

The background is a dark blue gradient. On the left side, there is a stylized globe with a network of glowing nodes and connecting lines. The nodes are colored in a gradient from blue at the top to yellow and orange at the bottom. The network lines are thin and light blue. On the right side, there are faint, glowing circuit-like patterns in blue and white.

Building a foundation of  
**trust.**

Karine Goris

# Behind The Numbers: The Attacks You'll Never Hear About

**1249**

Average amount of CYBER  
ATTACKS RECORDED  
by organization per week in the  
third trimester of 2025

*Source: RTBF*

**>1000**

Amount of  
CYBER THREATS  
INVESTIGATED on a yearly  
base, by large Financial  
Institutions.

**>150.000**

Average amount of PHISHING  
EMAILS RECEIVED  
on a yearly base, by Financial  
Institutions.



Understanding **why** Belgium  
is attacked.

# What Makes Belgium a Prime Target

Undersea data cables and center of Europe's energy transition (windmills).

2<sup>nd</sup> biggest port in Europe, logistics & shipping hub, critical for trade & supply chains.  
Attack could impact global trade routes

North Sea

Port of Antwerp-Bruges

Brussels

EU & NATO, over 100 international organizations and 300+ foreign diplomatic missions.  
Target for espionage and data theft.

NATO base

La Hulpe & Brussels

SWIFT, Euroclear and other key financial institutions.  
Attack could undermine trust in Belgium as a financial hub location

The background of the slide features a dark blue, almost black, space. In the center, a faint, glowing outline of a world map is visible. Overlaid on this map is a complex network of nodes and connecting lines. The nodes are colored in a gradient: blue and cyan at the top, transitioning through green and yellow in the middle, and ending in orange and red at the bottom. The lines connecting the nodes are thin and light blue. The overall effect is a sense of global connectivity and digital infrastructure. On the right side, there are faint, stylized circuit board traces in a light blue color.

Cyber threats shape the  
world around us

# Cyber threats shape the world around us

Over the past decade, adversaries have transformed significantly. What once was the domain of lone hackers has changed into a battleground of well-funded criminal organizations [driven by profit and monetization](#), launching phishing, scamming and spear phishing campaigns.

At the same time, [hacktivism](#) has gained momentum, with actors [promoting their political and social beliefs](#).

Lastly, nation-states also entered the frontline, [to secure and advance their geopolitical interests](#). As cyber capabilities offer strategic advantages over traditional warfare, an [increasing number of countries](#) are rapidly developing both offensive and defensive cyber programs. This growing diversification makes the [global threat landscape unpredictable and complex](#).

**POLITICAL**



**ECONOMIC**



**SOCIAL**



**TECHNOLOGICAL**



**LEGAL**



Cyber threats do not evolve in isolation, they are [shaped by the world around us](#): geopolitical tension, economic pressure, social behavior, and technological acceleration and innovation.

Connecting these dots helps us understand why cybersecurity is no longer just an IT concern, but a [strategic business opportunity and risk](#).

# POLITICAL



## Political

Cyber to secure and advance geopolitical interests.

## The flags behind the attacks

POLITICAL



# The flags behind the attacks

## POLITICAL



### Russia

Disruptive actions, influence and disinformation



## The flags behind the attacks

POLITICAL



## The flags behind the attacks

### POLITICAL



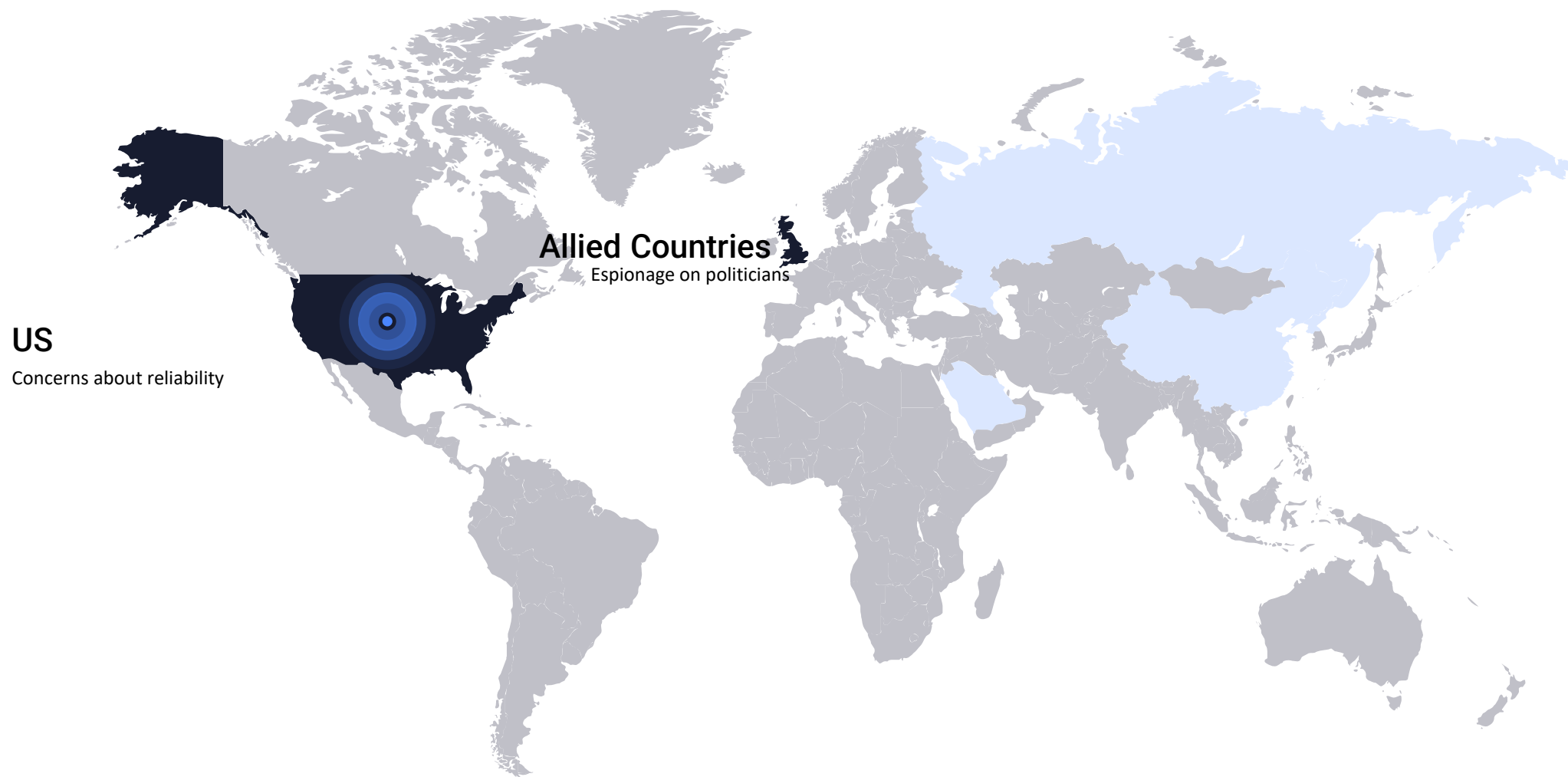
## The flags behind the attacks

### POLITICAL



# The flags behind the attacks

## POLITICAL





## ECONOMIC

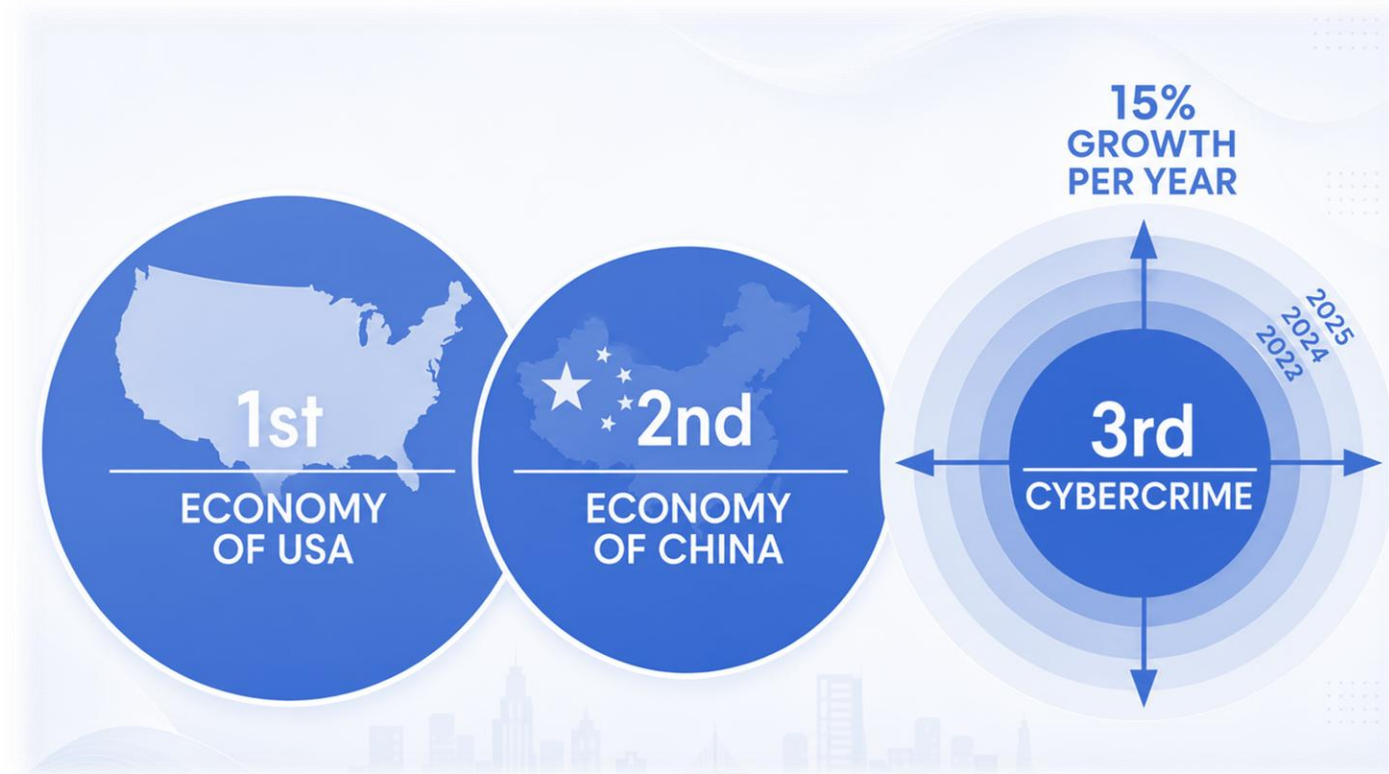


# Economic

Cyber as a financial weapon.



Cyber risk has become a **direct business and economic threat**. Attacks are aimed at creating **financial gain**, **market instability** and operational pressure. From fraud to ransomware to cyber conflict between nations, the **impact** is increasingly **measured in business continuity, financial loss and trust in the broader economy**.





**SOCIAL**



# Social

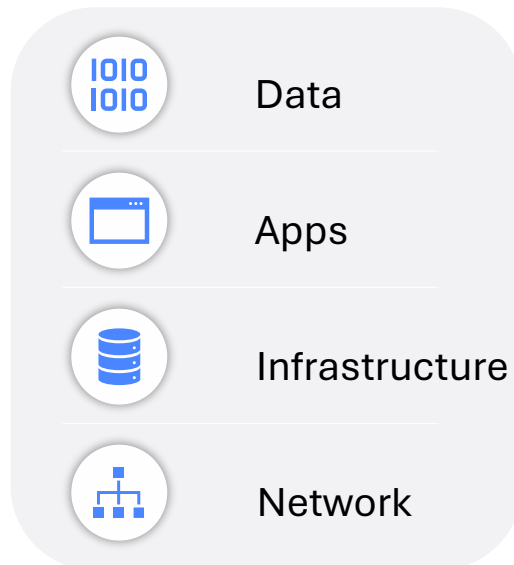
Trust has become the new frontline in cyber.



The attack surface has moved **closer to the business**. Risk is no longer limited to the systems we own, but also comes through the **access, devices and relationships** that keep us connected. The security approach must therefore evolve from defending the perimeter to **continuously validating trust across the ecosystem**.

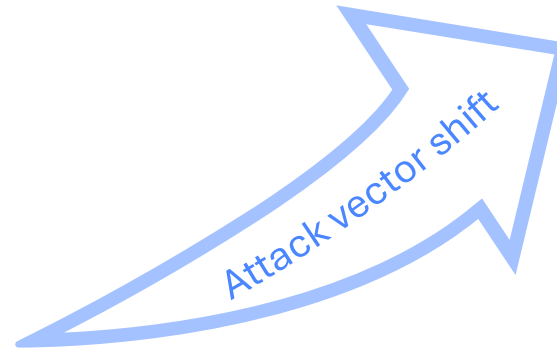
## Legacy attack vectors

*Well-established methods targeting weaknesses in technology.*



## New attack vectors

*Sophisticated and adaptive approaches that exploit complexity, connectivity and trust relationships within modern environments.*





## TECHNOLOGICAL



# Technological

Innovation is accelerating both opportunity and exposure.



Technologies expand what organizations can do — and how fast, how far, and through how many dependencies cyber risks can propagate.

## Risk is being amplified by

● Speed

**Technology cycles move faster than governance cycles**

Frontier AI • automation • rapid SaaS adoption

● Scale

**Platforms operate across entire ecosystems**

Cloud • identity providers • managed services

● Interconnection

**One weak link can cascade across many organizations**

APIs • supply chains • data sharing

● Uncertainty

**Risks emerge before controls mature**

Quantum • AI model behavior • autonomous agents



# LEGAL

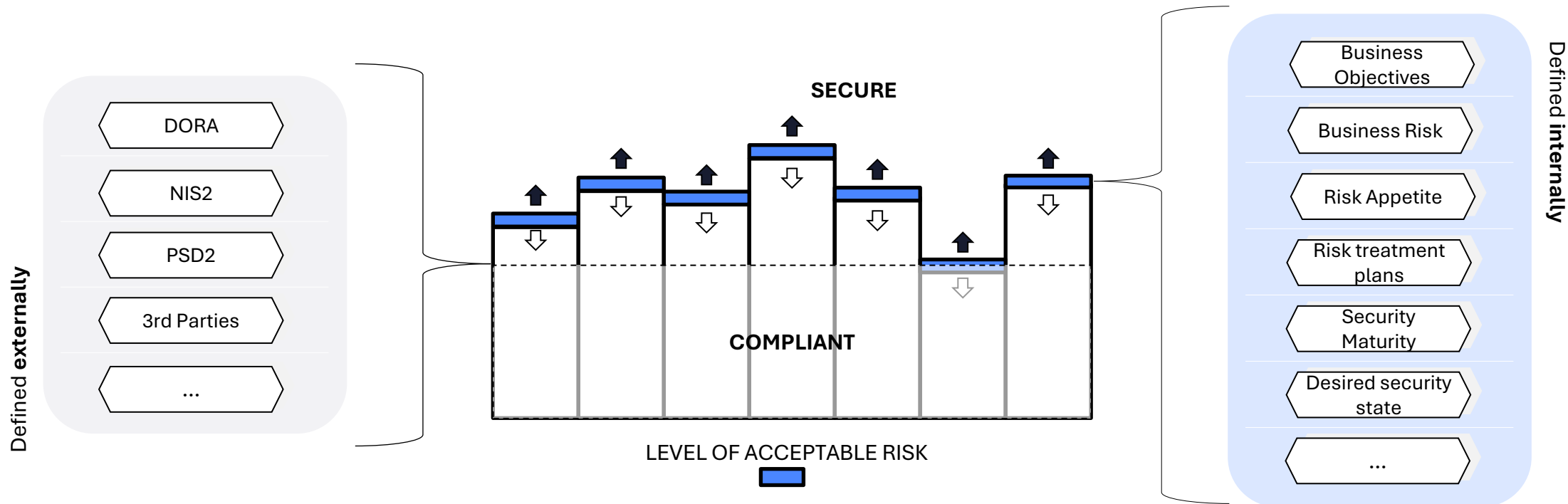


## Legal

Compliance sets the baseline, true security goes beyond it.



Information security compliance means following laws, regulations, and external requirements. Companies do this by setting up controls to protect data (keeping it confidential, accurate, and available). However, compliance doesn't always equal security—**real security also depends on internal measures that fit the company's risks and needs.**





# The Belgian Cyber Security Coalition unite the Belgium defense

# Cyber Security Coalition

## The Place to unite Cyber Experts in Belgium



The Coalition is Belgium's **largest non-profit cybersecurity community** and reference platform

Bringing together **public authorities, industry and academia** in a **neutral, trust-based** environment

To **strengthen Belgium's cyber resilience** by building a strong national cybersecurity ecosystem grounded in **trust, collaboration and shared responsibility**

### How we create impact

Experience  
Sharing

2025  
12 Events  
1,340  
participations

Operational  
Collaboration

2025  
12 Focus Groups  
49 meetings  
964 participations

Awareness  
Raising

Since 2015  
10 national  
awareness  
campaigns with

Policy  
Recommendations

Focus on EU  
Regulations &  
Standardizations  
Practical guidelines



- 230+ member organizations
- 1,400+ engaged cybersecurity professionals
- 16,000+ LinkedIn followers

