

THE CYBERSECURITY THREAT LANDSCAPE FOR 2023 AND BEYOND: ENISA EFFORTS

Dr Apostolos Malatras
Team Leader, Knowledge and Information



ENISA THREAT LANDSCAPE TRADITION



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

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 - HIGHLIGHTS



Impact of geopolitics on the cybersecurity threat landscape



Threat actors increasing their capabilities



Ransomware and attacks against availability rank the highest during the reporting period

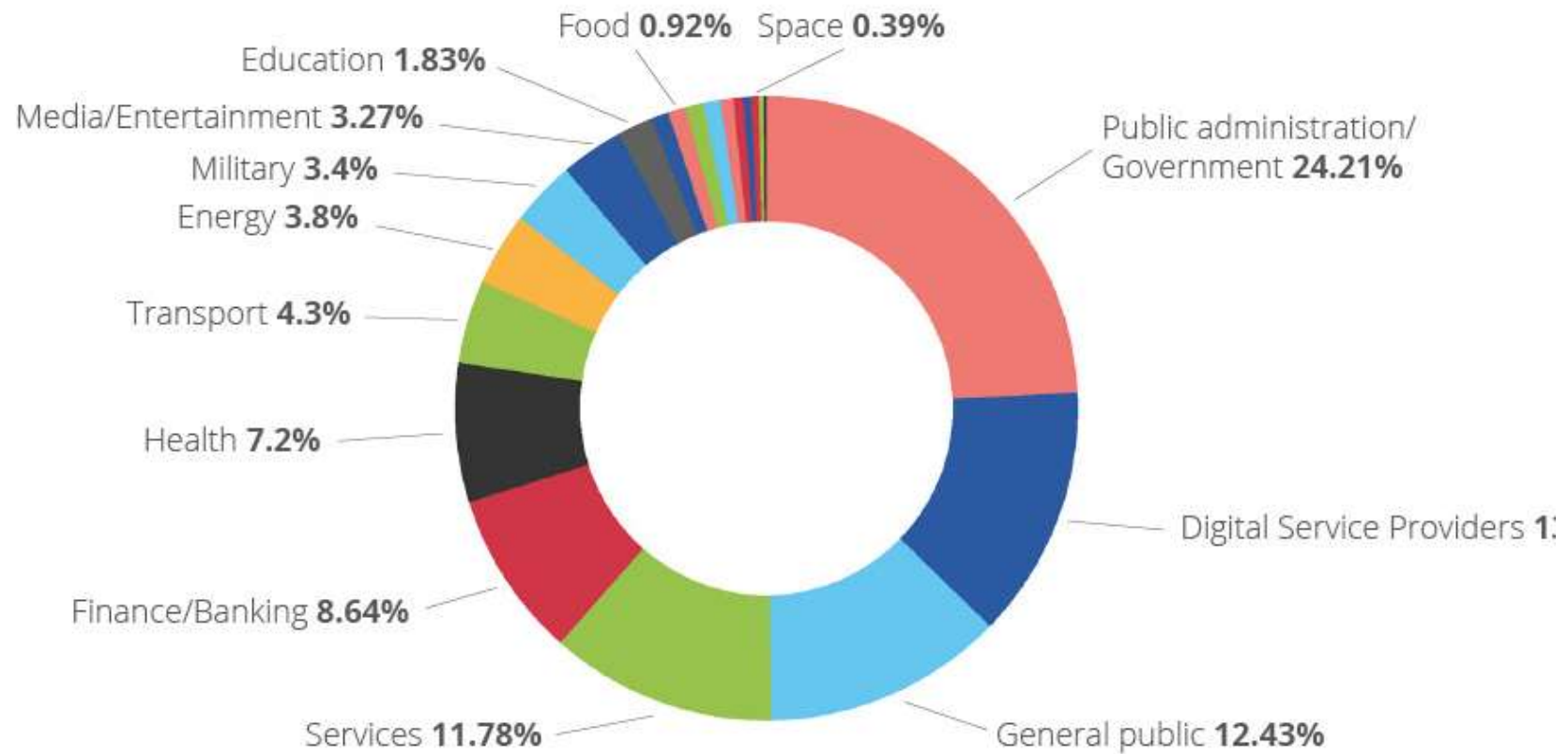


Novel, hybrid and emerging threats are marking the threat landscape with high impact

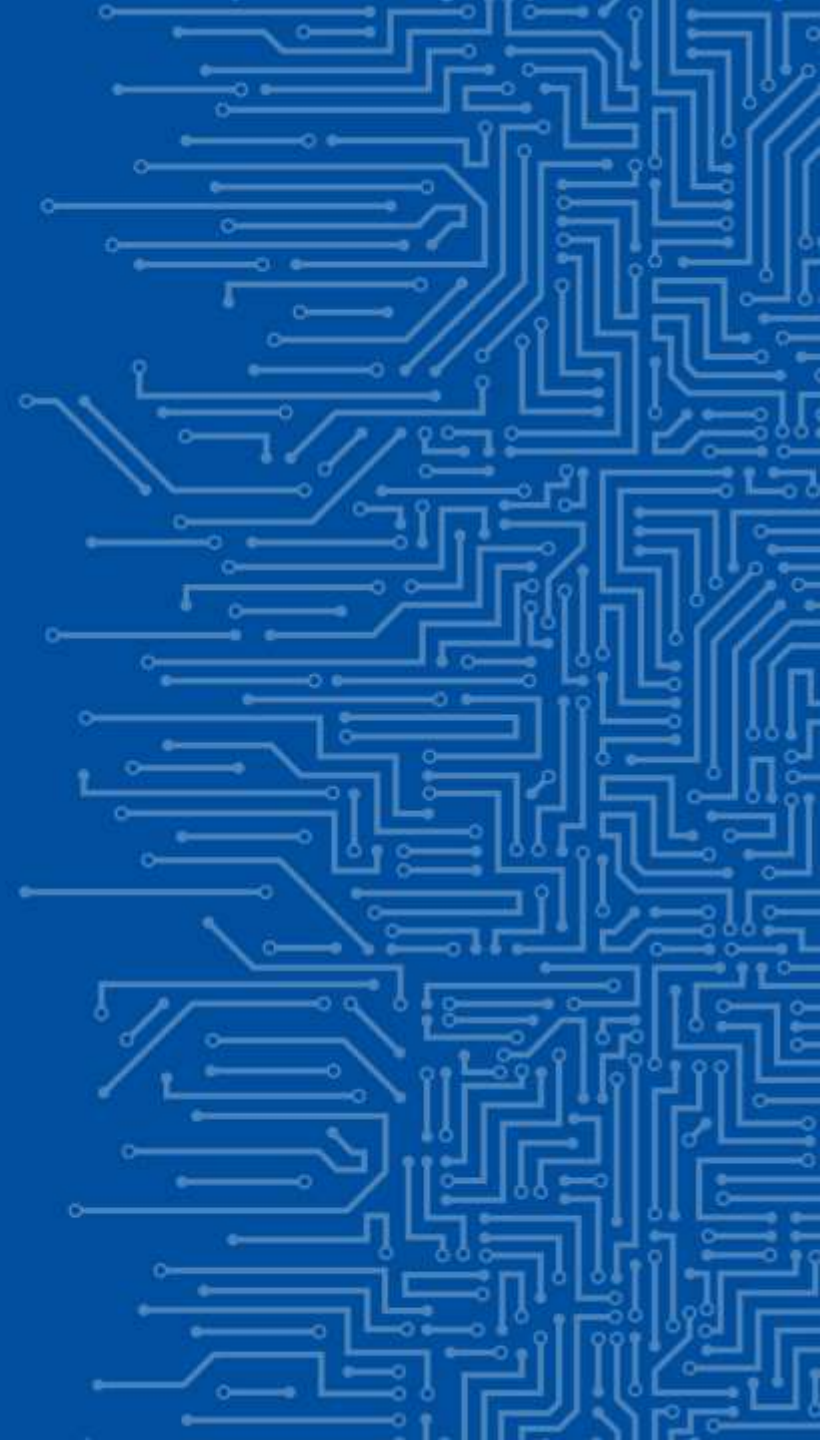
SECTORS BREAKDOWN



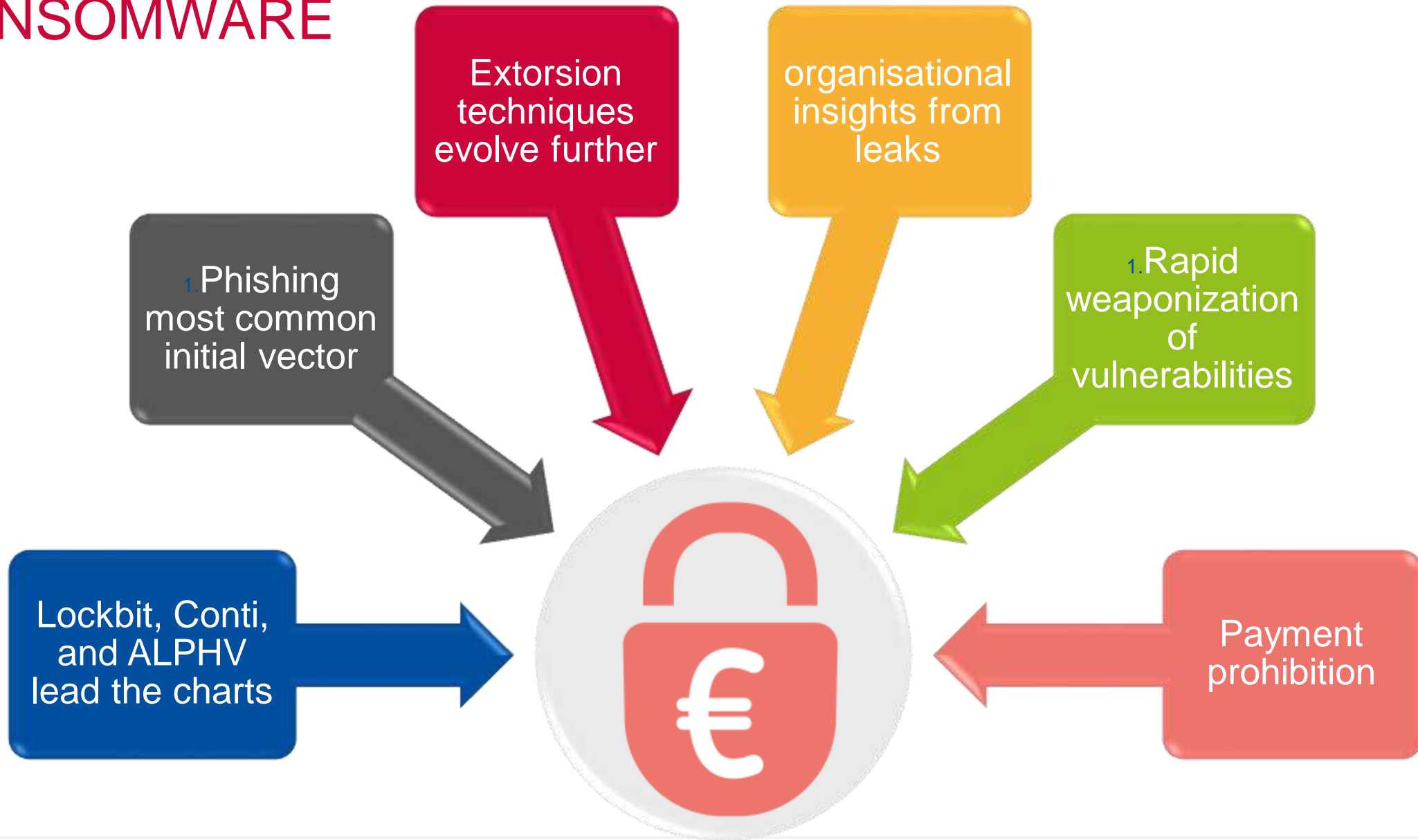
Large number of incidents targeting public administration and government and digital service providers



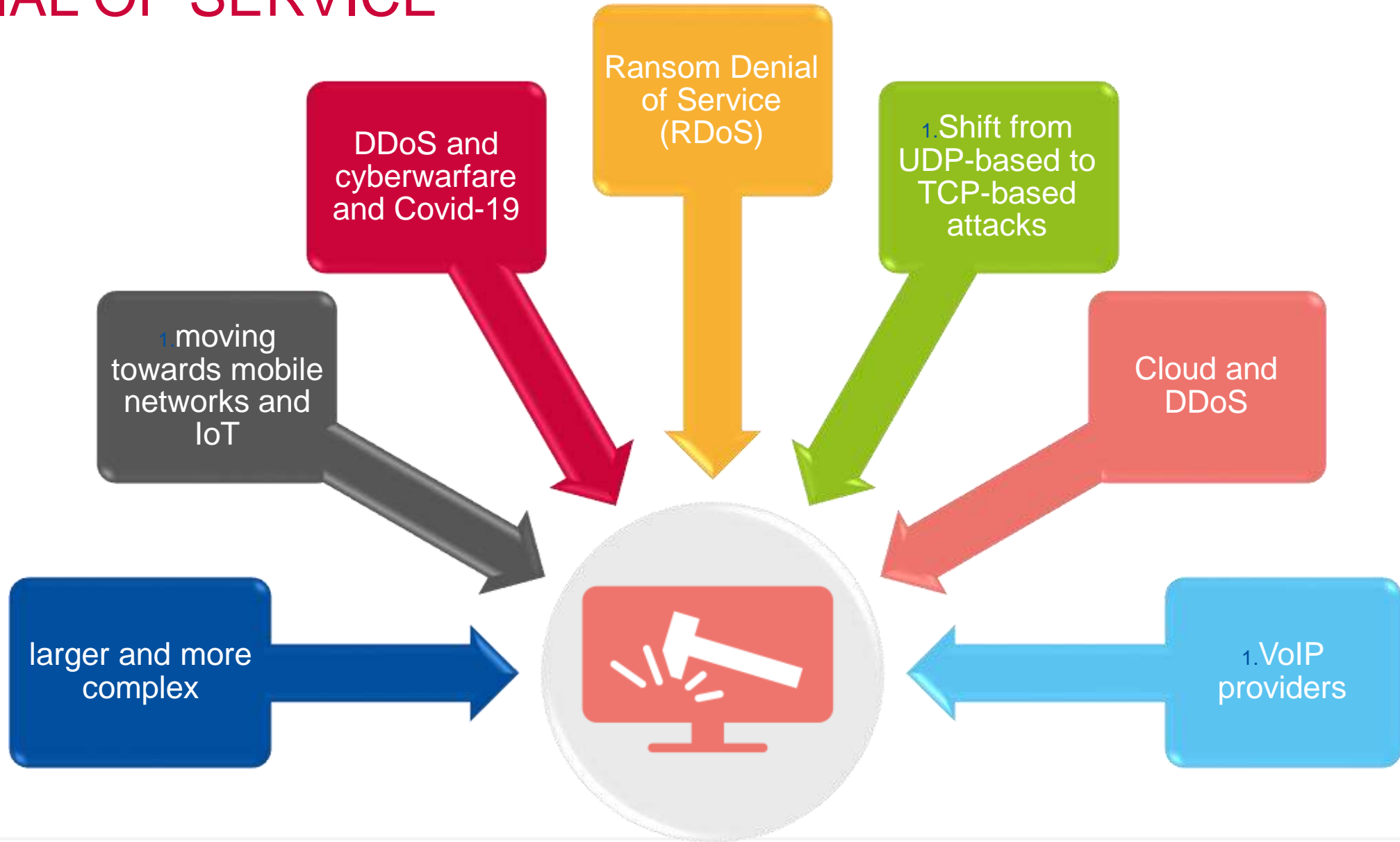
PRIME THREATS



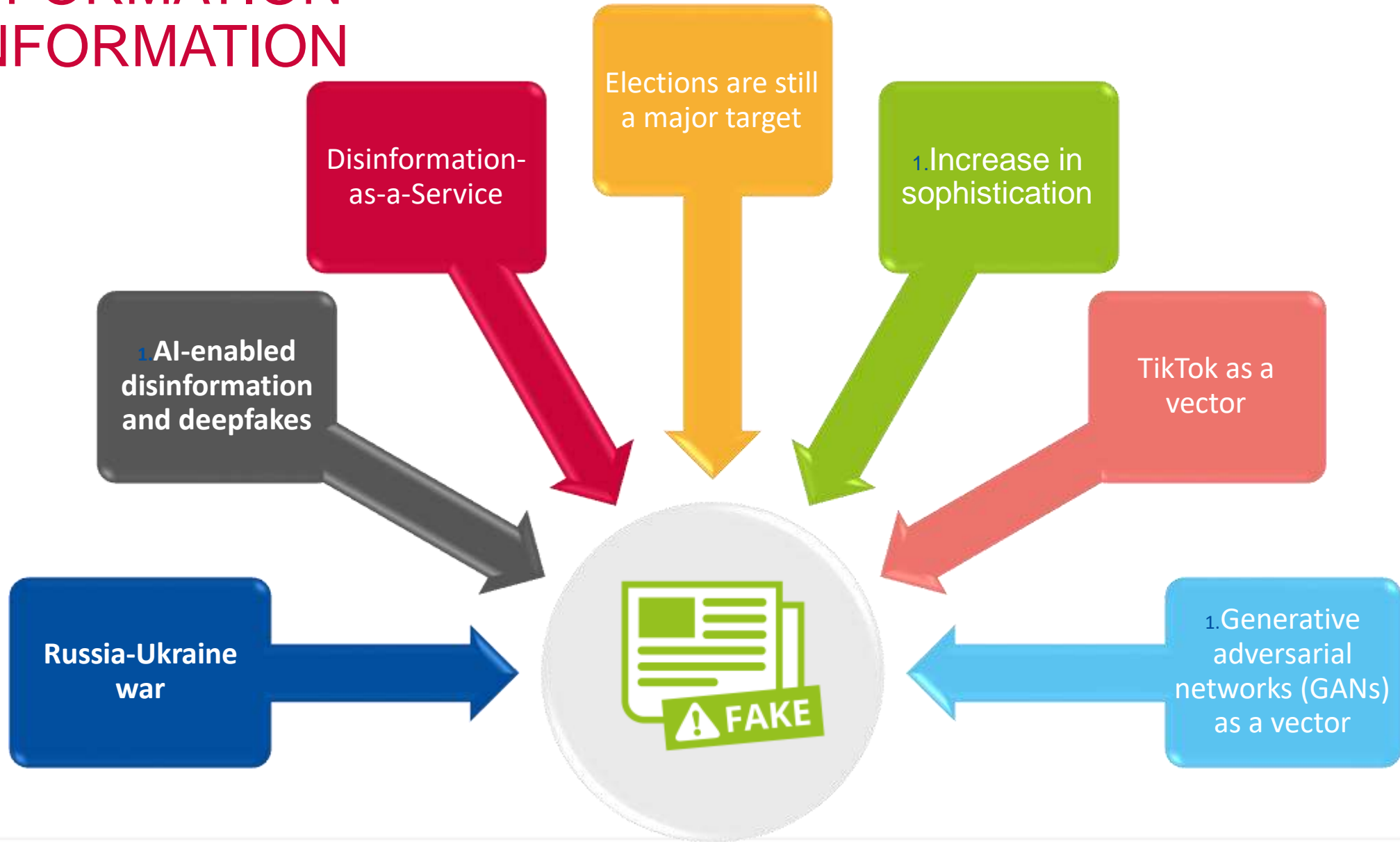
RANSOMWARE



DENIAL OF SERVICE



DISINFORMATION- MISINFORMATION



KEY FINDINGS



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

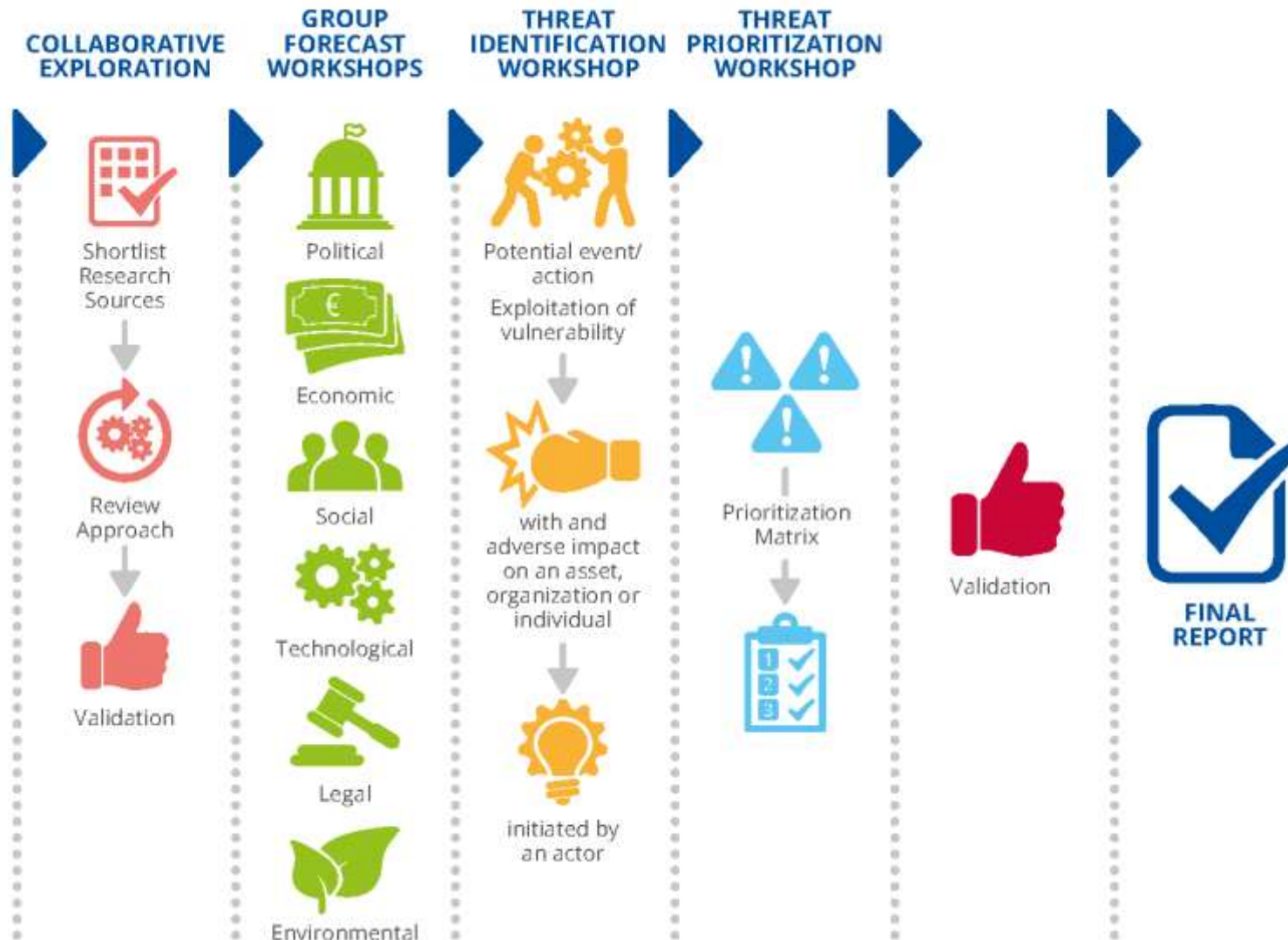
**Information Sharing is caring...
It helps potential victims , it helps researchers.. it also helps cybersecurity authorities and ENISA**

FORESIGHT ON EMERGING AND FUTURE CYBERSECURITY THREATS

TOP 10 EMERGING CYBERSECURITY THREATS FOR 2030



FORESIGHT 2030 EXERCISE



TOP 10 EMERGING CYBERSECURITY THREATS FOR 2030



THREATS 2030



1 Supply chain compromise of software dependencies

More integrated components and services from third party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side.



2 Advanced disinformation campaigns

Deepfake attacks can manipulate communities for (geo) political reasons and for monetary gain.



3 Rise of digital surveillance authoritarianism/ loss of privacy

Facial recognition, digital surveillance on internet platforms or digital identities data stores may become a target for criminal groups.



4 Human error and exploited legacy systems within cyber-physical ecosystems

The fast adoption of IoT, the need to retrofit legacy systems and the ongoing skill shortage could lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem, which can lead to security issues.



5 Targeted attacks enhanced by smart device data

Through data obtained from internet-connected smart devices, attackers can access information for tailored and more sophisticated attacks.



6 Lack of analysis and control of space-based infrastructure and objects

Due to the interconnections between private and public infrastructure in space, the security of these new infrastructures and technologies need to be investigated as a lack of understanding, analysis and control of space-based infrastructure can make it vulnerable to attacks and outages.



7 Rise of advanced hybrid threats

Physical or offline attacks are evolving and becoming often combined with cyberattacks due to the increase of smart devices, cloud usage, online identities and social platforms.



8 Skill shortage

Lack of capacities and competencies could see cybercriminal groups target organisations with the largest skills gap and the least maturity.



9 Cross border ICT service providers as a single point of failure

ICT sector connecting critical services such as transport, electric grids and industry that provide services across borders are likely to be targeted by techniques such as backdoors, physical manipulation, and denial of service and weaponised during a future potential conflict.



10 Artificial Intelligence Abuse

Manipulation of AI algorithms and training data can be used to enhance nefarious activities such as the creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots and data poisoning.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece



 info@enisa.europa.eu

 www.enisa.europa.eu

