Cyber Warfare

62.2k views

App Security | Attack Tools | Essentials | Threats

What Is Cyber Warfare?

Cyber warfare is usually defined as a cyber attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.

There is, however, a debate among cyber security experts as to what kind of activity constitutes cyber warfare. The US Department of Defense (DoD) recognizes the threat to national security posed by the malicious use of the Internet but doesn't provide a clearer definition of cyber warfare. Some consider cyber warfare to be a cyber attack that can result in death.

Cyber warfare typically involves a nation-state perpetrating cyber attacks on another, but in some cases, the attacks are carried out by terrorist organizations or non-state actors seeking to further the goal of a hostile nation. There are several examples of alleged cyber warfare in recent history, but there is no universal, formal, definition for how a cyber attack may constitute an act of war.

7 Types of Cyber Warfare Attacks

Here are some of the main types of cyber warfare attacks.

7 Types of Cyberwarfare Attacks
Espionage
Sabotage
Denial-of-service (DoS) Attacks
Electrical Power Grid
Propaganda Attacks
Economic Disruption
Surprise Attacks

Espionage

Refers to monitoring other countries to steal secrets. In cyber warfare, this can involve using botnets or spear phishing attacks to compromise sensitive computer systems before exfiltrating sensitive information.

Sabotage

Government organizations must determine sensitive information and the risks if it is compromised. Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

Denial-of-service (DoS) Attacks

DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests. This type of attack can be used to disrupt critical operations and systems and block access to sensitive websites by civilians, military and security personnel, or research bodies.

Electrical Power Grid

Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

Propaganda Attacks

Attempts to control the minds and thoughts of people living in or fighting for a target country. Propaganda can be used to expose embarrassing truths, spread lies to make people lose trust in their country, or side with their enemies.

Economic Disruption

Most modern economic systems operate using computers. Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

Surprise Attacks

These are the cyber equivalent of attacks like Pearl Harbor and 9/11. The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses. This can be done to prepare the ground for a physical attack in the context of hybrid warfare.

Examples of Cyber Warfare Operations

Here are several well-publicized examples of cyber warfare in recent times.

Stuxnet Virus

Stuxnet was a worm that attacked the Iranian nuclear program. It is among the most sophisticated cyber attacks in history. The malware spread via infected Universal Serial Bus devices and targeted data acquisition and supervisory control systems. According to most reports, the attack seriously damaged Iran's ability to manufacture nuclear weapons.

Sony Pictures Hack

An attack on Sony Pictures followed the release of the film "The Interview", which presented a negative portrayal of Kim Jong Un. The attack is attributed to North Korean government hackers. The FBI found similarities to previous malware attacks by North Koreans, including code, encryption algorithms, and data deletion mechanisms.

Bronze Soldier

In 2007, Estonia relocated a statue associated with the Soviet Union, the Bronze Soldier, from the center of its capital Tallinn to a military cemetery near the city. Estonia suffered a number of significant cyber attacks in the following months. Estonian government websites, media outlets, and banks were overloaded with traffic in massive denial of service (DoS) attacks and consequently were taken offline.

Fancy Bear

CrowdStrike claims that the Russian organized cybercrime group Fancy Bear targeted Ukrainian rocket forces and artillery between 2014 and 2016. The malware was spread via an infected Android application used by the D-30 Howitzer artillery unit to manage targeting data.

Ukrainian officers made wide use of the app, which contained the X-Agent spyware. This is considered to be a highly successful attack, resulting in the destruction of over 80% of Ukraine's D-30 Howitzers.

Enemies of Qatar

Elliott Broidy, an American Republican fundraiser, sued the government of Qatar in 2018, accusing it of stealing and leaking his emails in an attempt to discredit him. The Qataris allegedly saw him as an obstacle to improving their standing in Washington.

According to the lawsuit, the brother of the Qatari Emir was alleged to have orchestrated a cyber warfare campaign, along with others in Qatari leadership. 1,200 people were targeted by the same attackers, with many of these being known "enemies of Qatar", including senior officials from Egypt, Saudi Arabia, the United Arab Emirates, and Bahrain.

How to Combat Cyber Warfare

The legal status of this new field is still unclear as there is no international law governing the use of cyber weapons. However, this does not mean that cyber warfare is not addressed by the law.

The Cooperative Cyber Defense Center of Excellence (CCDCoE) has published the Tallinn Manual, a textbook that addresses rare but serious cyber threats. This manual explains when cyber attacks violate international law and how countries may respond to such violations.

Conducting Risk Assessments with Cyber Wargames

The best way to assess a nation's readiness for cyber warfare is to conduct a real-life exercise or simulation, also known as a cyber wargame.

A wargame can test how governments and private organizations respond to a cyber warfare scenario, expose gaps in defenses, and improve cooperation between entities. Most importantly, a wargame can help defenders learn how to act quickly to protect critical infrastructure and save lives.

Cyber wargames can help cities, states, or countries improve readiness for cyber warfare by:

- **Testing different situations** – such as detecting attacks in early stages, or mitigating risks after critical infrastructure has already been compromised.
- **Testing unusual scenarios** – attacks are never conducted "by the book". By establishing a red team that acts as the attackers and tries to find creative ways to breach a target system, the defenders can learn how to mitigate real threats.
- **Division of labor and cooperation mechanisms** – cyber warfare requires many individuals from different organizations and government units to collaborate. A cyber wargame can bring together those people, who may not know each other, and help them decide how to work together in the event of a crisis.
- **Improving policies** – governments may establish cyber warfare policies, but need to test them in practice. A cyber wargame can test the effectiveness of policies and provide an opportunity for improving them.

The Importance of Layered Defense

Under the pressure of cyber warfare, governments of many countries have issued operational national security policies to protect their information infrastructure. These policies typically use a layered defense approach, which includes:

- Securing the cyber ecosystem
- Raising awareness for cybersecurity
- Promoting open standards for combating cyber threats
- Implementing a national cybersecurity assurance framework
- Working with private organizations to improve their cybersecurity capabilities

Securing the Private Sector

A strategic factor in cyberwarfare is the resilience of local businesses to cyber attacks. Businesses need to tighten their security measures to reduce the benefits of an attack on a nation-state. The following is a set of measures to ensure corporate cybersecurity, which can promote national security:

- Create obstacles to breaching the network
- Use web application firewalls (WAF) to quickly detect, investigate, and block malicious traffic
- Quickly respond to a breach and restore business operations
- Facilitate cooperation between the public and private sectors
- Use local hackers as a resource to help protect against foreign cyber threats

Imperva Cyber Warfare Protection

Imperva can help organizations protect themselves against cyberwarfare by implementing a comprehensive cybersecurity solution, including both application and data security.

Imperva Application Security

Imperva provides comprehensive protection for applications, APIs, and microservices:

Web Application Firewall – Prevent attacks with world-class analysis of web traffic to your applications.

Runtime Application Self-Protection (RASP) – Real-time attack detection and prevention from your application runtime environment goes wherever your applications go. Stop external attacks and injections and reduce your vulnerability backlog.

API Security – Automated API protection ensures your API endpoints are protected as they are published, shielding your applications from exploitation.

Advanced Bot Protection – Prevent business logic attacks from all access points – websites, mobile apps and APIs. Gain seamless visibility and control over bot traffic to stop online fraud through account takeover or competitive price scraping.

DDoS Protection – Block attack traffic at the edge to ensure business continuity with guaranteed uptime and no performance impact. Secure your on premises or cloud-based assets – whether you're hosted in AWS, Microsoft Azure, or Google Public Cloud.

Attack Analytics – Ensures complete visibility with machine learning and domain expertise across the application security stack to reveal patterns in the noise and detect application attacks, enabling you to isolate and prevent attack campaigns.

Client-Side Protection – Gain visibility and control over third-party JavaScript code to reduce the risk of supply chain fraud, prevent data breaches, and client-side attacks.

Imperva Data Security

Imperva protects all cloud-based data stores to ensure compliance and preserve the agility and cost benefits you get from your cloud investments

Cloud Data Security – Simplify securing your cloud databases to catch up and keep up with DevOps. Imperva's solution enables cloud-managed services users to rapidly gain visibility and control of cloud data.

Database Security – Imperva delivers analytics, protection, and response across your data assets, on-premise and in the cloud – giving you the risk visibility to prevent data breaches and avoid compliance incidents. Integrate with any database to gain instant visibility, implement universal policies, and speed time to value.

Data Risk Analysis – Automate the detection of non-compliant, risky, or malicious data access behavior across all of your databases enterprise-wide to accelerate remediation.

Latest Blogs

Application Security

Preventing Bot Attacks and Online Fraud on APIs

Application Security

What We Learned from the 2023 Imperva Bad Bot Report

Application Security

Imperva Continues to Innovate With New Features for Online Fraud Prevention

Applica

Imperv
API Se
Enhan

Erez Hasson
May 17, 2023 6 min read

Erez Hasson
May 10, 2023 3 min read

Erez Hasson
May 1, 2023 5 min read

Latest Articles

App Security

OSI Model

909k Views

App Security

Phishing attacks

621.5k Views

App Security

Penetration Testing

569.9k Views

App Security

Social Engineering

526k Views

App Security

SQL (Structured query language) Injection

404.8k Views

+1 866 926 4678

Partners

Imperva Partner Ecosystem

Channel Partners

Technology Alliances

Find a Partner

Partner Portal Login

Resources

Imperva Blog

Resource Library

Case Studies

Learning Center

About Us

Why Imperva

Who We Are

Events

Careers

Press & Awards

Contact Information

Network

Network Map

System Status

Support

Emergency DDoS Protection

Support Portal

Imperva Community

Documentation Portal

API Integration