

**REMEMBER
REMEMBER**



**THE
5TH OF
NOVEMBER**

**The
Cybersecurity
Landscape
of
2025**



1 The Fundamentals

2 The Core - CIA Triad

3 Types of Attack

4 Types of Defense

5 Real-world Examples

6 The Landscape

7 What Can You Do?



The Fundamentals

1

The Fundamentals

WHAT IS CYBERSECURITY?

The practice of protecting systems, networks, information and data from being **accessed, altered, accumulated or destroyed by unauthorized entities**.

→ It's about digital containment and protection practices

WHAT ARE WE PROTECTING?

- Personal information (Identity, credentials, bank accounts etc)
- Business data (clients' information, financial data, intellectual property etc)
- Critical services (power grids, hospitals, public services etc)

YOUR PERSONAL DATA HAVE MORE VALUE THAN YOU THINK!

1

The Fundamentals

ATTACKERS

- Individuals (either for gain or entertainment)
- Hacktivists
- Disgruntled employees
- Organized groups
- Industrial competitors
- Foreign intelligence services



TARGETS

- Individuals
- Public sectors
- Machines (from dedicated clusters of servers to IoT sensors measuring the temperature)
- Big companies
- Everyone and everything really...



MOTIVES?

- Money
- Disruption
- Data theft
- Espionage
- Geopolitics

PERSONAL DATA ARE VALUABLE!

Hackers usually target the weakest link which often is people

1

The Fundamentals

LAYERED APPROACH / MULTIPLE LAYERS OF DEFENSE

- Physical
- Perimeter
- Network Monitoring
- Access Controls
- Device Protection
- Data Protection
- User Awareness

EVER EVOLVING

- New technologies birth new threats.
- The threats are getting smarter (excessive usage of AI).
- More attack surfaces with each new smart device being brought to the public.
- Old defenses stop working.
- Unmaintained software or hardware are easy targets.

CYBERSECURITY IS A CONTINUOUS 6-STEP PROCESS OF PREPARING, DETECTING, ANALYSING, CONTAINING, ERADICATING, AND RECOVERING

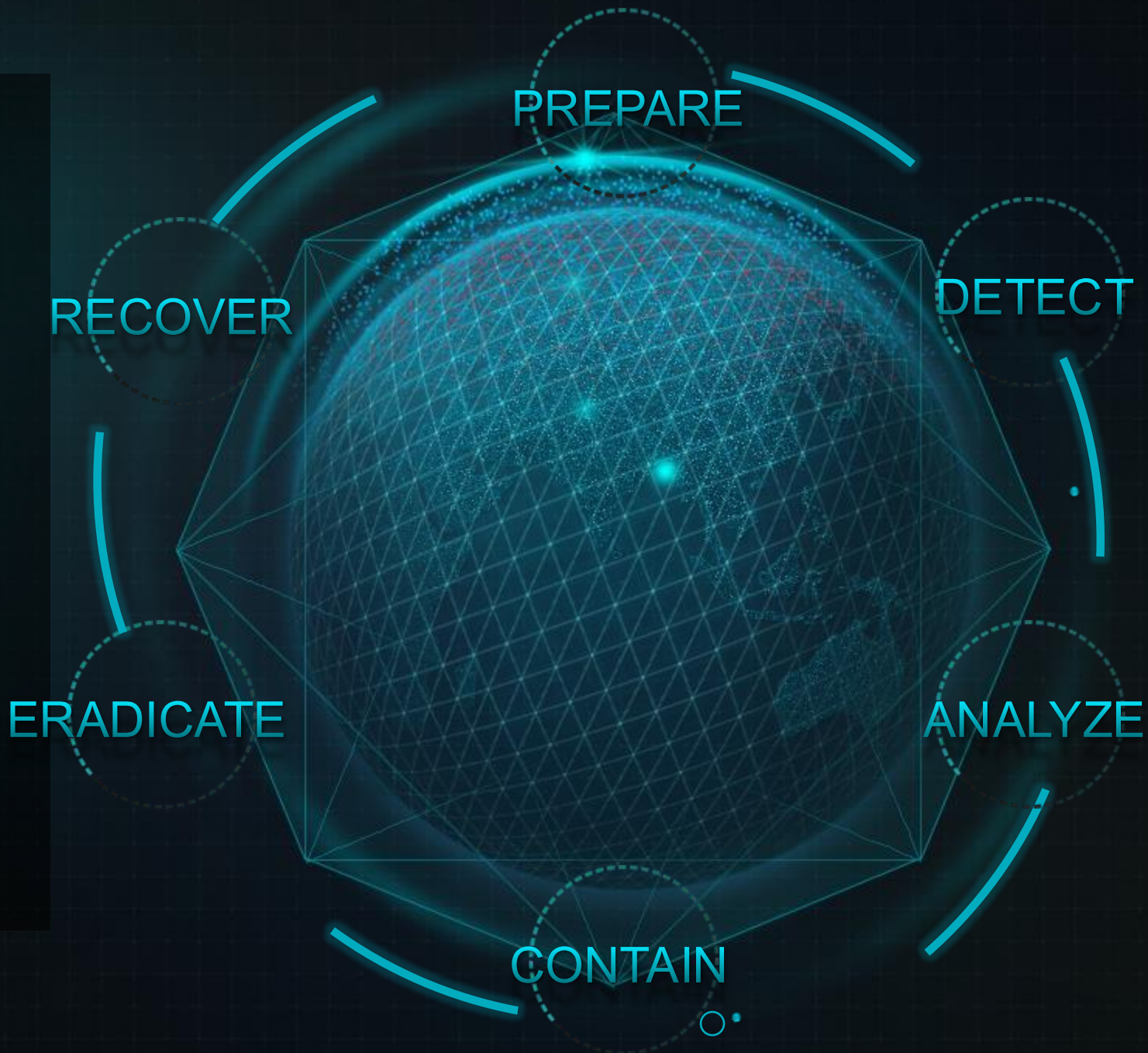


THE 6-STEP PROCESS

CONTINUOUS AND
NEVERENDING

1. PREPARE
2. DETECT
3. ANALYZE
4. CONTAIN
5. ERADICATE
6. RECOVER

AND REPEAT



2

The CIA Triad

2

The CIA Triad

C - CONFIDENTIALITY

Keep data **private** - Only authorized people should have access to them

I - INTEGRITY

Keep data **accurate** - Information stays unchanged and is not tampered, unless done so by an authorized source

A - AVAILABILITY

Keep data **available** - Systems and data are accessible when needed, without disruption

2

The CIA Triad expansion

C - CONFIDENTIALITY

I - INTEGRITY

A - AVAILABILITY

As cybersecurity has evolved in the years, so has our understanding of what needs to be protected, so in the CIA triad the following were added:

A - AUTHENTICATION

Are you *really* who you say you are?

A - AUTHORIZATION

And if you are who you say you are, are you authorized to access those data?

3

Types of Attack

3

Types of Attack

SO, WHY IS CIAAA IMPORTANT?

- Defines clearly what needs to be protected
- Offers a structured way of assessing, designing, and placing security controls.
- Enables effective risk assessment.
- Each C-I-A-A-A element helps evaluate threats and prioritize mitigations.
- Security controls like firewalls, encryption, MFA, RBAC, ACLs, backups are designed to protect one or more C-I-A-A-A elements.
- Helps guide policy creation, compliance standards and technical implementation.
- Helps understand multi-dimensional impacts

CIAAA IS NOT JUST A CHECKLIST. IT'S THE FOUNDATION OF SECURITY THINKING

ATTACK TYPE	IMPACT				
	C	I	A	A	A
Phishing	●			●	
Man-in-the-Middle (MitM)	●			●	
SQL Injection	●	●			
Ransomware		●	●		
Denial-of-Service (DoS)			●		
Brute Force				●	
Privilege Escalation				●	●
Insider threat		●			●
Cross-Site Scripting (XSS)	●	●			
Replay Attacks				●	
Session Hijacking	●			●	●
Data Exfiltration	●				
Malware/Trojans	●	●	●	●	●
Misconfiguration Exploits			●		●
Zero-Day Exploits	●	●	●	●	●

4

Types of Defense

4

Types of Defense

Because attackers don't target just one thing, CIAAA also helps in:

- Understanding multidimensional impacts
- Create layered defenses
- Continuously refine and create new defenses based on new vulnerabilities or adversary techniques (MITRE ATT&CK aligned)

MITRE ATT&CK - ADVERSARIAL TACTICS, TECHNIQUES AND COMMON KNOWLEDGE

Is a globally accessible knowledge base of how real-world attackers behave. Mapped in a structural way, it stands for a playbook of adversary behaviours, categorized by:

- **what** they are trying to achieve (tactics), and
- **how** they do it (techniques and sub-techniques)

4

Types of Defense

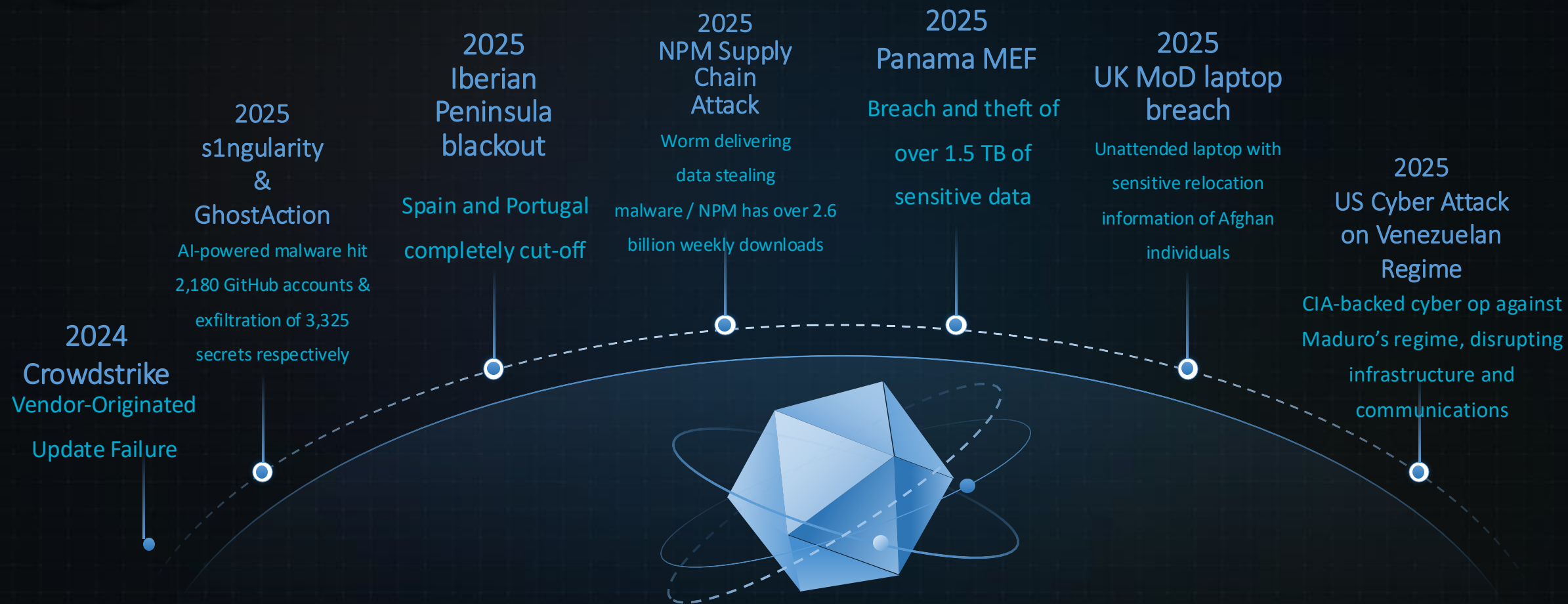
Attack type	Defenses
Phishing	MFA, User Awareness
Man-in-the-Middle	TLS everywhere (HTTPS, VPN), Certificate Pinning, Secure DNS
SQL Injection	Parameterized queries, Input Validation, Web Application Firewall (WAF)
Ransomware	Regular offline backups, Endpoint Protection, Endpoing Detection and Recovery (EDR)
Denial-of-Service (DoS)	Rate limiting, Traffic Shaping, Cloud DDoS Mitigation
Brute Force	Account Lockout Policies, CAPTCHA, MFA
Privilege Escalation	Least Privilege Access (RBAC), Patching known exploits quickly
Insider threat	User Behaviour Analytics, Separation of Duties, Access Reviews
Cross-Site Scripting (XSS)	I/O Encoding (HTML escaping), Content Security Policy
Replay Attacks	Timestamps in Tokens, Short-Lived Session Tokens
Session Hijacking	Secure Cookies (i.e. HttpOnly, SameSite etc), TLS, Session Expiry
Data Exfiltration	Data Loss Prevention (DLP), Outbound Traffic Monitoring, Security Information and Event Management Alerts (SIEM)
Malware/Trojans	EDR with Heuristic Detection Algorithms, Application Whitelisting, Antivirus
Misconfiguration Exploits	Baseline hardening, Automated Config Audits, Cloud Security Posture Management (CSPM) Tools
Zero-Day Exploits	Behaviour-Based Detection, EDR, Threat Intelligence, Patch Fast Once Known

5

Real world examples

5

Real world examples



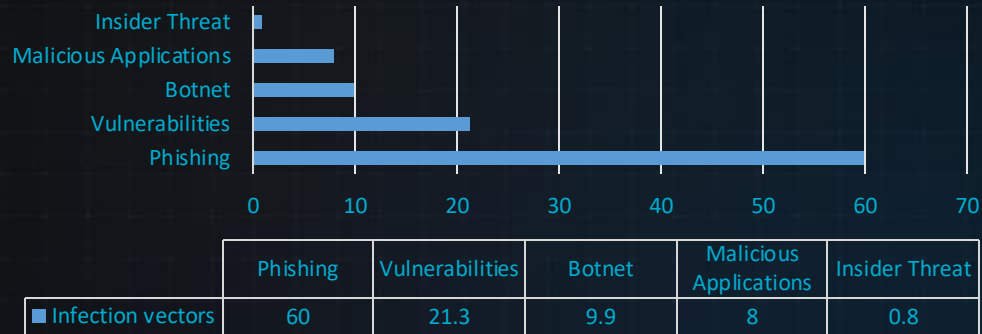


The Landscape of 2025

6

The Landscape of 2025

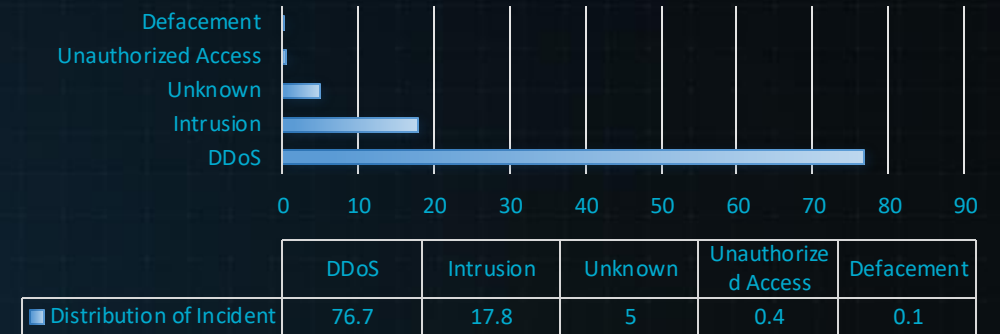
Infection vectors



Axis Title

■ Infection vectors

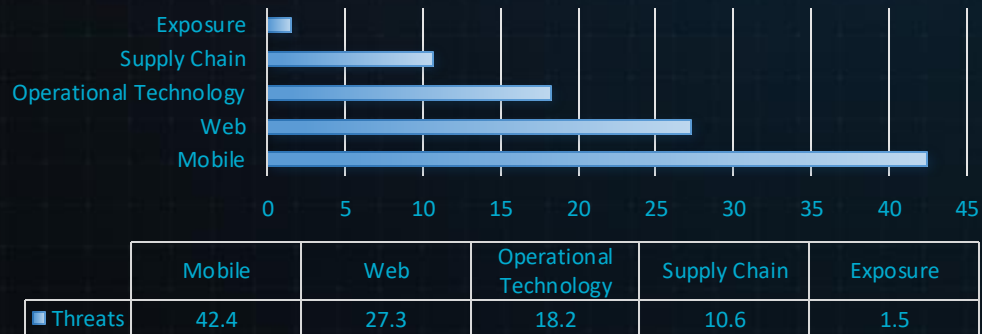
Distribution of Incident



Axis Title

■ Distribution of Incident

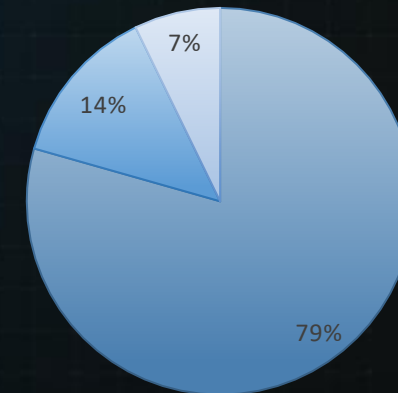
Threats



Axis Title

■ Threats

Objectives



■ Ideology ■ Financial ■ Espionage

6

The Landscape of 2025

KEY TAKEAWAYS

Phishing remains a primary initial intrusion vector

- ClickFix-style
- Phishing-as-a-Service
- QR phishing - quishing

Dependencies and third-party service providers get increasingly targeted

Exploitations of the supply chain

Continuous targeting of mobile devices (esp. Android) and exploitation of outdated devices

Spyware for surveillance purposes increasingly documented



What Can You Do?

7

Prevention is the best defense!

PREPARE - DETECT - ANALYZE

- Use **STRONG & LONG** passwords (at least 26 characters)
- **MFA** wherever possible
- **CAUTIOUS** with links and attachments!
- **NEVER TRUST** emails asking for your personal credentials or information!
- **UPDATE** devices and applications
- **BACKUP** important files
- **ONLY INSTALL TRUSTED** software
- **REPORT** anything suspicious

7

If you've been compromised?

ACT FAST! - CONTAIN / ERADICATE / RECOVER

- DISCONNECT your device from the network
- DO **NOT** SHUT DOWN THE MACHINE!
- REPORT the incident
- CHANGE PASSWORDS
- SCAN system for malware
- RESTORE from a clean backup
- WATCH for follow-up fraud

THANK YOU

MSOUVAL@IIT.DEMOKRITOS.GR