



WAVESTONE

# Cybersecurity & innovation the double-edged sword challenge

CEPS - Keynote

**Gérôme BILLOIS**

gerome.billois@wavestone.fr

(+33) 6 10 99 00 60

@gbillois



# Who am I?



Jérôme BILLOIS, Partner Cybersecurity & Digital Trust

 @gbillois

WAVESTONE

14

countries

3500

professionals

600

consultants and experts  
in Cybersecurity & Digital Trust

Experience feedback from our CERT





*In 2021, **Ransomware** will remain the threat #1...*

Waves of non-targeted  
ransomware affecting  
**companies** (since 2015)

Non-targeted ransomware  
mostly affecting  
**individuals** (since 2010)

Targeted ransomware also  
**leaking data**  
(since end of **2019**)

**But what is coming next?**  
Improved attackers' capabilities  
New ways to "ensure" payment

Targeted Ransomware  
**"Big Game Hunting"**  
(since 2018)

# 3 Trends *that will carry on* 2021...



**THE RANSOMWARE  
HYDRA**



**PROVIDER  
HACKING**



**NEW CLOUD  
ATTACKS**

# A *rapidly* GROWING CYBERCRIME

## Increasing number of targets

- Digital transformation of companies
- Broad spread of technologies to the public

## Accessible expertise

- Skills widely available
- Black Market of Attack Tools
- Mafia organization

## Impunity

- Anonymization / absence of trails
- Complex legal response
- Cryptocurrencies

## Important Profits

- DDOS : \$20 to hundred of \$ / hour
- Credit card data: 3 to \$150 / card
- Personal data : 0,3 to \$2 / person
- Business fraud/spying: thousands of \$

*Increase cyber security level "by design" for companies and suppliers*

*Regulate and criminalize part of the market*

*Increase international cooperation and judiciary efficiency*

*Attack profitability and complexify money laundering*

Becoming a **CHALLENGE**  
*for* **POLICY MAKING**

# Cloud



**Cloud is already and will be an enabler  
for an industrialized vision of IT...**

*Large scale, flexibility...*

**...and many new security technologies**

*API, transparency cybersecurity, Zero-Trust, CASB...*

**But criminals know how to  
exploit new Cloud features**

*Exposed database, identity and  
access management higher  
complexity...*

**Cloud adoption is slowed by cyber  
borders / protectionism**

*Multiplication of policies and regulations  
avoiding free flows of data*

**A new hope with confidential computing?**

*Ability to work on encrypted data without decrypting it*

# Artificial intelligence



## A tool for cybercriminals

*AI-powered reconnaissance, social engineering, breaking captcha...*

## A target for cybercriminals

*AI poisoning, inference, evasion*

## But also a key tool for cybersecurity

*Automation of attack detection and reaction...*

*And many innovations to protect AI are required*

Inputs

Filtering

Force noise  
Prevention

Outputs

Moderator

Black List

Processing Learning

Adversarial  
Learning

Advanced  
Learning

Gradient  
Masking

Defensive  
Distillation

# Artificial intelligence

*A glimpse into the future...*

*A tool for cybercriminals*

*AI-powered reconnaissance, social engineering,  
breaking captcha...*

## The Cyber Grand Challenge - 2016



1<sup>st</sup> **AI-based**  
hacking tournament

Organized by  
**DARPA**

But also a key tool for  
cybersecurity

*Automated attack detection  
and reaction*

**\$55M** reward  
for the winner

7 super computers  
with (flawed)  
services to protect

Inputs

Filtering

Force noise  
Prevention

Outputs

Moderator

Black List

AI  
Processing Learning

Adversarial  
Learning

Advanced  
Learning

Gradient  
Masking

Defensive  
Distillation

# Quantum computing and communications

A sword with a dark hilt and a silver blade, symbolizing the dual nature of quantum computing as both a threat and an opportunity.

## **A major threat for cryptography**

*A Quantum Computer (around 2040) might be able to break RSA2048, security corner stone of our communication*

## **But also a key opportunity for cybersecurity**

*Quantum Key Distribution & Quantum Random Number Generators*

# Quantum computing and communications

## 6 steps towards the *Quantum Internet*...

Stage	Network typology	Research & development
0	Pre-quantum networks	<b>Basic quantum link between classical nodes</b> , already exist in some large cities of Switzerland, Japan, China...
1	Proto-quantum networks	<b>Quantum link with quantum nodes (or repeaters)</b> , experimented in laboratories for the moment and a satellite experimentation carried out by a Chinese team linking 2 quantum nodes.
2		
3	Advanced quantum networks	<b>Quantum computer interconnection with quantum link and quantum nodes (or repeaters)</b> <i>Only theoretical for now</i>
4		
6		



# A real **CHALLENGE** *for* **POLICY MAKING**

THREATS QUICKLY ADAPTING WITH HUGE CAPABILITIES

TECHNOLOGIES EVOLVING AT THE SPEED OF LIGHT

POLICIES THAT SHOULD ENABLE AND NOT BLOCK  
*FINDING THE RIGHT BALANCE*



**Gérôme Billois**  
Partner

**M** +33 (0)6 10 99 00 60  
gerome.billois@wavestone.com

wavestone.com  
@wavestone\_