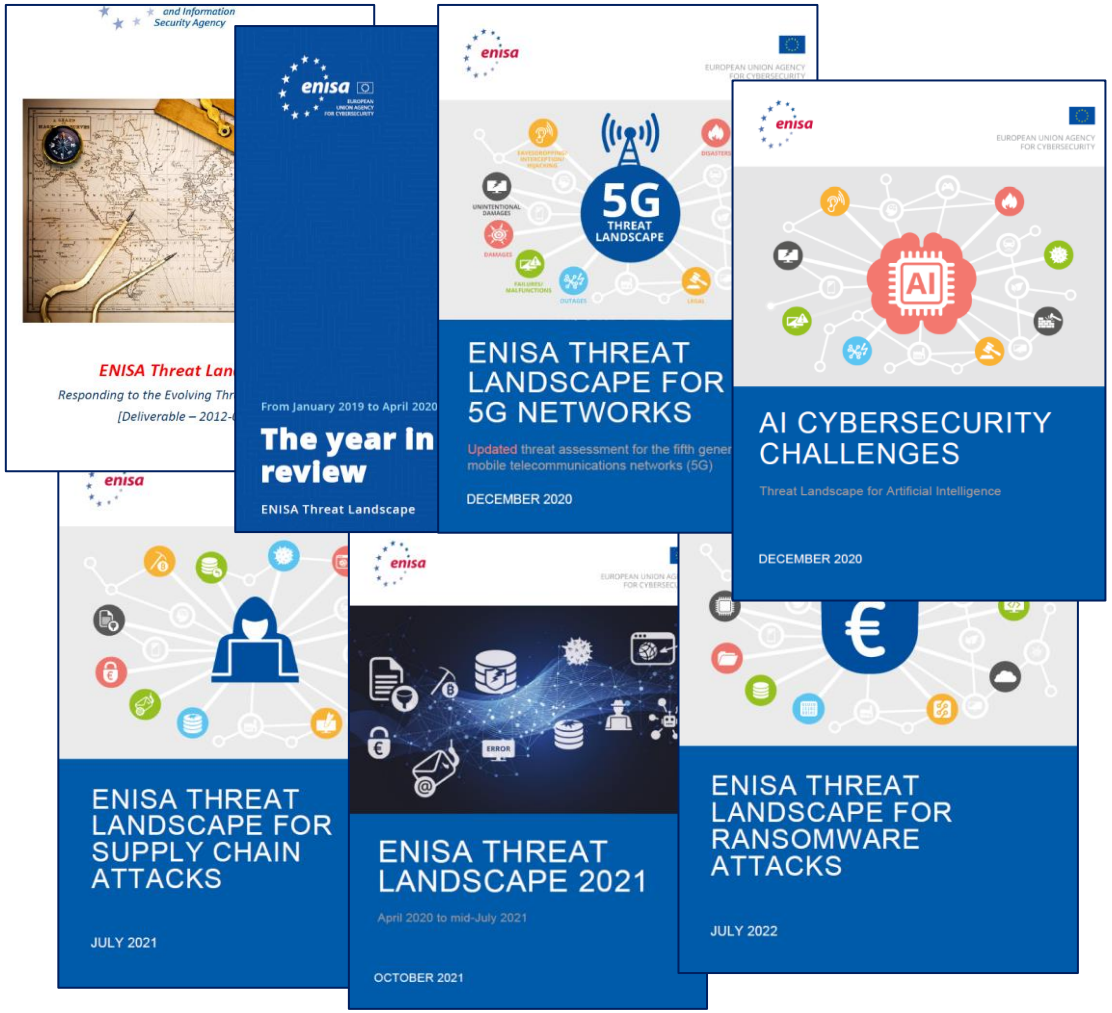
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA'S THREAT LANDSCAPE 2022

Ifigeneia Lella, Cyber Security Expert
ENISA

16 | 03 | 2023

ENISA THREAT LANDSCAPE TRADITION

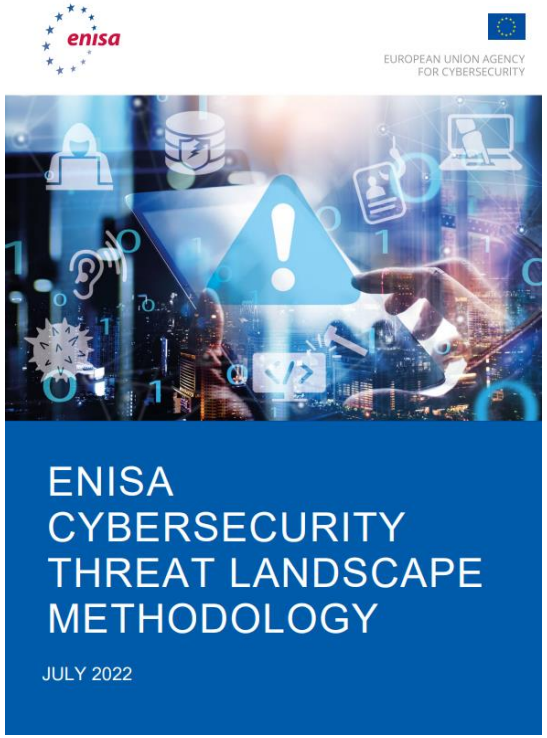


It's reflecting on the PAST to prepare for the FUTURE

10 YEARS

THREAT LANDSCAPE METHODOLOGY

WHAT DID WE DO? WHAT IS IT ABOUT?



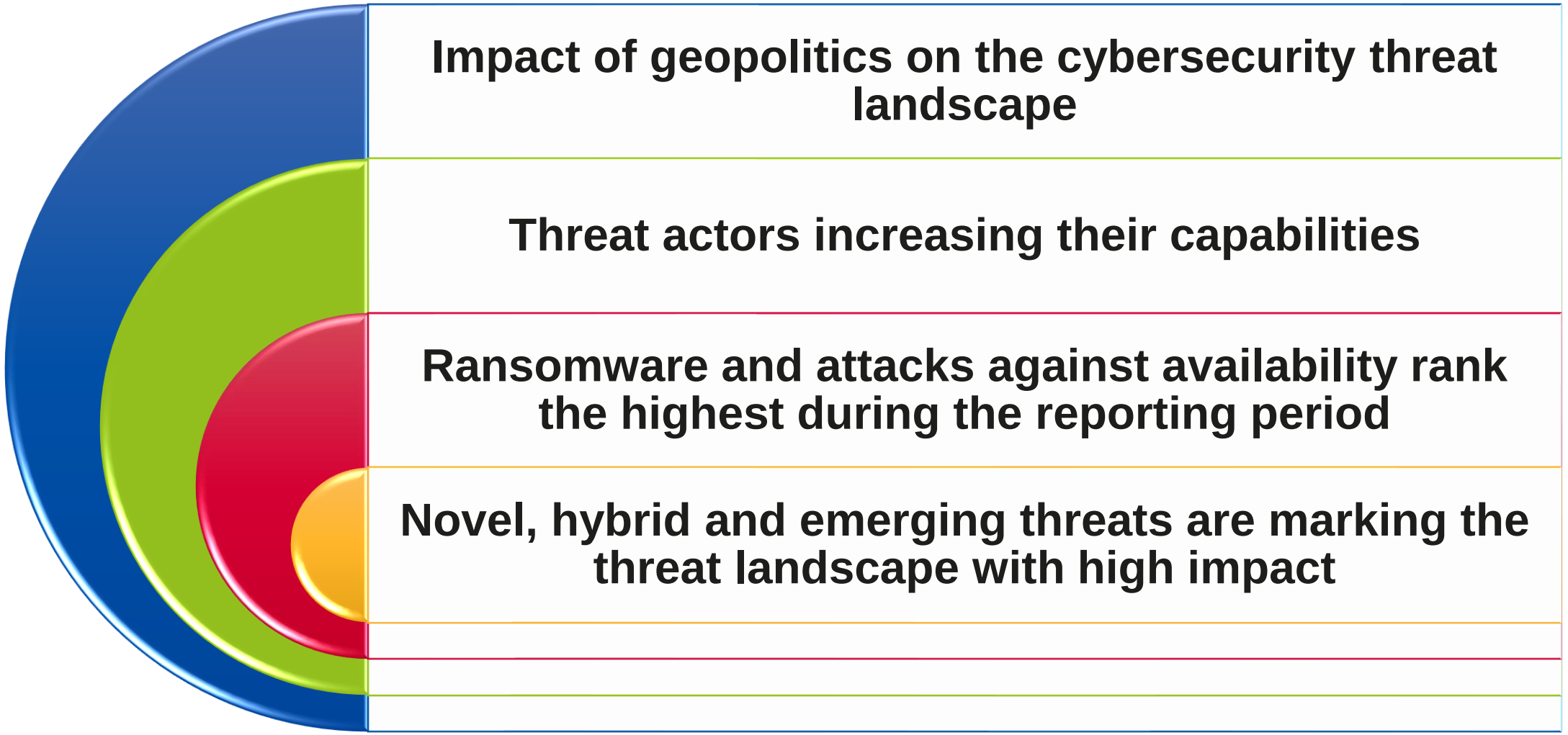
The ENISA Cybersecurity Threat Landscape (CTL) Methodology describes a systematic process for relevant data collection and analysis, to be used for the formation of CTLs

By establishing a methodology to develop threat landscapes, ENISA aims to set a baseline for the transparent and systematic delivery of horizontal, thematic, and sectorial cybersecurity threat landscapes

ENISA THREAT LANDSCAPE 2022

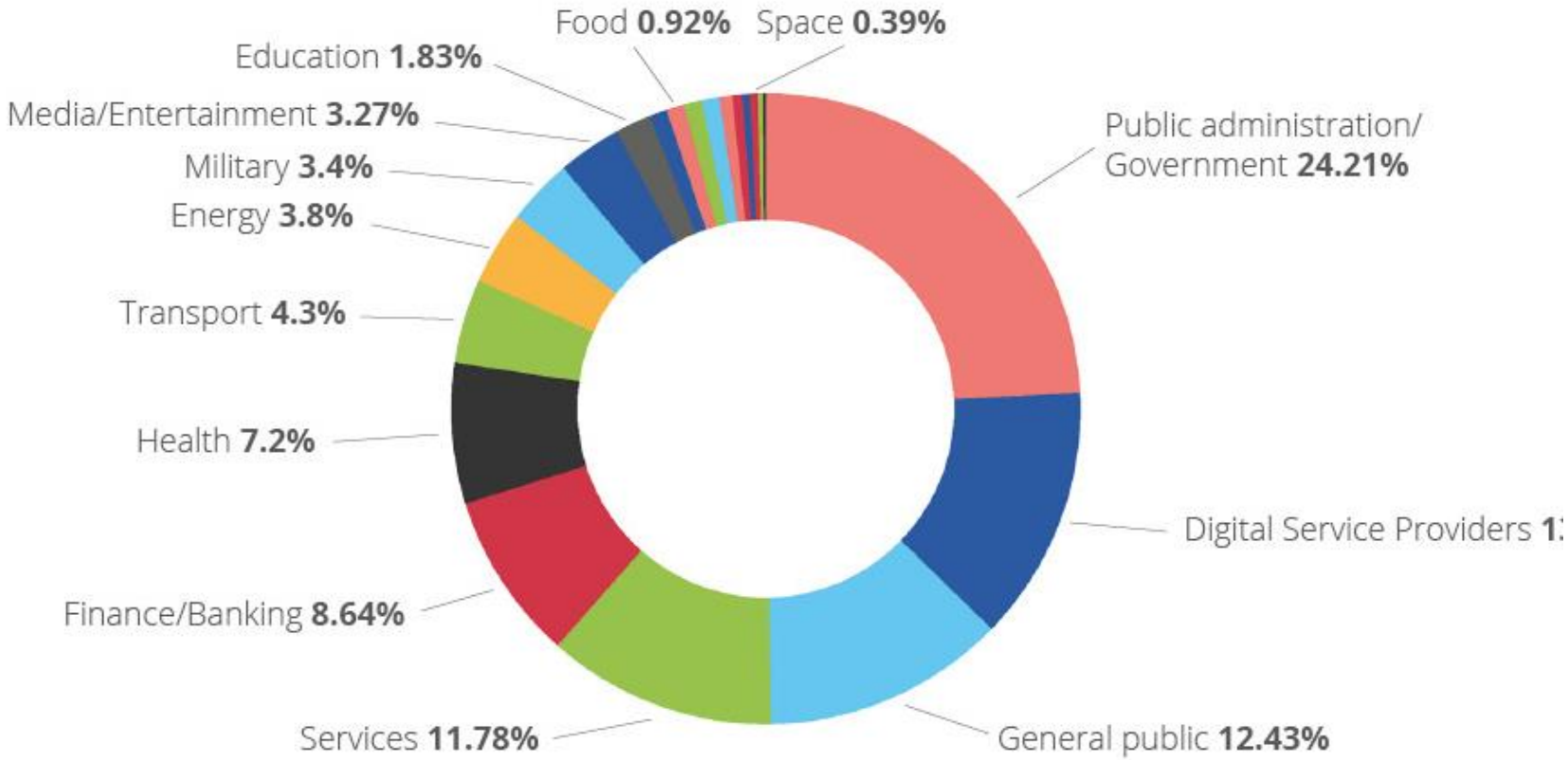
- Data related threats (e.g. data leakage, data breach etc.)
- Availability related threats (e.g. DoS, DDoS, RDoS, botnets etc.)
- Misinformation - disinformation
- Supply chain threats
- Social engineering threats (spear phishing/phishing, Smishing/Vishing, BEC etc.)
- Ransomware
- Malware (e.g. RAT, Trojan, Miner/Crypto, Trojan, Spyware etc.)
- Threats against availability – internet threats (e.g. BGP hijacking, DNS attacks, defacement etc.)

ENISA THREAT LANDSCAPE 2022



SECTORS BREAKDOWN

large number of incidents targeting public administration and government and digital service providers

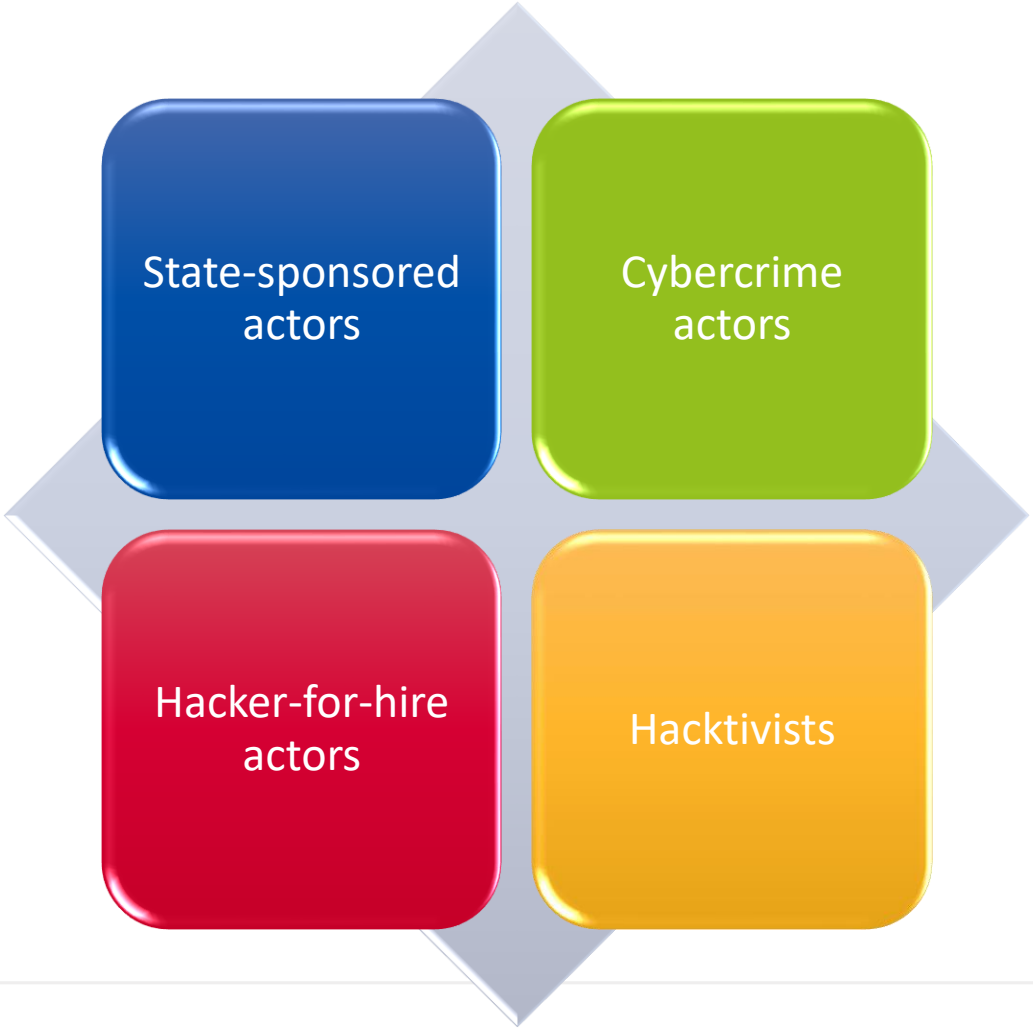


THREAT ACTORS

THREAT ACTORS

- **Integral** part of overall threat assessment
- **Entities** aiming to carry out **a malicious act** by taking advantage of existing **vulnerab**ilities with the intent to harm their victims
- **Understanding how threat actors** (trends, targets , techniques, tools and procedures) **think and act and their motivations and goals** are essential for a good cyber security strategy

4 types of threat actors considered



STATE-SPONSORED ACTORS

- Increase 0-day and other critical vulnerabilities
- Heightened risk for Operational Technology networks
- Destructive attacks part of state actors' operations
- Public attribution and legal actions continue
- Armies of cyber volunteers?
- focus on supply chain compromises
- Geopolitics continue to influence cyber operations

CYBER CRIMINALS

- Target industrial sector
- cloud opportunities
- Continuous 'retirements' and rebranding
- Data exfiltration without ransomware
- cybercrime ecosystem thrives
- Russia Ukraine conflict impact

HACKERS-FOR HIRE AND HACTIVISTS

HACKERS-FOR HIRE

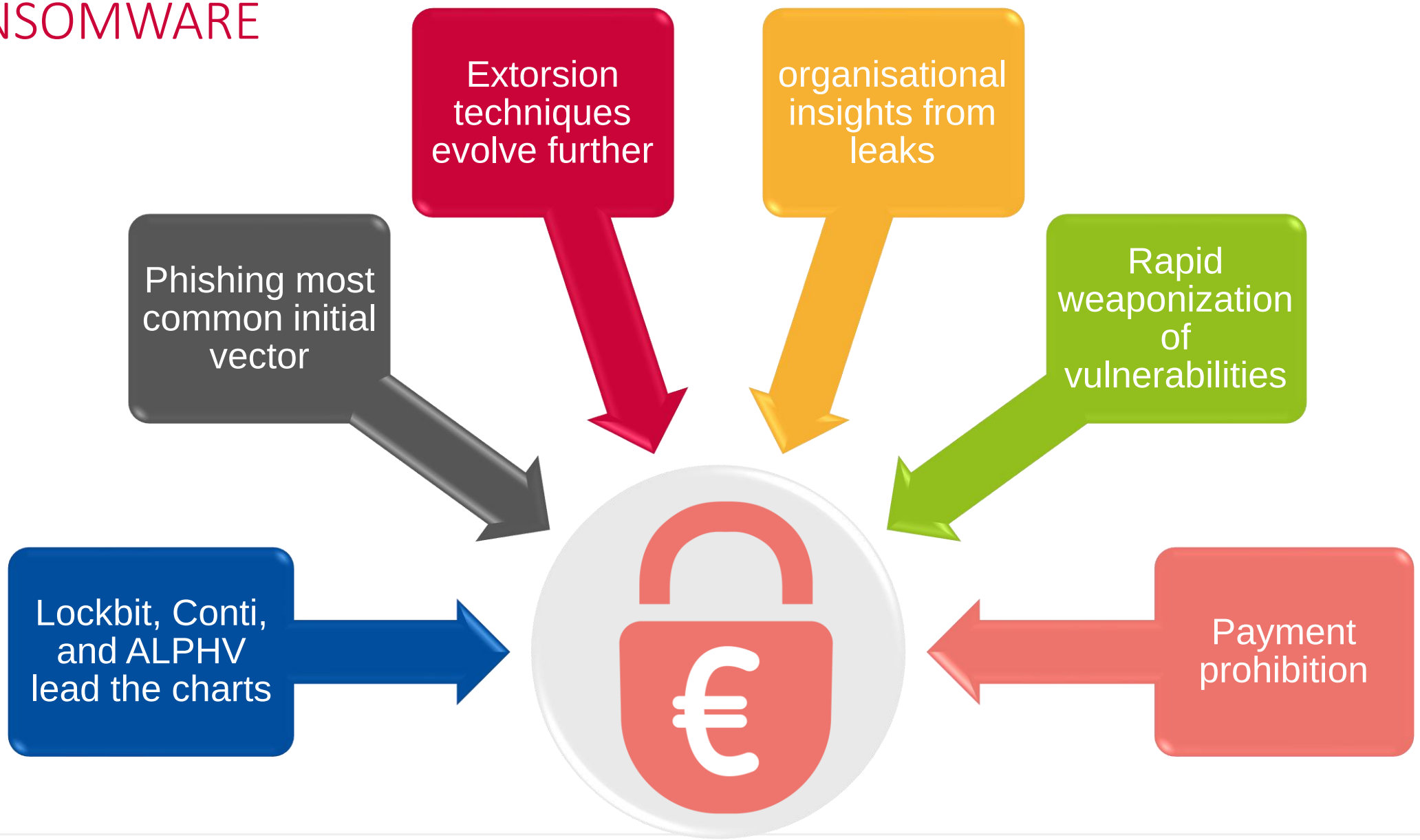
- Access-as-a-Service market continues to enable state actors
- The Pegasus case - Surveillance and targeting of civil society

HACTIVISTS

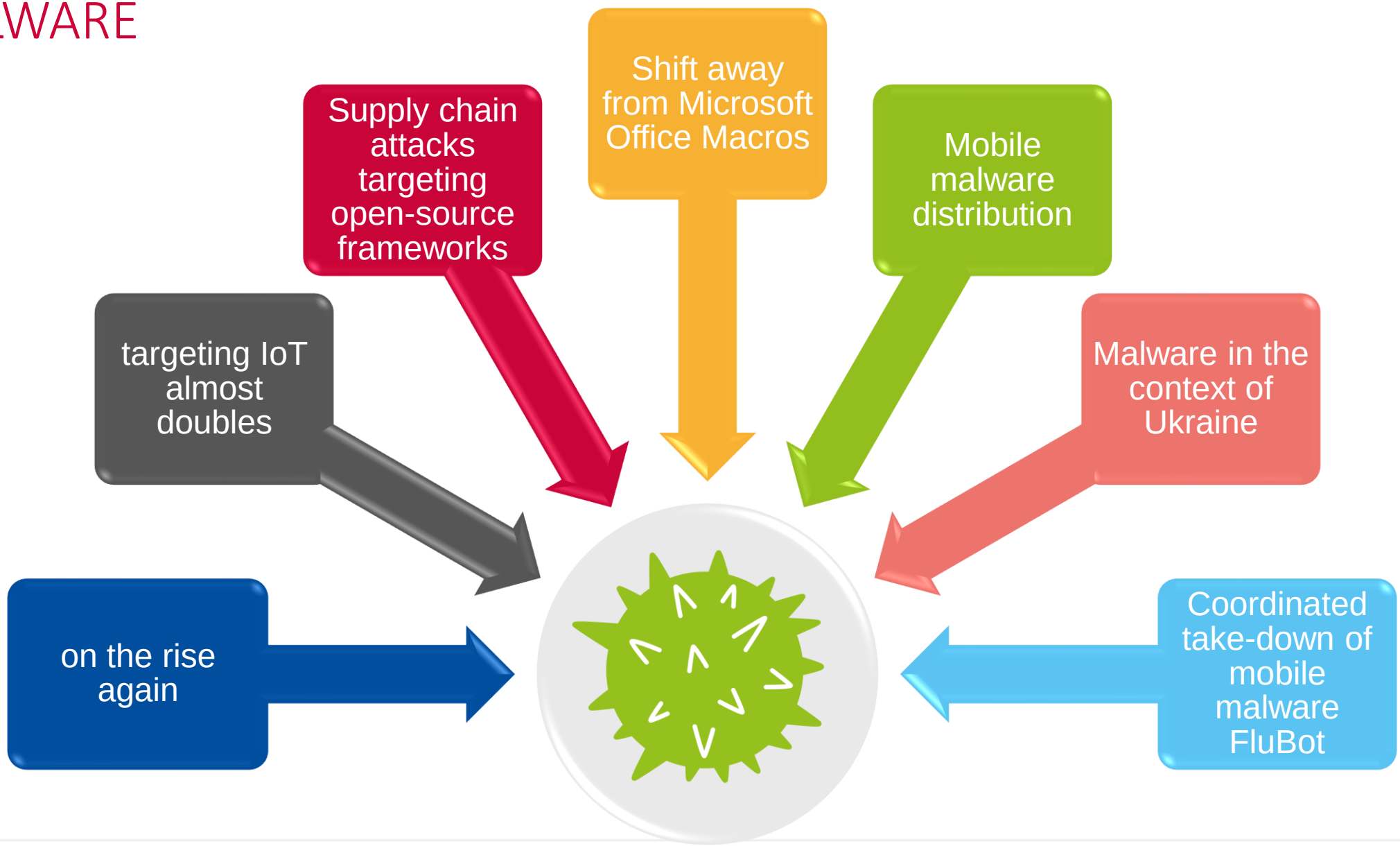
- A new wave of hacktivism
- Hacktivist Ransomware

PRIME THREATS

RANSOMWARE

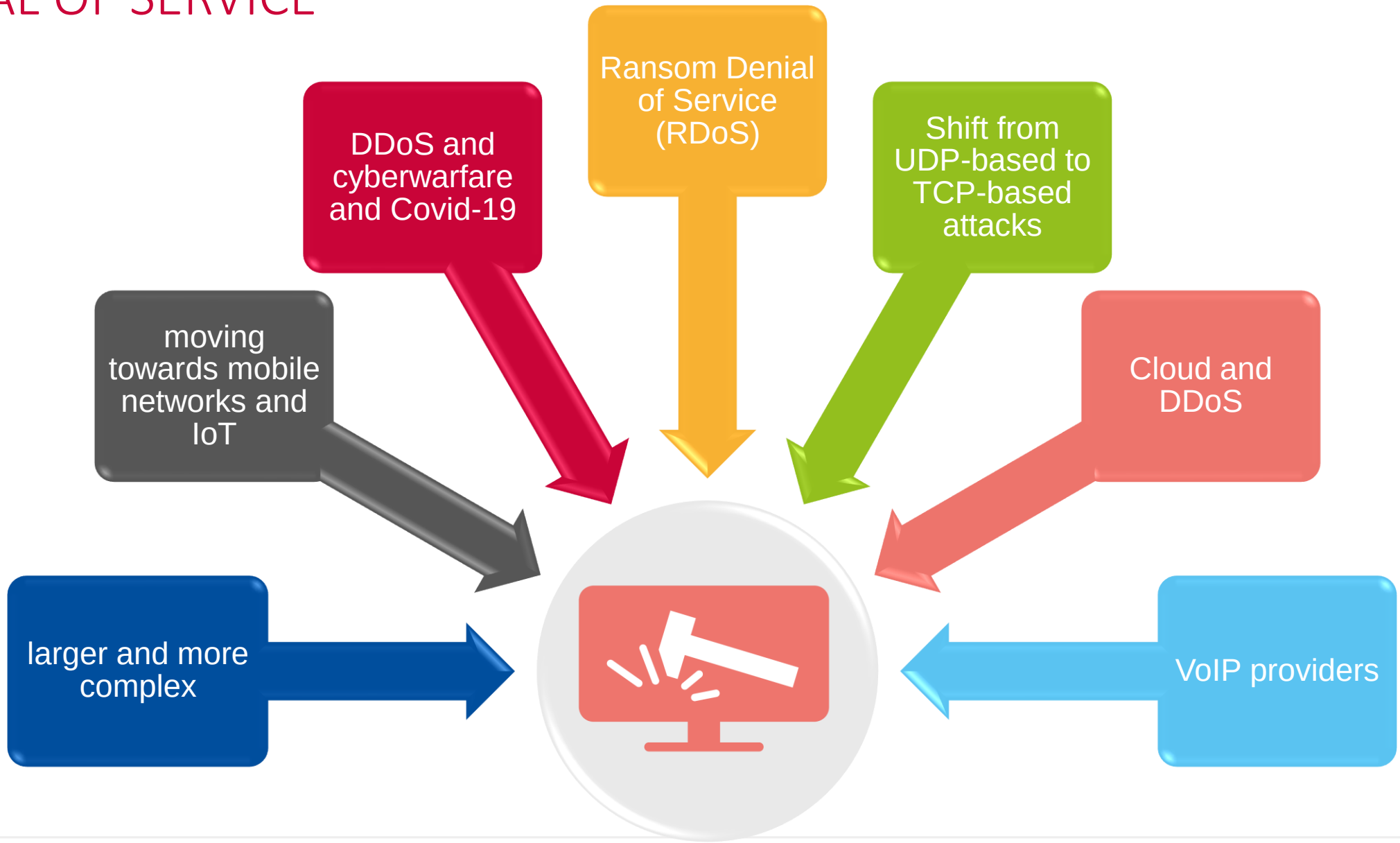

Extorsion techniques evolve further
organisational insights from leaks
Phishing most common initial vector
Rapid weaponization of vulnerabilities
Lockbit, Conti, and ALPHV lead the charts
Payment prohibition

MALWARE

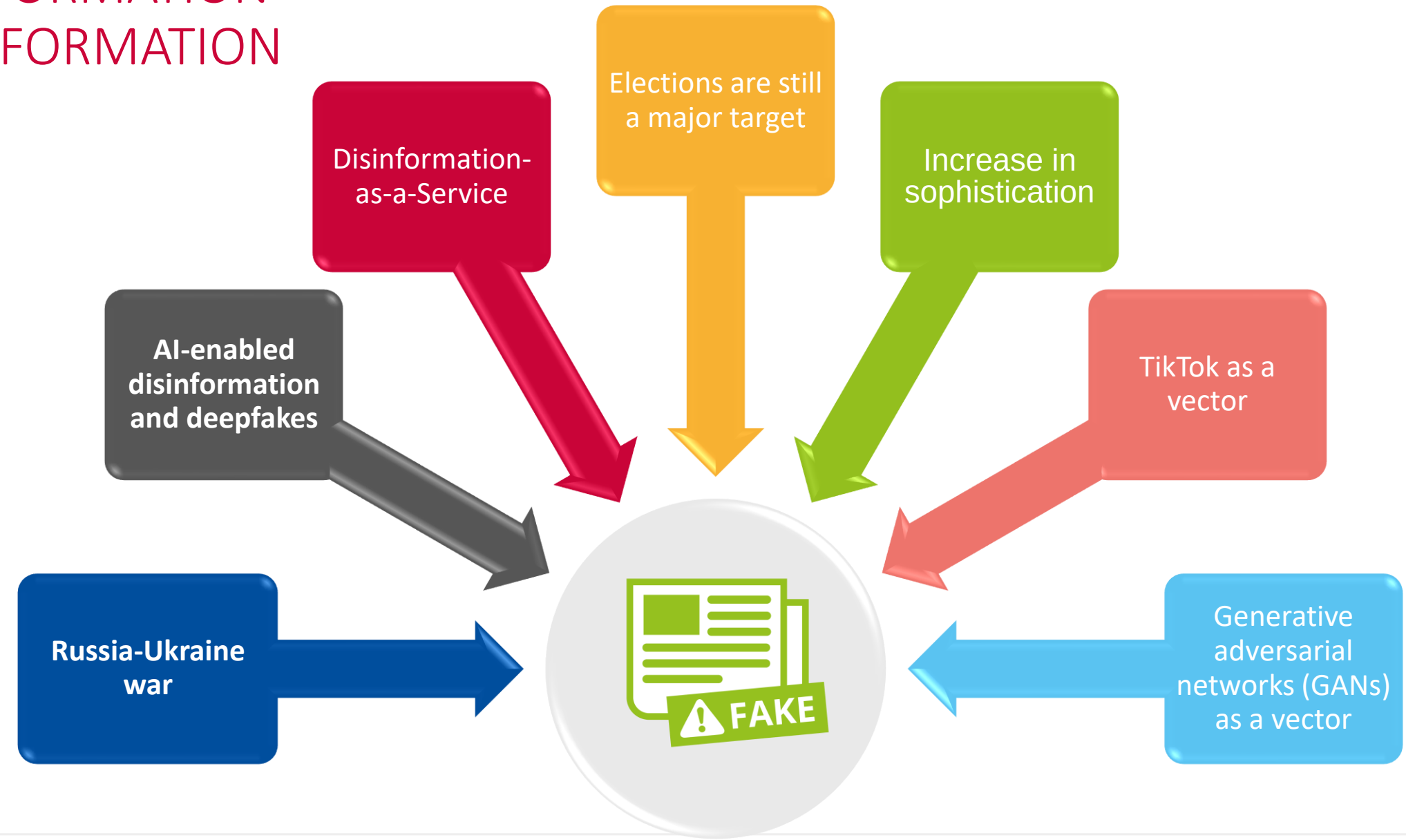

Supply chain attacks targeting open-source frameworks
Shift away from Microsoft Office Macros
Mobile malware distribution
targeting IoT almost doubles
Malware in the context of Ukraine
on the rise again
Coordinated take-down of mobile malware FluBot

SOCIAL ENGINEERING THREATS

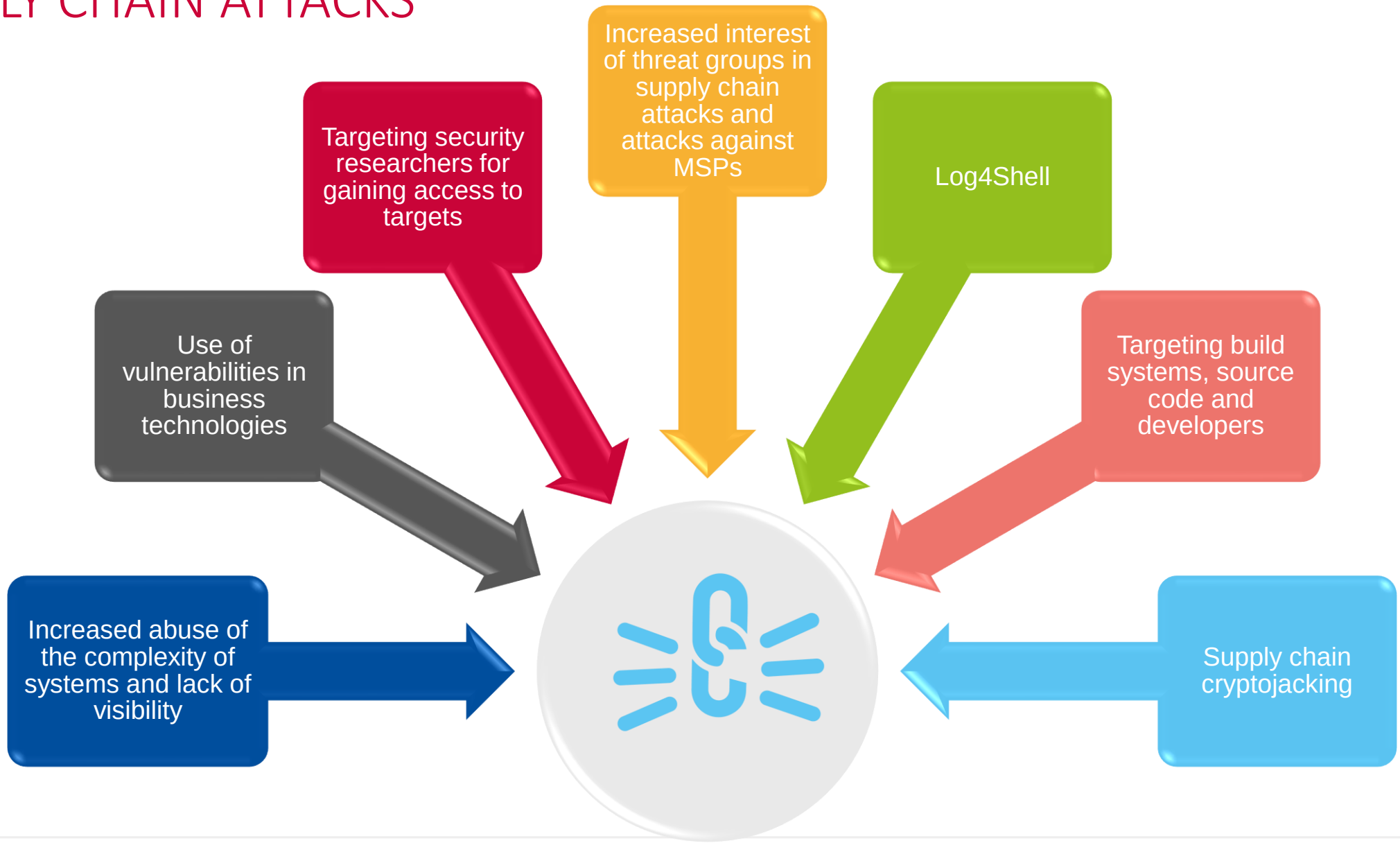
DENIAL OF SERVICE



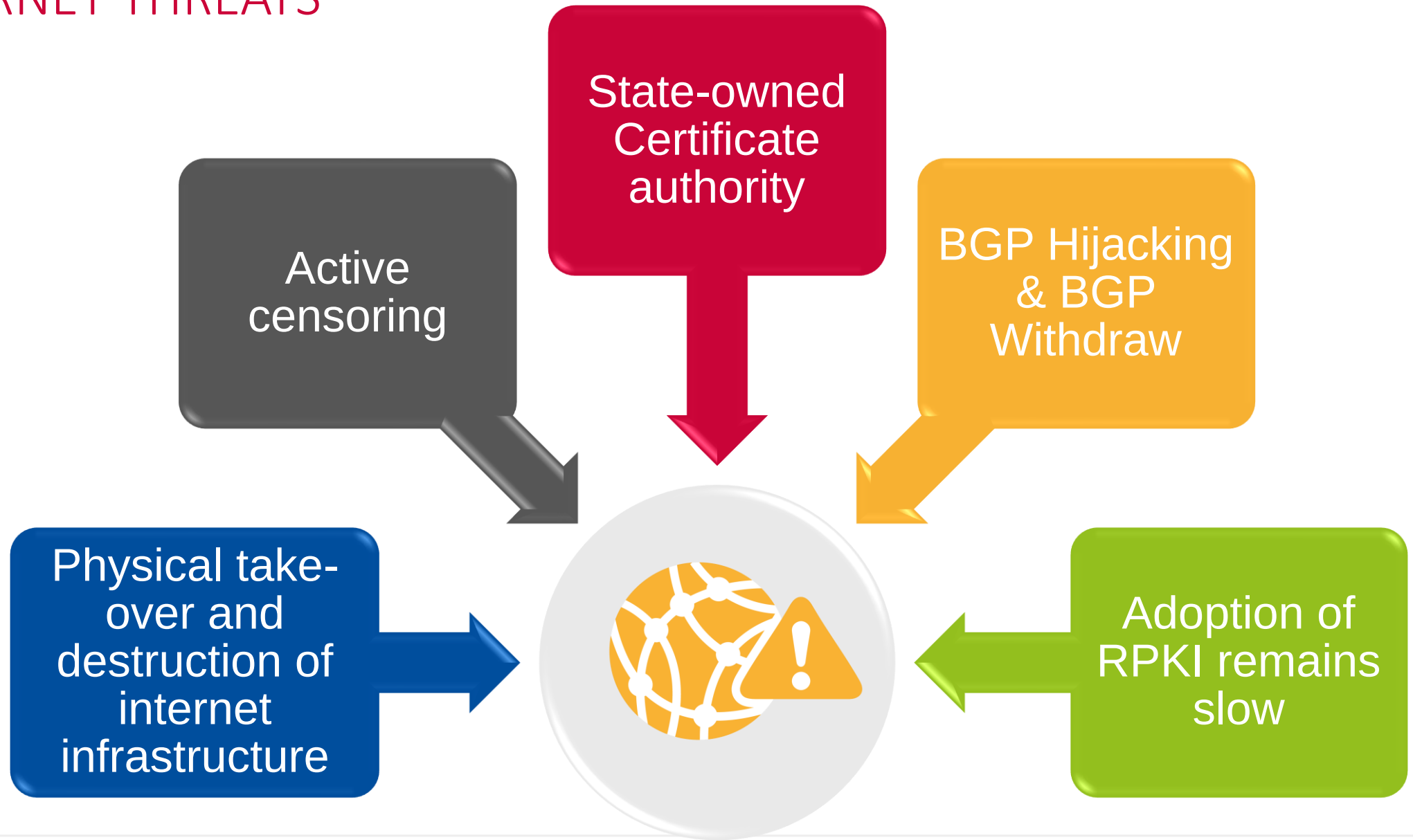
DISINFORMATION-MISINFORMATION



SUPPLY CHAIN ATTACKS



INTERNET THREATS



SUMMARY

Threat actors use whatever is more relevant and evolve and adapt to the changing of technologies

Good practices and coordinated actions are important to reach a common high level of cybersecurity.

Cyber attacks has increased by a lot compared to last year but we still lack the visibility

Information Sharing is caring…

It helps potential victims , it helps researchers.. it also helps cybersecurity authorities and ENISA

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

info@enisa.europa.eu

www.enisa.europa.eu