

2<sup>ND</sup> ENISA CYBERSECURITY MARKET ANALYSIS CONFERENCE

PANEL 1 : CYBERSECURITY MARKET FORCES



# Accelerating cyber threats

## Geopolitical threats.

The conflict between Russia and Ukraine has leaped into cyberspace through multiple cyberattacks, affecting several countries.

## Attacks against the energy industry.

During the energy crisis in the EU, the EU energy industry has been the target of several cyberattacks that have jeopardized its operations.

## Ransomware.

Security measures and the emergence of new ransomware operators increase competition. 60% of affected organizations may have paid the ransom.

## Zero-day exploits.

Cyberhackers can better identify and exploit these vulnerabilities to achieve their goals.

## Cyber attacks against public agencies.

Attacks against government institutions, including healthcare organizations, have increased by over 150% compared to 2021.

## AI-enabled Disinformation/misinformation.

Escalating AI-enabled disinformation, deep fakes and disinformation-as-a-service

## DDoS attacks.

DDoS attacks are growing in magnitude and getting more complex, moving towards mobile networks and IoT.

## Hactivism.

Hactivists-motivated cyberattacks have been linked to conflicts and social and human rights disputes.

## Crime as a service.

The price of malicious services offered on the dark web has fallen, due to increased competition.

# Cyber costs and resource drain



**€5.5 trillion** at the end of 2020  
Source: EU Commission



**350,000** unfilled jobs in cybersecurity in  
the EU in 2022  
Source: Cybersecurity Ventures

# Our panelists



James Baty



Nicolas Guillermin



Francesco Sacco

# James Baty



# Nicolas Guillermin



# Francesco Sacco

