# Cyber-security

Impact on national competitiveness, jobs and growth

Rene Summer Government & Industry Relations 2018-03-07

# PERSPECTIVE

# Political economy of cyber-security - interest and values at stake

**Citizens**

- Privacy (control)
- Confidentiality (surveillance)
- Integrity / authenticity (crime)

**Business**

- Security /availability (running business)
- Confidentiality (protect trade secrets)
- International data flows (scale)
- Innovation (differentiation)

**Nation state**

- National security, public order, autonomy
- Law enforcement, intercept, retention, encryption/decryption
- National competitiveness, growth and jobs

**Cyber-Security**

- **Threats**: confidentiality, availability and integrity
- **Motives**: money, power (hard, soft), conviction/ideology
- **Threat actors**: criminals, espionage, warfare, insiders hacktivists and terrorism. + any combo
- **Targets**: citizens, businesses, public sector, societies and nations
- **Tools**: botnet, rootkit, worm, trojan, file infector, backdoor, RAT, ransomware, scareware, spyware, adware + any combo

# THREAT ANALYSIS

# What is being attacked ?

Three overarching categories of cyber-threats can be identified:

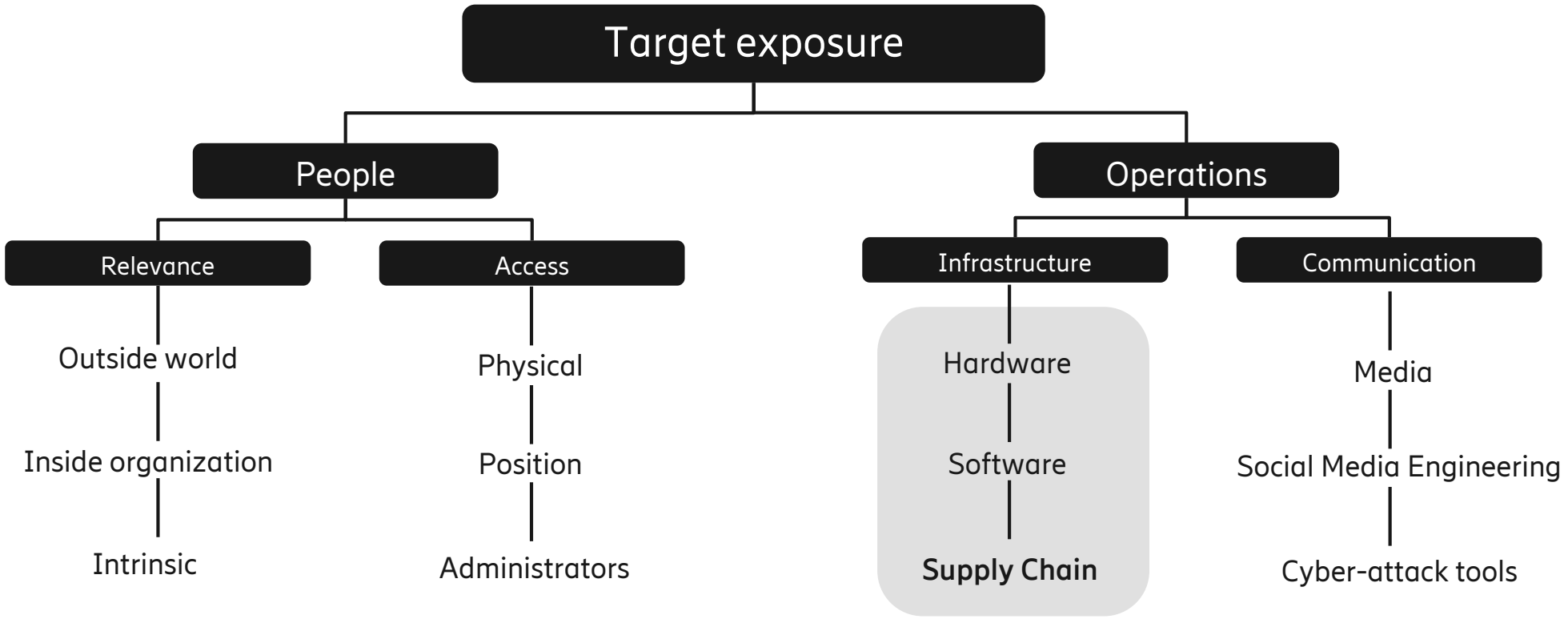
1) **Attacks on confidentiality**, or the theft of protected information,
   - Financial/criminal or state sponsored economic/political/military espionage

2) **Attacks on integrity**, whereby information or systems are maliciously changed to facilitate further exploitation,
   - Geopolitics, Cyber-warfare, state actors or cyber-terrorism

3) **Attacks on availability**, whereby services are disrupted.
   - Securing critical infrastructure, public order and continuity of business

*An attack targeting one aspect of security (Confidentiality, Availability, Integrity) will often target other aspects: for instance a DDOS attack (on Availability) being used as cover for Data Theft attack (on Confidentiality)*

# Threat exposure - target perspective




**If the target is a provider of public telecom or other CI - exposure is extended to the entire society**

# Why telecom networks in particular?

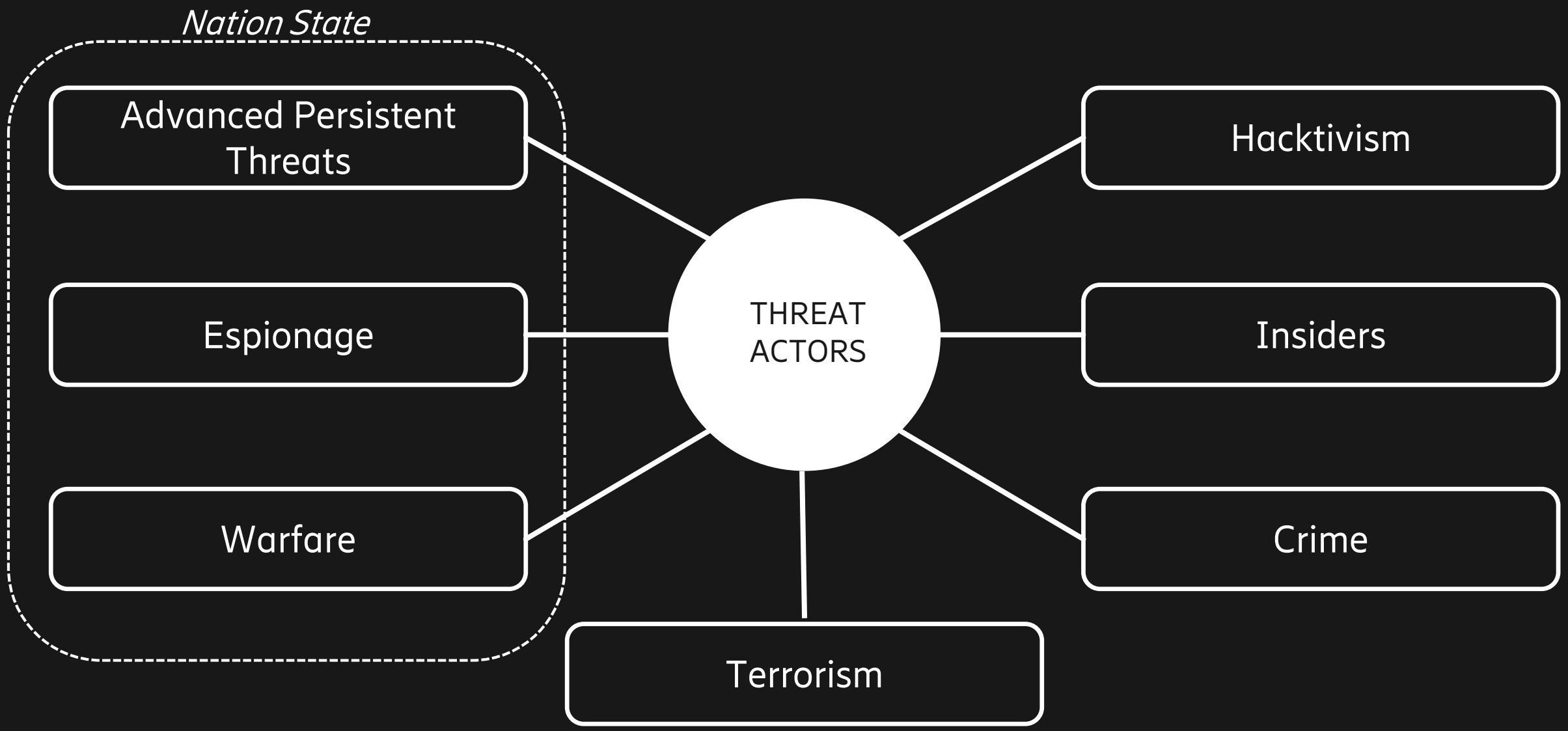
Dutch national security and intelligence agencies' **joint analysis of the risks from economic espionage**

"Damage to interests in the telecom sector has an almost **immediate adverse effect on national safety and security.** Communication, including data communications, is vitally important to enable Dutch **society to function unimpeded**.

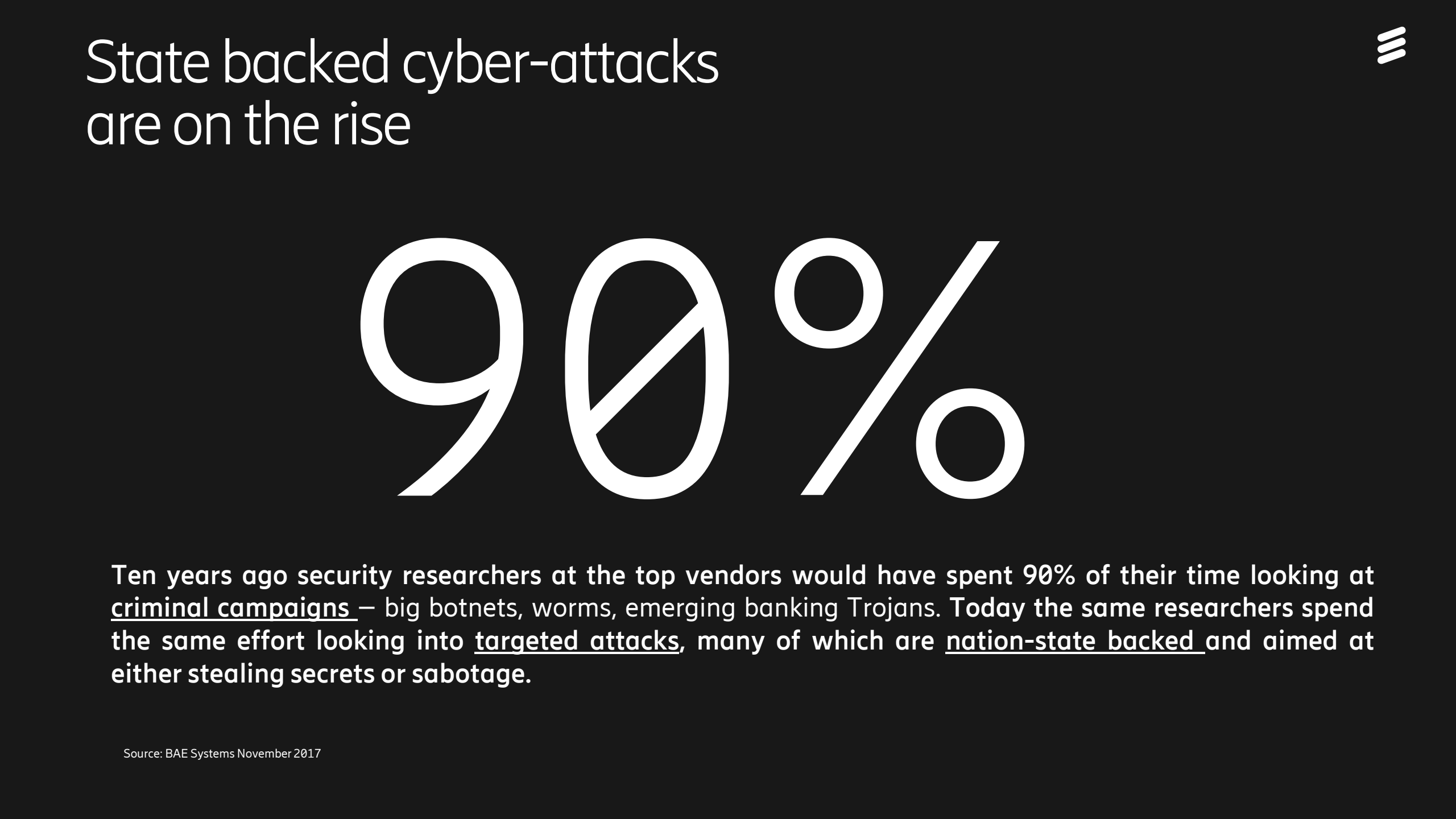
The telecom networks areas being **targeted by foreign intelligence** services (espionage). This makes telecom both a core interest and a vulnerability. The vulnerabilities in the telecommunication sector have **direct repercussions on all other sectors**."

Source: *Analysis of vulnerability to espionage, General Intelligence and Security Service of the Netherlands (AIVD), Directorate General for Safety and Security (DGV) Ministry of BZK (access Federation of American Scientists).*

# Threat landscape



# State backed cyber-attacks are on the rise

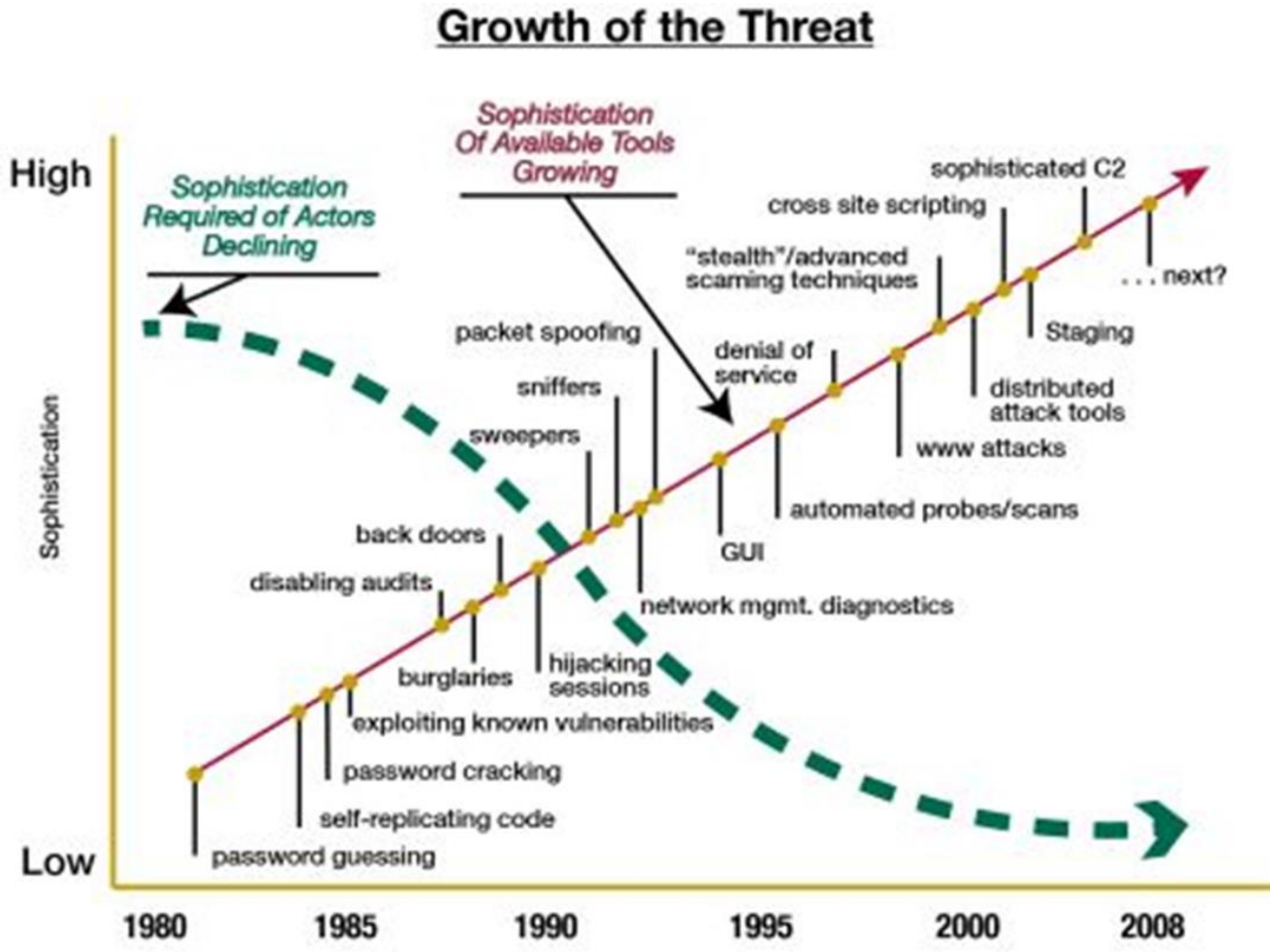



**Ten years ago security researchers at the top vendors would have spent 90% of their time looking at criminal campaigns** – big botnets, worms, emerging banking Trojans. **Today the same researchers spend the same effort looking into targeted attacks, many of which are nation-state backed and aimed at either stealing secrets or sabotage.**

Source: BAE Systems November 2017

# Sophistication of tools ↑ & skills required ↓

## - blurs the line where the state supported action ends…




SOURCE: NATO review magazine,

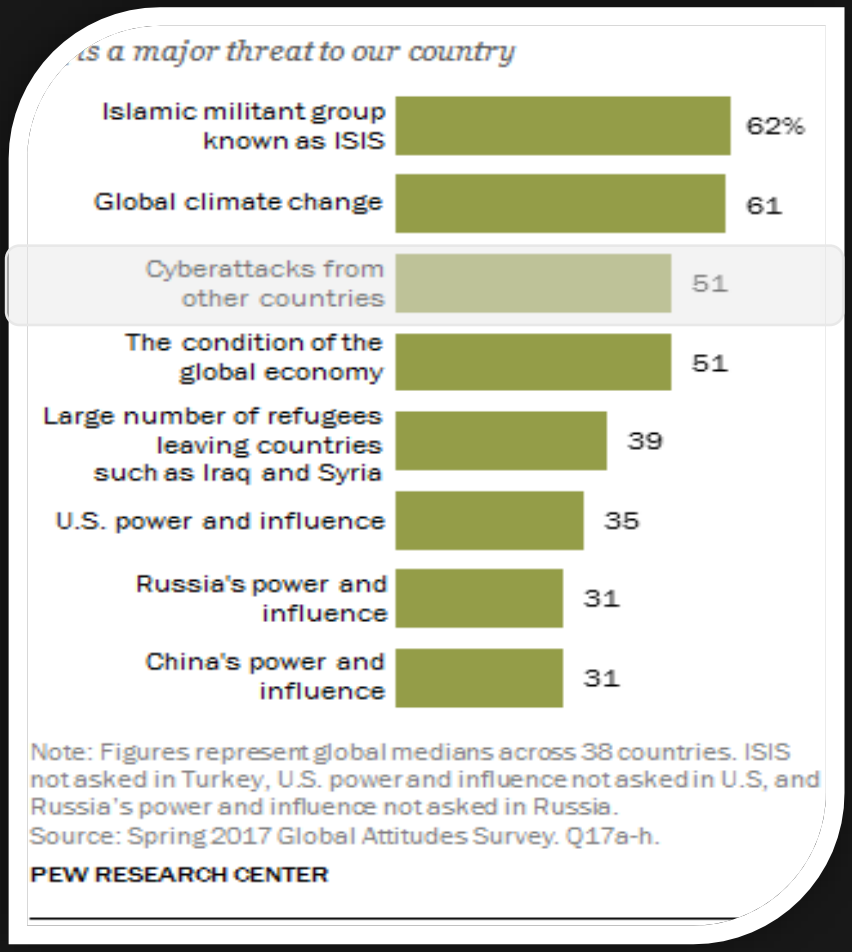
— Many more states now consider cyber capabilities as a legitimate and necessary part of their strategic toolbox alongside diplomacy, economic prowess and military might.

— Experience to date on the actual uses of cyber capabilities by states suggests such capabilities are better characterized as either ***espionage*** **or** ***sabotage***, making their employment most likely below the threshold of armed attack.

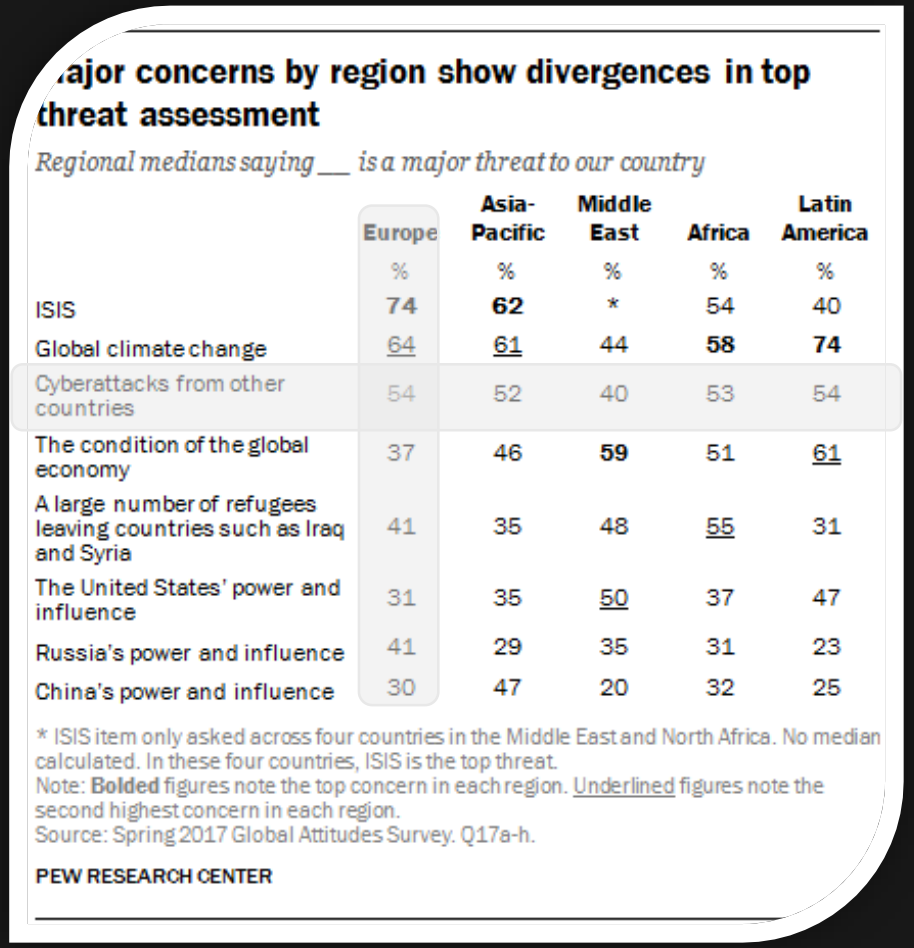
# THREAT PERCEPTION, REALITY & IMPACT

# Citizens' perception of cyber-threats from other countries

## Cyberattacks from other countries #3 global top risk




## Regional Ranking



**...ajor concerns by region show divergences in top threat assessment**

*Regional medians saying ___ is a major threat to our country*

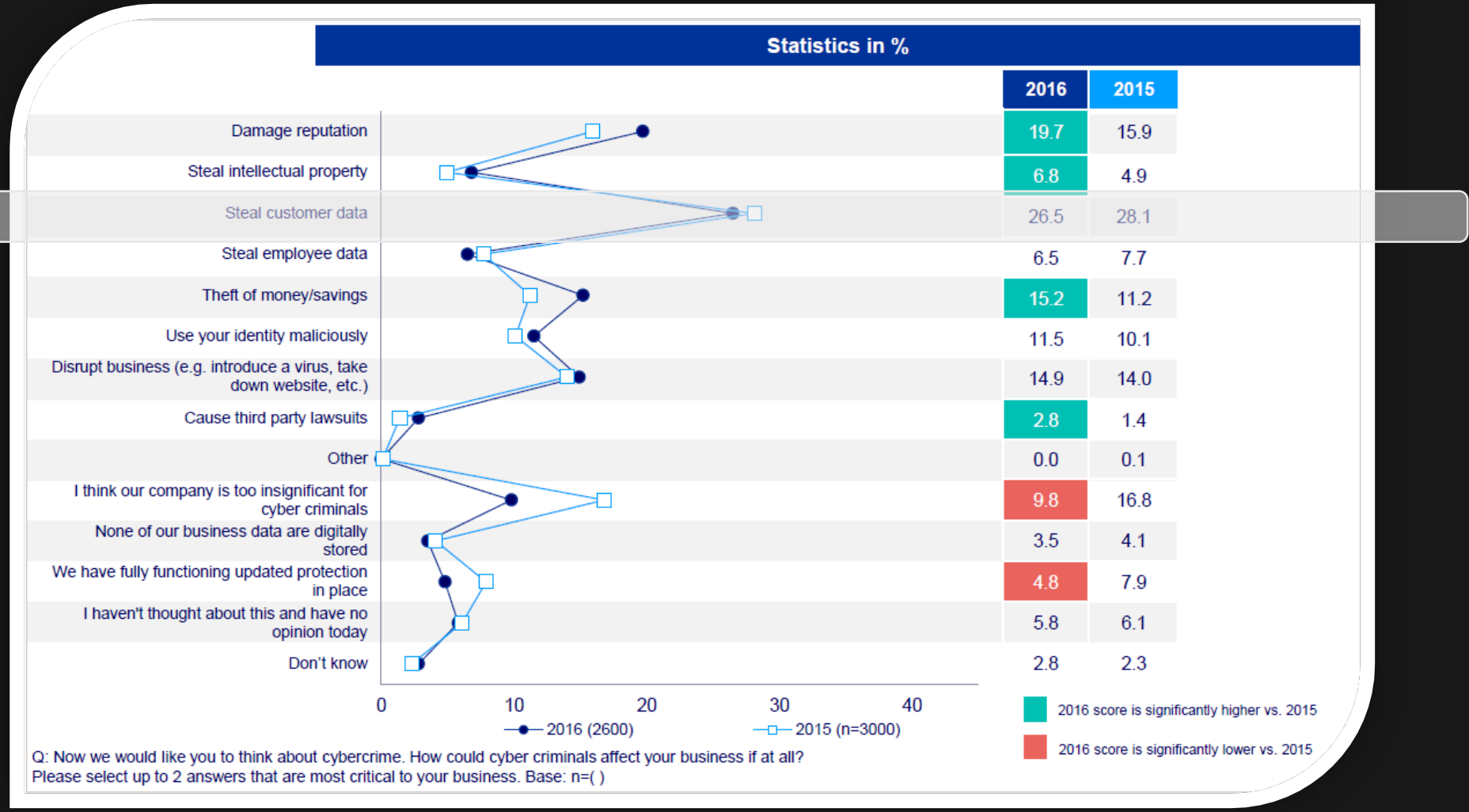
| | Europe | Asia-Pacific | Middle East | Africa | Latin America |
|---|---|---|---|---|---|
| | % | % | % | % | % |
| ISIS | **74** | **62** | * | 54 | 40 |
| Global climate change | 64 | 61 | 44 | **58** | **74** |
| Cyberattacks from other countries | 54 | 52 | 40 | 53 | 54 |
| The condition of the global economy | 37 | 46 | **59** | 51 | 61 |
| A large number of refugees leaving countries such as Iraq and Syria | 41 | 35 | 48 | 55 | 31 |
| The United States' power and influence | 31 | 35 | 50 | 37 | 47 |
| Russia's power and influence | 41 | 29 | 35 | 31 | 23 |
| China's power and influence | 30 | 47 | 20 | 32 | 25 |

* ISIS item only asked across four countries in the Middle East and North Africa. No median calculated. In these four countries, ISIS is the top threat.
Note: **Bolded** figures note the top concern in each region. Underlined figures note the second highest concern in each region.
Source: Spring 2017 Global Attitudes Survey. Q17a-h.

PEW RESEARCH CENTER

Source: Global Attitudes, Pew Research Center 2017.

# SMEs' perception of cyber-attacks



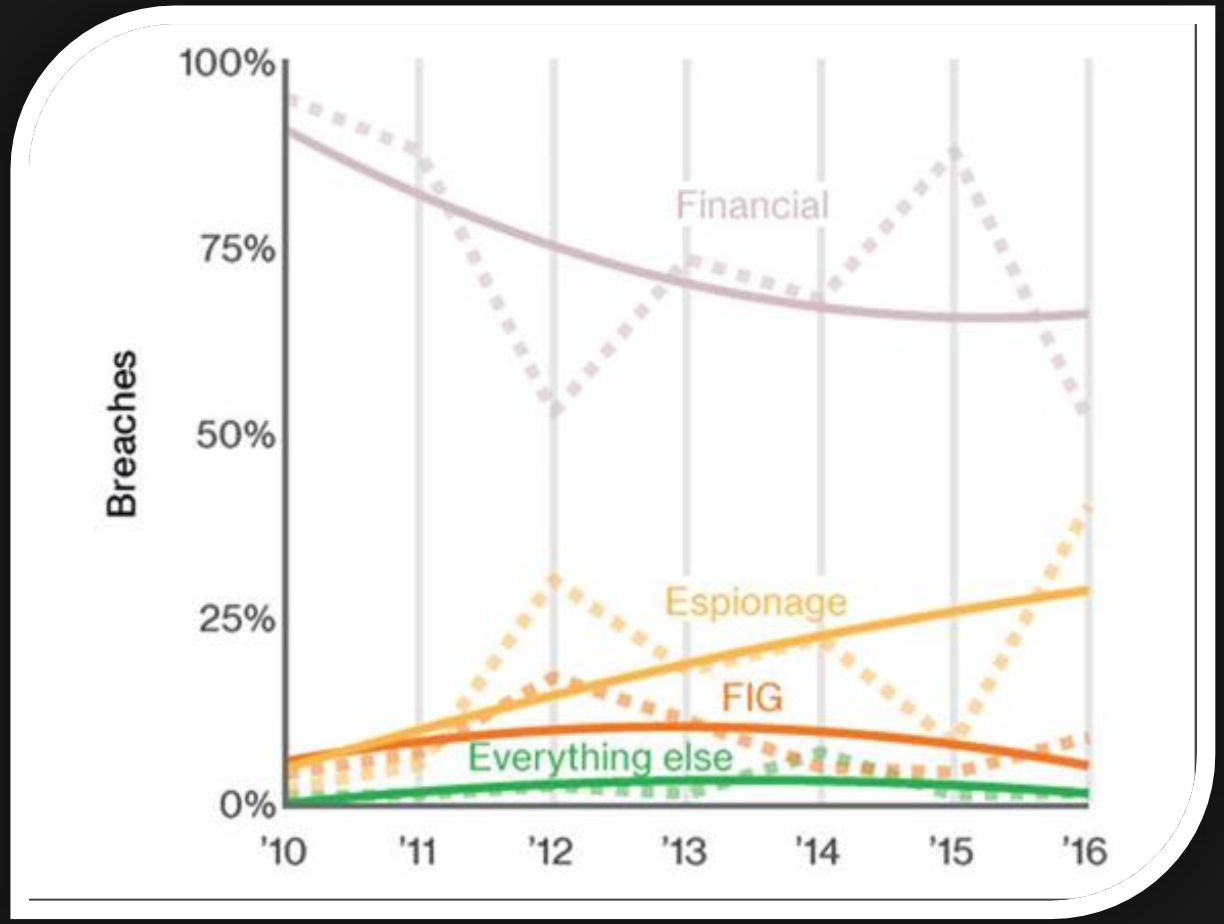

Source: Zurich Global Survey 2016

# Multinational firms' perception of cyber-attacks

- 20 % of global organizations rank **cyber espionage as the most serious threat to their business,**
- 20 % U.S. organizations have suffered a cyber espionage-related attack in the last year.
- Businesses in Italy (36 %), France (24 %), Germany (20 %) and Netherlands (17 %) topped the list for regions who fear cyber espionage the most.
- As more of our critical data is being moved online, nation states are now targeting businesses.

Source: Trend Micro 2017

# Reality: Global Cyber-attack trend



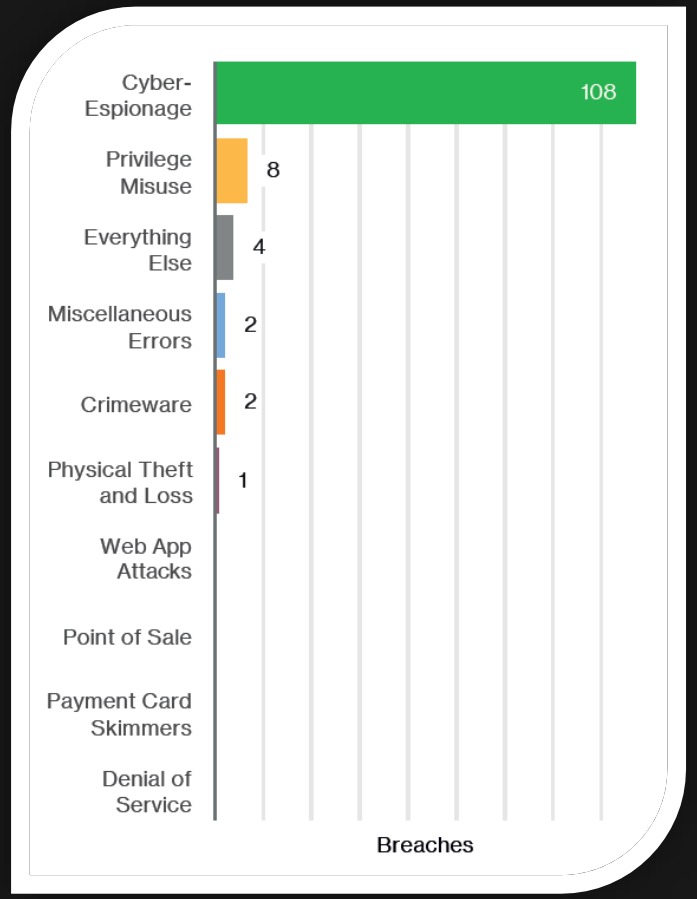

*ESPIONAGE 25 % OF ALL CYBER ATTACKS*

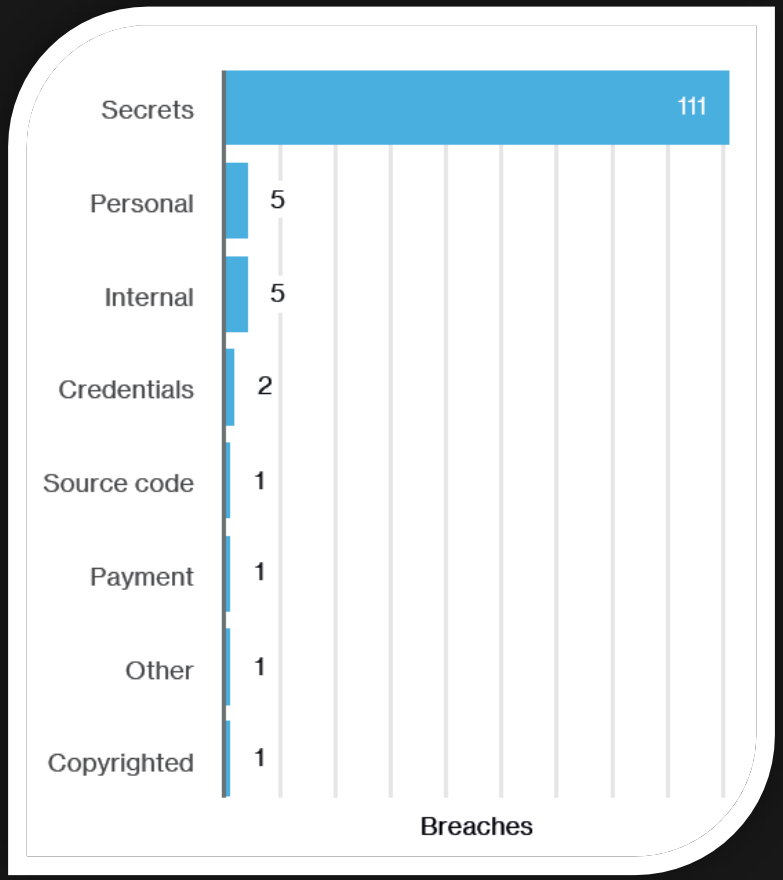
Sectors targeted by **espionage:**

- Manufacturing
- Public Administration
- Educational services

Source: Verizon 2017 Data Breach Investigations Report 10th Edition

# Manufacturing sectors : 94 % of all attacks motivated by economic espionage



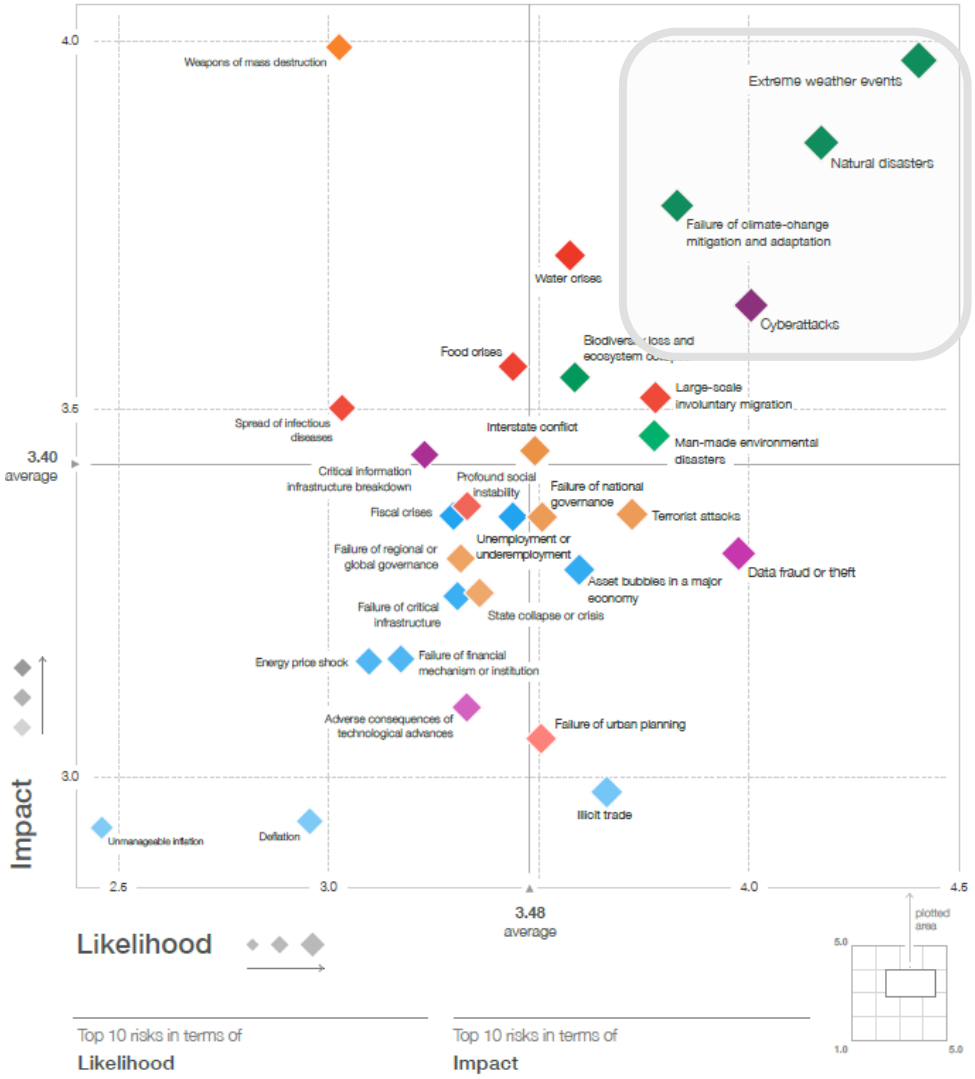




*Cyber-theft: 94 % OF ALL CYBER ATTACKS*

Manufacturing sector include: mechanical, physical or chemical transformations of materials, substances, components into new products."

Source: Verizon 2017 Data Breach Investigations Report 10th Edition

# WEF – Global Risk Report 2018




Source: [World Economic Forum Global Risk Report 2018]

Over the next five years the **cost of cybercrime** to businesses is expected to be **US$8 trillion**.

Beyond its financial cost to business, cyber attacks **disrupted critical and strategic infrastructure** across the world.

This illustrates **a growing trend** of using cyberattacks to **target critical infrastructure** and strategic industrial sectors, in a worst case scenario, attackers could trigger a **breakdown in the systems that keep societies functioning**.

Many of these attacks are thought to be **state sponsored.**

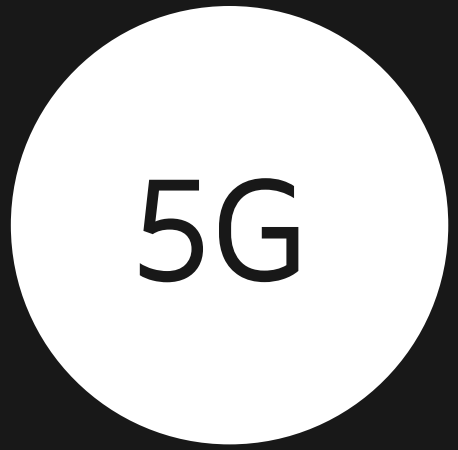
**>400 BUSD ~1 % GDP**

**Total global cost of cyber crime and espionage**

Source: Estimating the Global Cost of Cybercrime, Intel Security, 2014

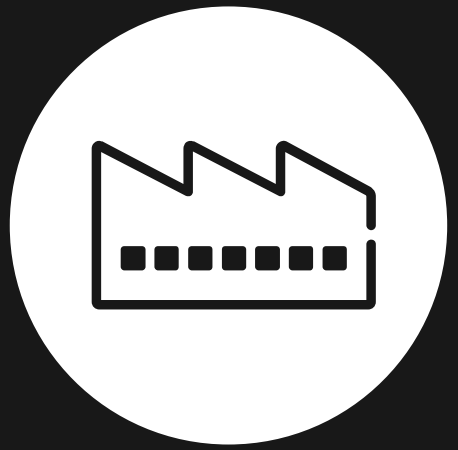
# The next frontier

## 5G GAME CHANGER




Enabler for new industrial use cases

## DIGITALIZATION

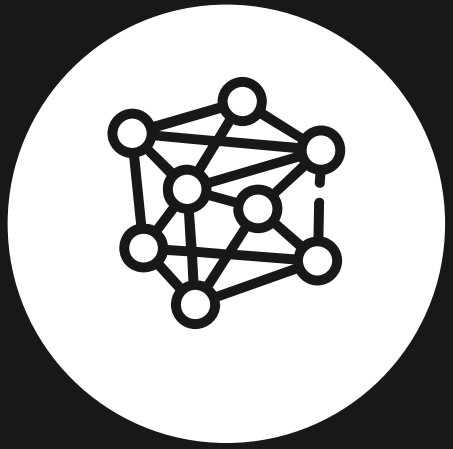


Every company will become a digital company

## SYSTEMS GO MOBILE

New attack vectors emerge - IOT

## MISSION CRITICAL ICT INFRASTRUCTURE



More value, concentrated more attacks

**RETURNS FROM ATTACKS WILL GROW IF THE COST OF UNDERTAKING ATTACKS REMAINS UNCHANGED**

# Key cyber policy objectives


INCREASE AWARENESS OF **ALL** TYPES OF THREATS

BUILD CAPABILITY: DETECT, PROTECT, RESPOND, .....

PROTECTING CRITICAL SECTORS IS A MOVING TARGET

PREMEPTIVE POLICY MEASURES NECESSARY

CYBER RESILIENCE: TECHNOLOGY, PROCESSES & PEOPLE