02 Luglio 2020

mega-trends e recente evoluzione del cybercrime

L’impatto a lungo termine del COVID sulle linee evolutive del cybercrime

Enrico Frumento, CEFRIEL (IT)

Senior Domain Expert

Cefriel

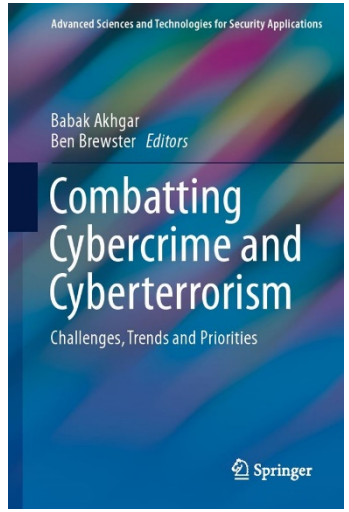
POLITECNICO DI MILANO

CHI SONO

- I am a “Security Guy”

- Principalmente svolgo ricerca nel mondo della sicurezza non convenzionale dal 2000, in CEFRIEL (www.cefriel.com).
  - Cybercrime intelligence
  - Offensive security
    - Malware
    - Social engineering
    - Intrusions
    - Innovative security solutions
    - Secure code development
    - Mobile terminal exploit
    - …

- Autore di oltre 60 articoli scientifici e pubblicazioni
- Twitter: @ENRICOFF



CAPACITA’ E TURNOVER DEL CYBERCRIME

- Il Cybercrime (CC) ed cyberterrorism (CT) hanno una disponibilità ben superiore a quella della IT Security

- Tempo fa è stata completata la “transizione” da un fenomeno principalmente geek-driven ad uno business-driven.

- La distinzione fra attacchi state-sponsored e private-sponsored non ha più alcun senso

CAPACITA’ E TURNOVER DEL CYBERCRIME

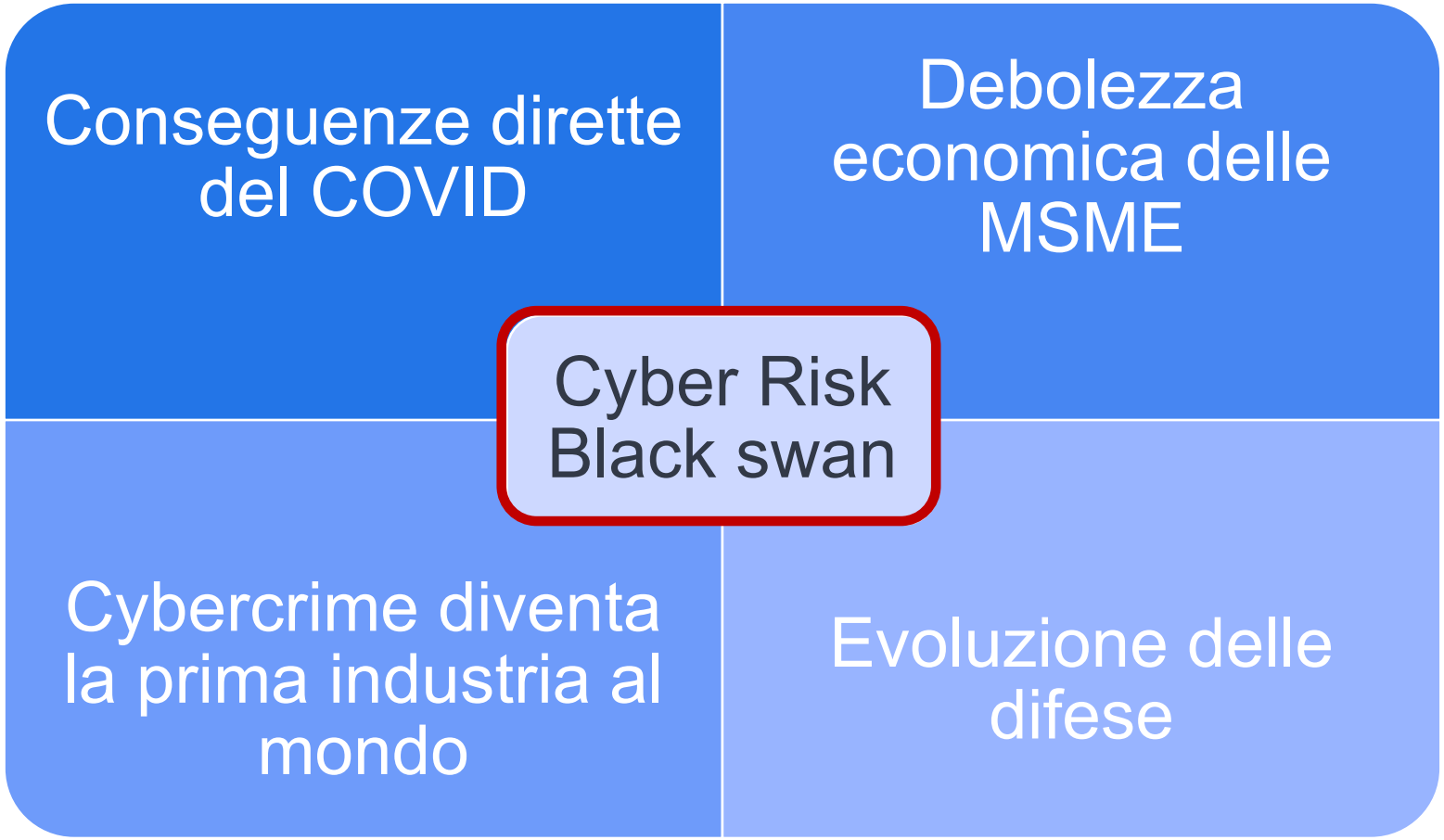
- **2017**, Il mercato globale annual del traffico di droga è stato stimato fra $426 e $652 miliardi (USD)
- **2018**, La cybercrime economy globale genera più di $1.5 trillioni (1 trillione=1k miliardi)
- **2021**, Il cybercrime potrebbe diventare la 3ª industria mondiale per fatturato, ($6 trillioni, fonte WEF)
- **cybercrime/droga = 1.5 ratio**

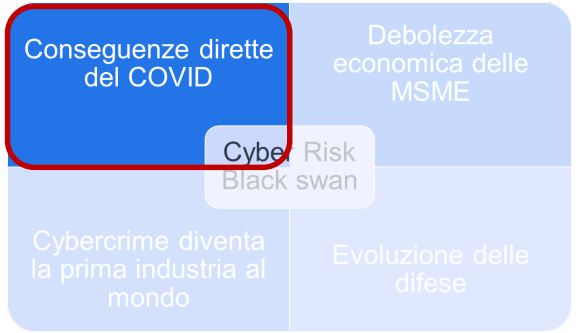
- **Oggigiorno i professionisti della sicurezza hanno ben compreso ed *internalizzato* come sia solo questione di tempo prima che le loro difese siano compromesse.**

- Questo a causa del fatto che la *threat landscape* ed i *business plan degli attaccanti* sono in continua evoluzione.

- **I cybercriminals sono stakeholders a tutti gli effetti dei sistemi informatici**
- E’ necessario considerarli in ogni fase di progettazione, a partire dal business use-case, in quanto
  - seguono una *digital transformation agenda* differente, in qualsiasi contesto applicativo
  - fanno business assieme a voi e con i vostri sistemi
  - hanno dei piani differenti

- **Mega tendenze ...**
- Commoditizzazione del CC/CT
- *Coopetizione* fra Crime e Cybercrime
- Gli attacchi sfruttano tutti e 7 I layer della sicurezza
- Approccio low and slow
- Alleanza fra cybercrime e cyberterrorism: evoluzione dell'Hybrid warfare
- Attacchi specifici contro asset tangibili ed intangibili
- La maledizione dei dati (per la difesa)
- Scenari politici complessi
- Artificial Intelligence (usata sia come strumento di attacco che entità attaccata)

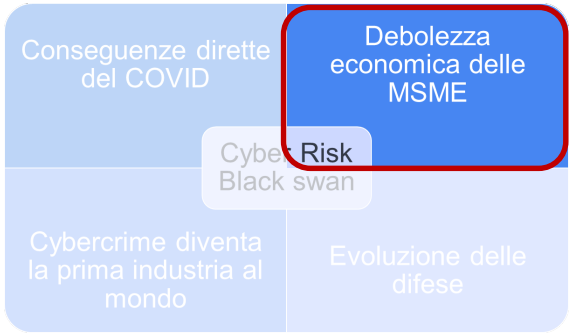




- Conseguenze dirette del COVID di rilievo per il cybercrime
  - Digital transformation agenda forzata
    - Smart working
    - De-localizzazione delle workforces
    - Ridefinizione della DMZ aziendale
  - Supply chain più corte e resilienti sia geograficamente che tecnologicamente

Questo rappresenta un occasione di crescita per il cybercrime in termini di proliferazione dei soft target

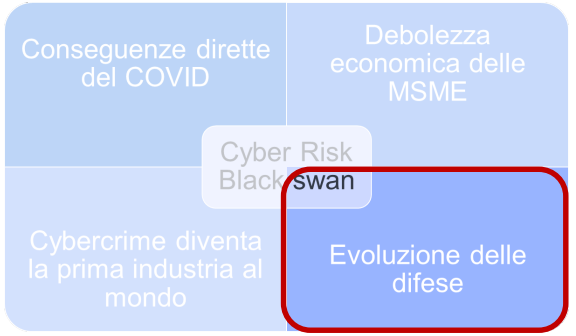
- In generale una maggiore attenzione agli investimenti in ambito cybersecurity
  - Sostenibilità della cybersecurity
  - Minore propensione al cyber rischio (es. moral hazard)
- Maggiore attenzione agli asset intangibili



Oggi più che mai si fa attenzione al delicato equilibrio tra le potenziali perdite derivanti dal rischio ed i costi immediati delle mitigazioni.

- COVID ha messo il cybercrime in «overdrive»
  - TTP (Tattiche, Tecniche e Procedure) rinnovate
  - Attacchi a nuove industrie (es. Agrifood, Costruzioni)
  - Attacchi rinnovati a vecchie industrie (es. sistemi IT/OT, ospedali)
  - WEF 2020, cybercrime 3° business per dimensione
- Il dark market si sta trasformando radicalmente per essere meno rintracciabile e diminuire i «takedown»

I precedenti modelli di calcolo del cyber rischio sono problematici a causa della discontinuità che il COVID rappresenta



- Avvento di una nuova generazione di sistemi di difesa aziendale
  - Basati su AI – evoluzione del cybercrime: AI vs AI
  - Basati su modelli di calcolo del cyber rischio rinnovati
  - Sostenibilità è la parola chiave: stimare cyber rischio e perdita economica a partire dal valore degli asset e comprendere il ROSI delle mitigation
  - Modello di governance integrato (es. IT/OT)
  - Re-skilling dei formatori e della forza lavoro

IL PROGETTO HERMENEUT – WWW.HERMENEUT.EU

Cefriel

ENGINEERING

Cefriel
POLITECNICO DI MILANO

UNIVERSITÉ PARIS SUD

deepblue
CONSULTING & RESEARCH

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Enterprises intangible Risk Management via Economic models based on simulatioN of modErn cyber-aTtacks

HERMENEUT

[ZenaByte] s.r.l.
Artificial Intelligence & Analytics

CATAPULT Digital

E S
EUROPEAN ORGANISATION FOR SECURITY

IAI ELTA

Dedalus
HEALTHCARE SYSTEMS GROUP

Risultati ed impatto

Il progetto HERMENEUT ha creato una metodologia per calcolare la probabilità che i beni tangibili e intangibili di un'organizzazione vengano attaccati con specifiche strategie di attacco, e collegare questo valore a una stima economica delle perdite, per calcolare mappe di cyber-risk ad hoc per un'organizzazione.

- **Cefriel partecipa alla stesura della SRIA 2021-2027**

- Quest'anno verranno preparate due SRIA:
  - Digital Europe Programme (DEP) – 2021-2027
    - *strategic areas for investment in order to develop a **Capability Development Plan** to increase **digital autonomy** and respond to the needs of our industrial sectors*
  - Horizon Europe Programme (HEU) – 2021-2027
    - *four main strategic areas for investment in order to develop a **comprehensive cybersecurity R&I strategy** in Europe to increase **digital autonomy and respond to the needs of our industrial sectors**, while protecting the European fundamental rights*

Enrico Frumento

Senior Domain Expert @ CEFRIEL

@enricoff

https://www.linkedin.com/in/enricofrumento/

Cefriel
POLITECNICO DI MILANO

Cefriel.com

MILANO
via Renato Fucini 2,
20133,
Milano - Italy

LONDON
4° floor
57 Rathbone Place
London W1T 1JU – UK

CINCINNATI
15° floor
250 East Fifth Street,
Cincinnati, OH 45202 - USA