

TABLE OF CONTENTS

Cybercrime

3 State Sponsored Hackers

5 Cyberwarfare

Hackers

Intelligence Agencies

<u>04</u>

Deep Fake

Cybercrime

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



Common Types of cybercrime

Phishing Attacks

Malware

Social Engineering

Ransomware

Identity Theft

DDoS Attacks

Insider Threats

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).

Script Kiddies

Amateurs using pre-made tools for minor disruption

Malicious Insider

Employees/partners leaking data or sabotaging systems.



Blue Hat

Revenge-driven; target organizations/individuals for retaliation.

Gray Hat

🕩 Unethical but not malicious; hack to expose flaws without permission.

Red Hat Hacker

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

m 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



NSA



8200 **Unit**





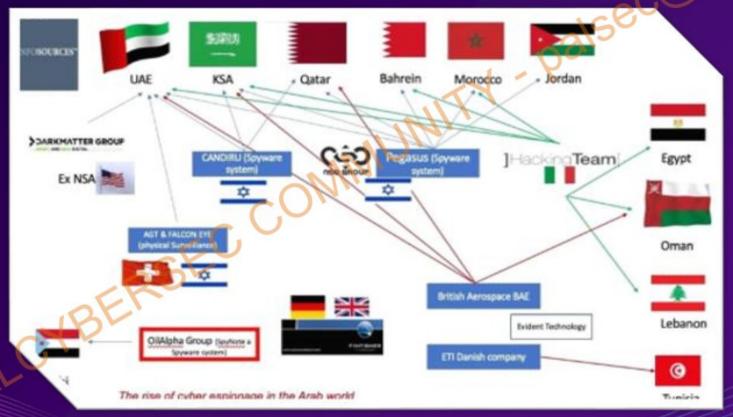
Cyberwarfare

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

THE CUCKOO'S EGG

First major cyber espionage case: German hacker Infiltrated U.S. military systems.

1986



1998



MOONLIGHT MAZE

State-sponsored Russian hackers targeted Pentago v NASA, and university for classify d. V. Fu

STUXNE

-U.S./Israel-create.t malware so is tay .d Irc it's nucleur entriunes, causing the sical damage.

2010



2017



NOTPETY

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

OLARWINDS HACK

-Russian APT group preached U.S. agencies e.g., Treasury, DoD) via a compromised software update

2020





Deep Fake

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







How To Spot Deepfakes

Visual & Behavioral Red Flags

- Facial & Eye Anomalies
- Body & Appearance Clues
- Technical Glitches



