Cyber Threats

Prepared by: PalCyberSec Team

TABLE OF CONTENTS

Cybercrime

🌐 Criminal activities conducted via **digital devices/networks**, leveraging technology for malicious intent.

Common Types of cybercrime

- Phishing Attacks
- Malware
- Social Engineering
- Insider Threats
- Ransomware
- Identity Theft
- DDoS Attacks

Understanding Hackers: Evolution & Perception

Original Definition (Neutral)

🧠 **Skilled IT Practitioners**

Experts who solve problems or achieve goals using **non-standard**, creative methods.

Modern Perception (Negative)

⚠️ **Exploit-Driven Actors**

Term now commonly refers to individuals who:

- Leverage **bugs, vulnerabilities, or exploits** to breach systems.
- Access unauthorized data.

Types of Hackers

Black Hat
🕶️ *Malicious actors exploiting systems for profit/destruction (e.g., ransomware).*

Blue Hat
💢 *Revenge-driven; target organizations/individuals for retaliation.*

Script Kiddies
🎮 *Amateurs using pre-made tools for minor disruption*

Gray Hat
🌓 *Unethical but not malicious; hack to expose flaws without permission.*

Malicious Insider
🔒 *Employees/partners* leaking data or sabotaging systems.

Hacktivists
✊ *Activists hacking for social/political causes (e.g., Anonymous).*

State-Sponsored
🏛️ *Government-backed; cyber espionage/warfare (e.g., APT attacks).*

State Sponsored Hackers

Government-Backed Cyber Advantages

🏛️ **Funding**
Unlimited budgets for tools, talent, & infrastructure.

🌐 **Scope**
Target energy, defense, elections — critical sectors.

🕵️ **Stealth**
Operate undetected for years (e.g., SolarWinds).

The Major Players

Here is a breakdown of the five-largest state-sponsored groups that are currently active.

1. APT1 (China)
🐉 *Sectors*: Defense, Tech • *Operation Aurora* (Google)

2. APT28 (Russia)
🐻 *Focus*: Elections • *DNC Hack*

3. Lazarus (NK)
💀 *Targets*: Banks • *WannaCry*

4. Equation (U.S.)
🔫 *Cyberweapon*: Stuxnet

5. APT33 (Iran)
🌻 *Sectors*: Energy • *Shamoon*

Intelligence Agencies

🕵️ Government entities that **collect**, **analyze**, and **act** on intelligence to:

- Protect national security.
- Inform military strategy.
- Guide foreign policy.
- Support law enforcement.

NSO Group

CIA

NSA

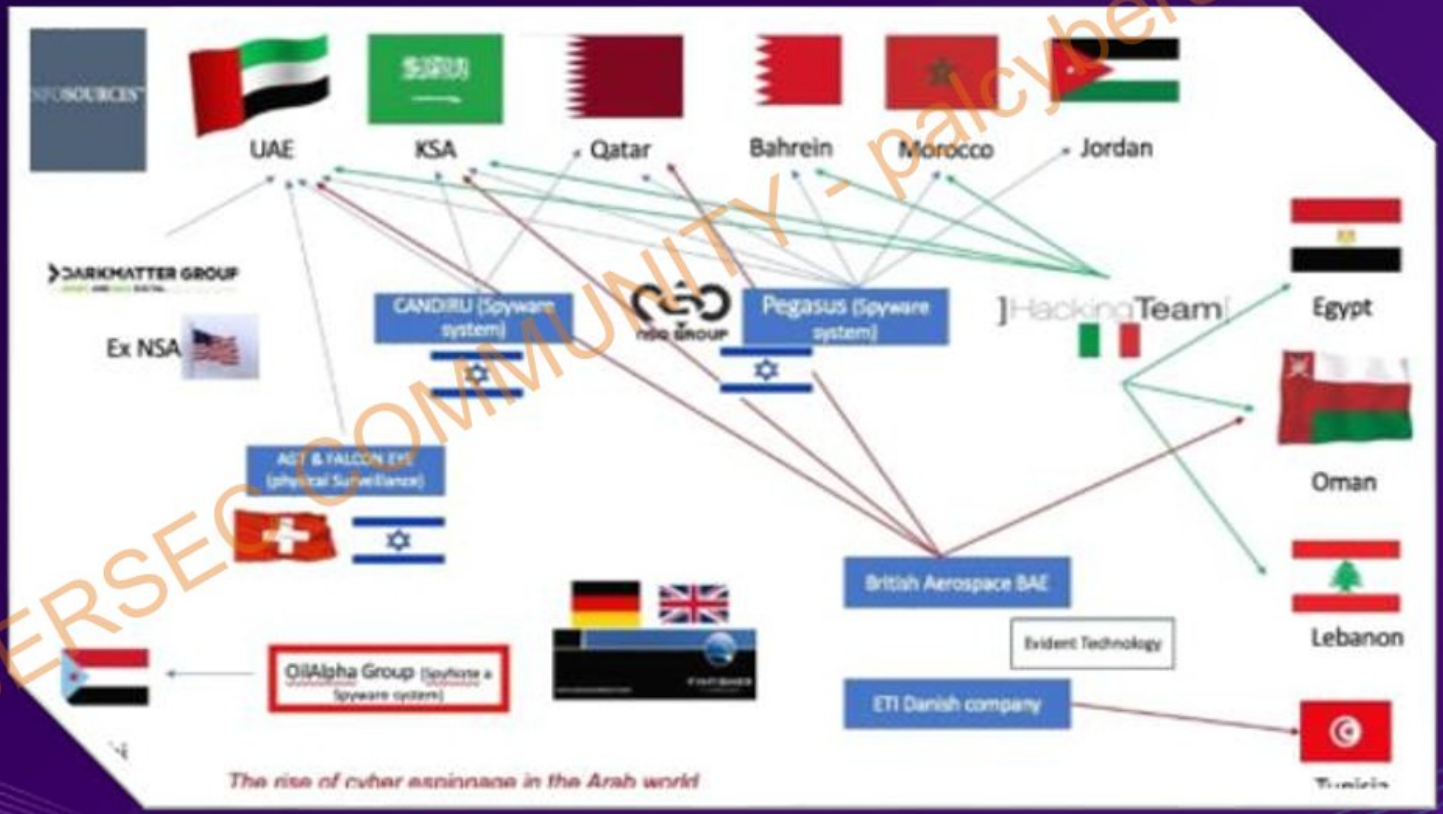
8200 Unit

Cyberwarfare

⚔️ Strategic cyber-attacks by *nation-states* or groups to disrupt critical systems, infrastructure, or cause physical harm.

Reasons and Motivations for Cyberwarfare

Military, Hacktivism, Income generation, Nonprofit research



Forms of Cyberwarfare

1. Financial Infrastructure Attacks

2. Public Infrastructure Attacks

3. Safety Infrastructure Attacks

4. Military/Defense Attacks

Forms of Cyberwarfare

1986

THE CUCKOO'S EGG
First major cyber espionage case: German hacker infiltrated U.S. military systems.

1998

MOONLIGHT MAZE
State-sponsored Russian hacker targeted [illegible] NASA, [illegible] universities for classified data.

2010

STUXNET
-U.S./Israel-created malware sabotaged Iran's nuclear centrifuges, causing physical damage.

2017

NOTPETYA
Russian ransomware masquerading as ransomware disrupted global businesses (e.g., Maersk, Merck).

2020

SOLARWINDS HACK
-Russian APT group breached U.S. agencies (e.g., Treasury, DoD) via a compromised software update.

Deep Fake

🎭 Hyper-realistic fake content generated via AI/ML algorithms, combining images, videos, and audio to mimic real people.

What Are Deepfakes Used For?

How To Spot Deepfakes

Visual & Behavioral Red Flags

- 👁️ **Facial & Eye Anomalies**
- 🧍 **Body & Appearance Clues**
- 🖥️ **Technical Glitches**

THANKS