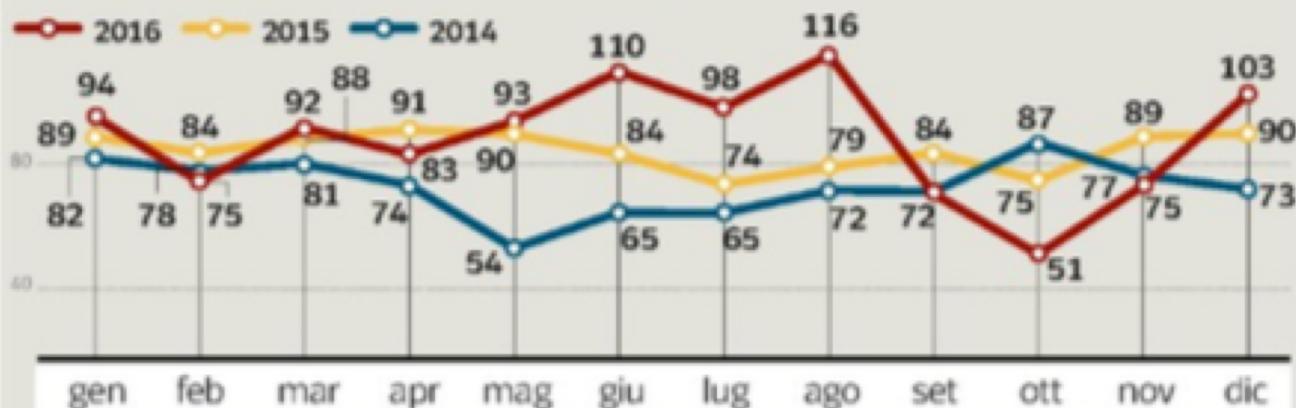
Sud e Isole

**35,9%**



Percentuale  
complessiva di  
aziende italiane  
attaccate

### IL NUMERO DI ATTACCHI



FONTE: Banca d'Italia, 2017 - Hackmageddon.com

L'Eg

# Perché occuparsene

25

Infrastrutture  
Critiche

Imprese

Sistema Paese

# Cybersecurity e Sistema Paese

26

- Un attacco informatico riuscito potrebbe destabilizzare il mercato azionario e sprofondare interi paesi nel caos, oppure bloccare i rifornimenti di gas in inverno o il ciclo dei rifiuti urbani: che scenario politico ne conseguirebbe?

# Perché occuparsene

27

Infrastrutture  
Critiche

Imprese

Sistema Paese

Diritti

# Cybersecurity e Diritti

28

- La sicurezza informatica oggi coincide con la sicurezza dei dati e delle informazioni che ci definiscono come cittadini, elettori, lavoratori, consumatori.
- Se la sicurezza di dati e informazioni viene meno, a risentirne è la nostra privacy, che è la precondizione per esercitare il diritto d'opinione, d'espressione, di cronaca, d'associazione, di movimento, d'impresa, alla proprietà.

# Caveat

29

*Qualsiasi “cosa”  
connessa a Internet  
può essere  
attaccata...*

Not IF,  
But WHEN ...

Qualsiasi “cosa”  
connessa a Internet  
può essere  
attaccata...

# Tutto è sotto attacco

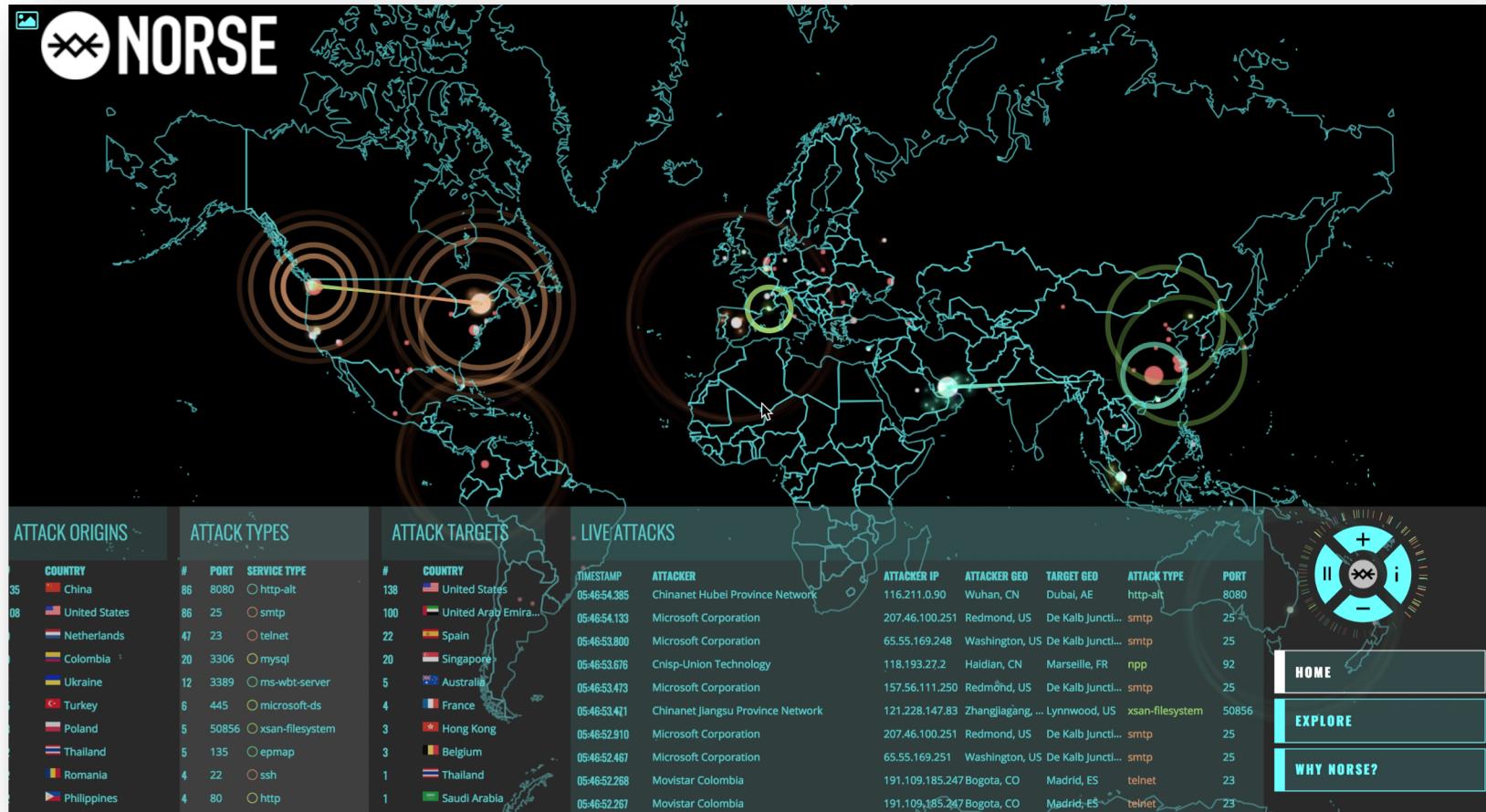
31



# ... sempre ...

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

32



# Outline

33

- Rilevanza
- Costi

# Costi

34

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



# Costi

35

CYBERSECURITY

TECH | MOBILE

SOCIAL MEDIA

ENTERPRISE

CYBERSECURITY

TECH GU

Cybercrime costs the global economy \$450 billion

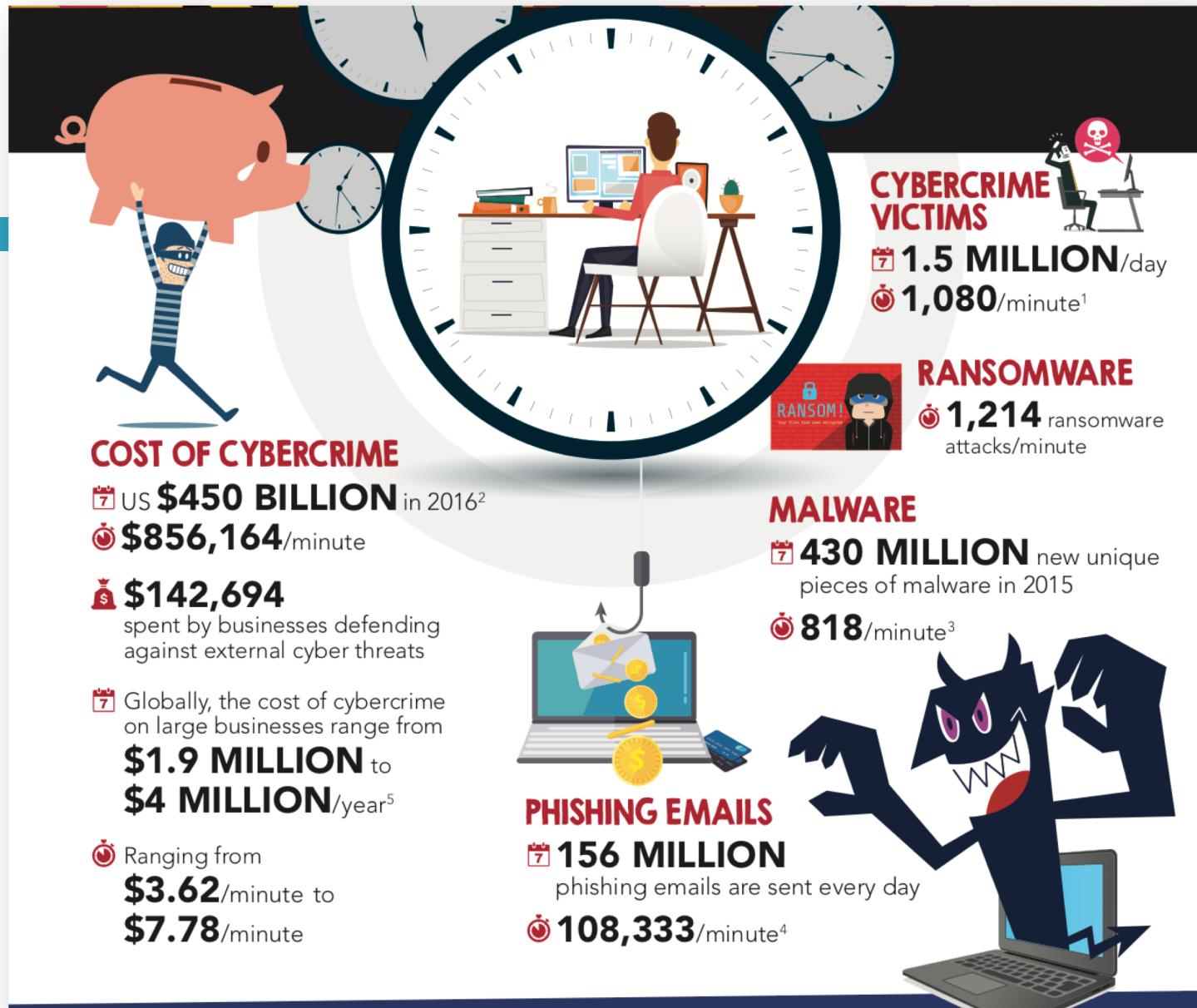
Luke Graham | @LukeWGraham  
Published 10:00 AM ET Tue, 7 Feb 2017

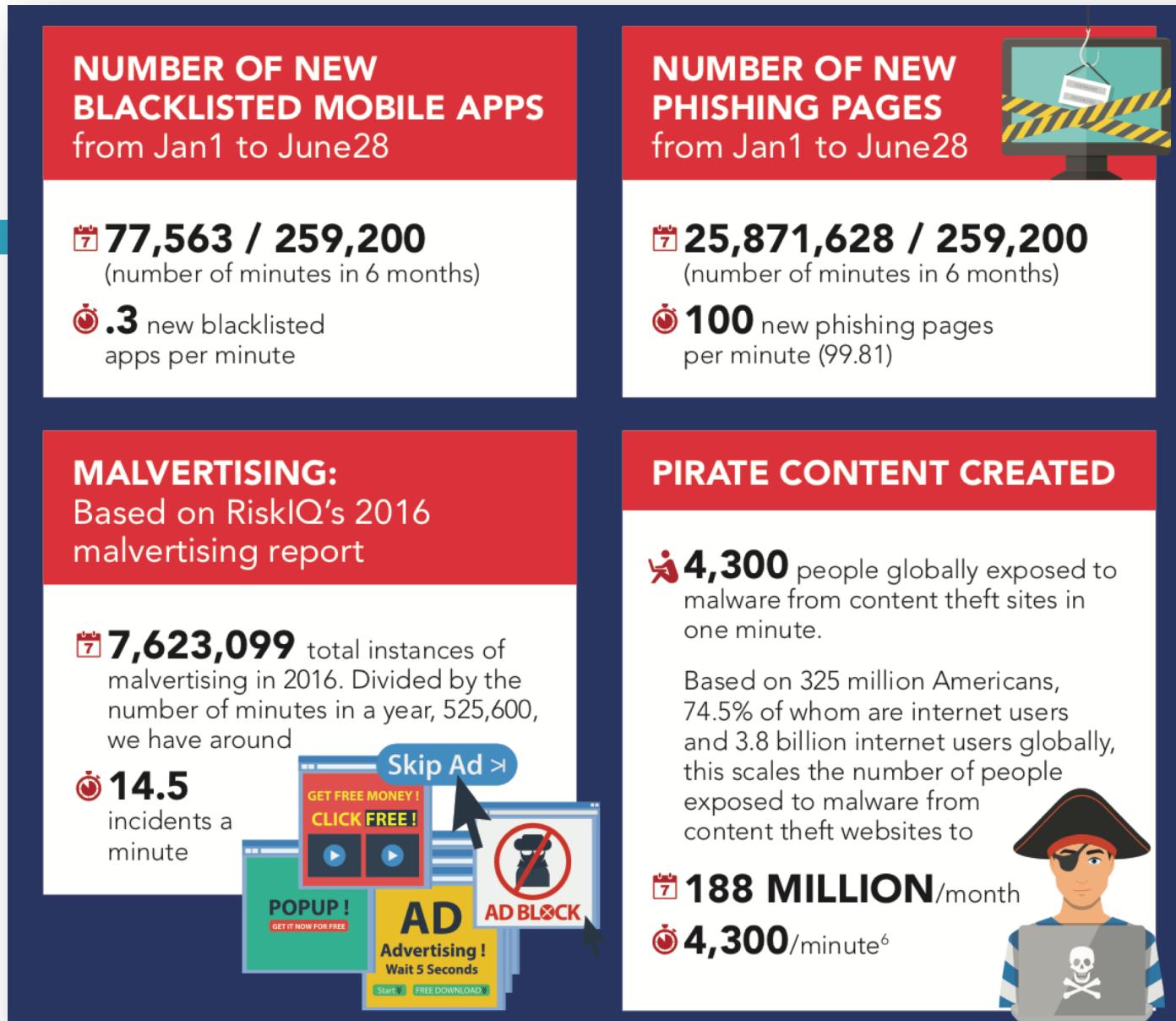


PIL dell'Austria nel 2017

434 miliardi di \$

 Cybersecurity National Lab





# Cybercrime vs. space

38



[E. Kaspersky, 2018] tional Lab

# Cybercrime vs. space

39



Малые Автюхи, Калинковичский район  
Республики Беларусь

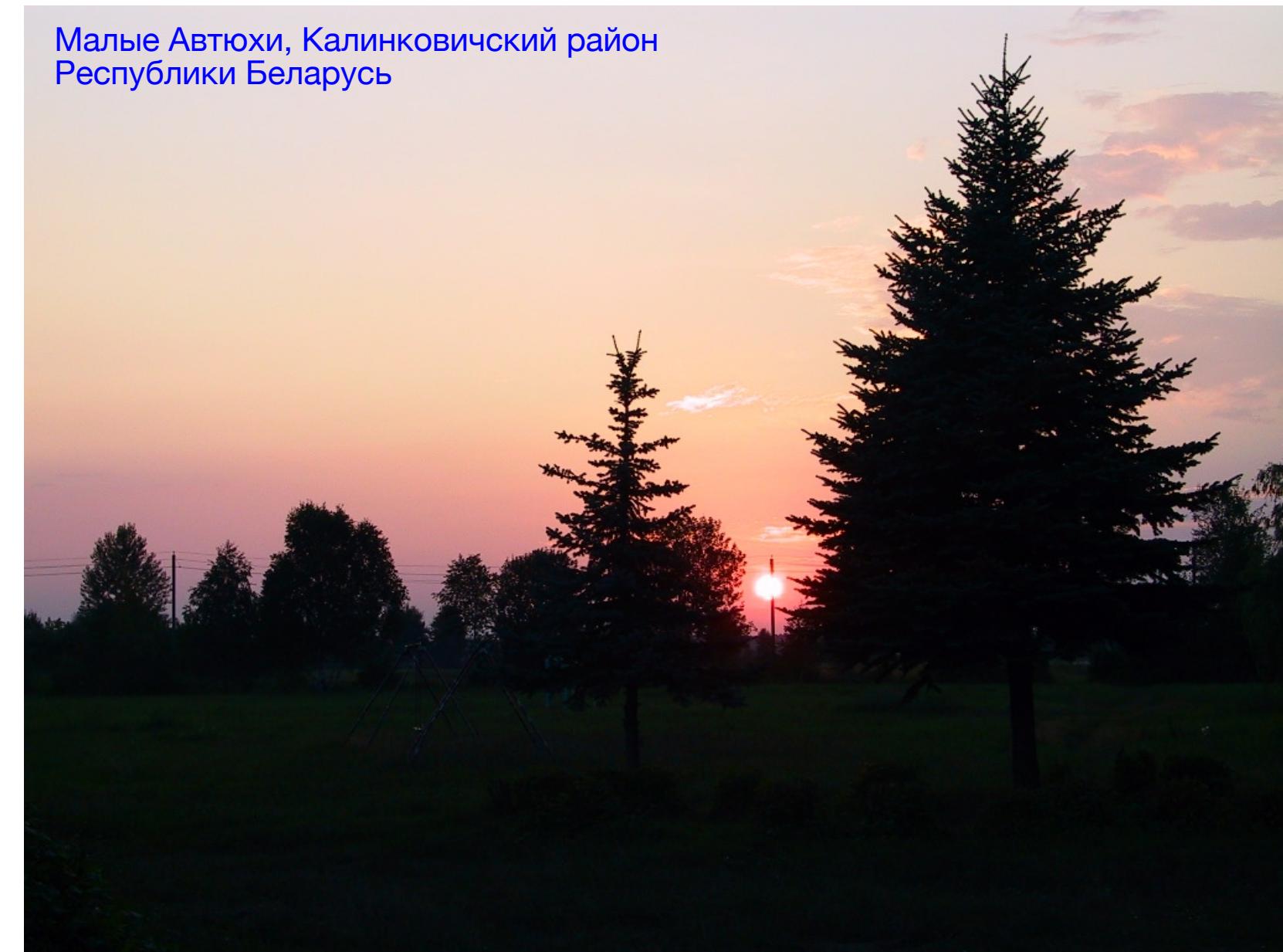
**Paolo PRINETTO**

Director

CINI Cybersecurity National  
Laboratory

[Paolo.Prinetto@polito.it](mailto:Paolo.Prinetto@polito.it)

Mob. +39 335 227529



 **cini**  
**Cybersecurity**  
**National Lab**

[www.consorzio-cini.it](http://www.consorzio-cini.it)