Internet Threats Update

By Jesse Black, Yellow Crayon LLC, June 18, 2025

Cyber Warfare

Definition

Cyberwarfare

Cyberwarfare is the use of cyber attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems.[1] Some intended outcomes could be espionage, sabotage, propaganda, manipulation or economic warfare.

From Wikipedia, the free encyclopedia

"**Cyber warfare** is a rapidly evolving field that involves the use of digital technologies to disrupt, degrade, or destroy an adversary's critical infrastructure, economy, or national security. AI-powered cyber threats are particularly concerning, as they can create deepfakes, polymorphic malware, and personalized phishing emails, making traditional attacks faster, stealthier, and more convincing."

– LiveMint.com via Leo/Llama

"Cyber warfare actors are a diverse group, but some of the most notable ones include nation-state actors, organized crime groups, and hacktivist collectives. Nation-state actors, such as Equation Group and Fancy Bear have been linked to sophisticated cyberespionage operations and have been accused of conducting attacks on critical infrastructure, governments, and private companies.

Organized crime groups, such as the North Korean IT worker scam, have been known to target individuals and organizations with phishing and other types of cyber attacks.

Hacktivist collectives, such as Cyber Av3ngers have been linked to cyber attacks on critical infrastructure and have been accused of conducting operations on behalf of nation-state actors.

These groups often use advanced tactics and techniques, including AI-powered attacks, to conduct their operations."

- Sources (via Leo AI): thehackernews.com, mediabrief.com, csoonline.com, www.itminister.co.uk, www.wbur.org, quointelligence.eu, medium.com, justsecurity.org

Terminology:

Key Characteristics of **Hybrid Warfare**: (Source: Google AI Overview)

- Blurring of Lines: **Hybrid warfare** blurs the distinction between wartime and peacetime, and between conventional and unconventional means. It often operates in the "grey zone," below the threshold of open armed conflict.
- Diverse Tactics: It incorporates a wide array of methods including disinformation, cyber attacks, economic pressure, irregular armed groups, espionage, sabotage, political interference, and use of regular forces.
- Exploiting Vulnerabilities: Hybrid adversaries exploit vulnerabilities in the target state's economic, political, and social fabric.
- Ambiguity and Deniability: A key aspect is the use of ambiguity and deniability to make attribution difficult.
- Goal of Destabilization: Rather than outright military victory, the aim is often to destabilize and undermine the targeted society and its institutions.

In the news:

Significant Cyber Incidents

Compiled by Center for Strategic & International Studies

"This timeline records significant cyber incidents since 2006, focusing on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars."

See https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (listed in reverse chronological order)

Stuxnet and the Future of Cyber War

By James P. Farwell and Rafal Rohozinski, *retrieved from Duke University Libraries by Google Search*
Emphasis added

The discovery in June 2010 that a **cyber worm** dubbed '**Stuxnet**' had struck the Iranian nuclear facility at Natanz suggested that, for cyber war, the future is now. Stuxnet has apparently infected over 60,000 computers, more than half of them in Iran; other countries affected include India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany. The virus continues to spread and infect computer systems via the Internet, although its power to do damage is now limited by the availability of effective antidotes, and a built-in expiration date of 24 June 2012.

German expert Ralph Lagner describes Stuxnet as a military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program'. Symantec Security Response Supervisor Liam O Murchu, whose company reverse-engineered the worm and issued a detailed report on its operation, declared: 'We've definitely never seen anything like this before'. Computer World calls it 'one of the most sophisticated and unusual pieces of software ever created'.

Also https://www.tandfonline.com/doi/full/10.1080/00396338.2011.555586
Retrieve original from https://doi.org/10.1080/00396338.2011.555586

Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience

Center for Strategic & International Studies

From the Executive Summary:

“The Russia-Ukraine war has emerged as a watershed moment in modern military history, fundamentally reshaping our understanding of contemporary warfare. … The conflict serves as both warning and blueprint—demonstrating how technological innovation, organizational adaptability, and strategic resilience have become the defining characteristics of military effectiveness in the twenty-first century.”

Cyber weapons in the Israel-Iran conflict may hit the US

“With Tehran’s military weakened, digital retaliation likely, experts tell *The Reg*

Jessica Lyons The Register Fri 13 Jun 2025 // 22:07 UTC

“The current Israel–Iran military conflict is taking place in the era of hybrid war, where cyberattacks amplify and assist missiles and troops, and is being waged between two countries with very capable destructive cyber weapons.

Iran is widely expected to retaliate against Israel's missile strikes with cyber operations — and these could extend to American targets, according to cyber warfare experts and threat analysts.

"I would expect there to be a cyber component of both the Israeli and Iranian activities," former White House advisor Michael Daniel told The Register.

Daniel, who now leads the threat-intel sharing nonprofit Cyber Threat Alliance, said both countries "have the capability to conduct a range of activities, from fully reversible DDoS [distributed denial-of-service] attacks, which could disrupt online services temporarily, to destructive wiper attacks. At the very least, I am sure both sides are using cyber capabilities to conduct espionage and reconnaissance."

… ”

Cyber Warfare needn’t be high-tech:

Internet cable cutting incidents

"Incidents of internet cable cutting, particularly those involving undersea cables, have been occurring with increased frequency, raising concerns about potential sabotage and the vulnerability of global internet infrastructure. While many cable faults are caused by accidents like ship anchors or fishing gear, some incidents are now under investigation for potential sabotage."

Source: Google AI Overview

Key Points:

Undersea cables are crucial for global internet connectivity:
They carry vast amounts of data traffic, including internet, voice, and financial transactions.

Accidents are common:
Ship anchors and fishing activity are the leading causes of unintentional cable damage.

Sabotage is a growing concern:
Some recent incidents, particularly in the Baltic Sea and around Taiwan, are being investigated for potential sabotage.

Suspects include Russia and China:
European officials suspect Russian involvement in the Baltic Sea incidents, while Taiwan has detained a Chinese vessel in connection with a cable cut.

Vulnerability is a major issue:
The global network of undersea cables is extensive, making it difficult to protect every section.

Specific Incidents:

Baltic Sea:
In late 2024, two undersea cables connecting Finland and Germany and Lithuania and Sweden were cut within hours of each other. European officials suspect sabotage, potentially by Russia.

Taiwan:
In early 2025, a Chinese-crewed ship was detained after an undersea cable connecting Taiwan to its Matsu Islands was severed.

"Taiwanese government says this may have been an example of Chinese "**gray-zone interference**," irregular military and nonmilitary tactics that aim to wear down an opponent without engaging in an actual shooting war."
Source: NBC News

Red Sea:
Damage to cables in the Red Sea disrupted telecoms networks, and while Houthi rebels denied responsibility, it highlighted the vulnerability of the region's infrastructure.

Implications:

Disruptions to internet and communication services:
Cable cuts can cause significant disruptions to internet access, voice calls, and other communication services.

Economic impact:
Damage to undersea cables can have significant economic consequences due to the reliance on these cables for financial transactions and other business activities.

Geopolitical tensions:
Suspected sabotage of undersea cables can exacerbate geopolitical tensions and raise concerns about cybersecurity and national security.

Ongoing Investigations:

European officials are investigating the Baltic Sea incidents:
They are working to determine the extent of the damage and the perpetrators behind the cuts.

Taiwan is investigating the incident involving the Chinese vessel:
They are seeking to determine whether the damage was deliberate or accidental.

International cooperation:
Efforts are underway to improve international cooperation in monitoring and protecting undersea cables.

Truly massive collection of leaked passwords

Search for “billions of passwords leaked”

ZDNET.com: 16 billion passwords leaked across Apple, Google, more: What to know and how to protect yourself

Tom's Guide: 16 billion password data breach hits Apple, Google, Facebook and more — LIVE updates and how to stay safe

CyberNews.com: 16 billion passwords exposed in record-breaking data breach, opening access to Facebook, Google, Apple, and any other service imaginable

Difficult-to-spot phishing and trojan scams

Fake Google scam: Urgent message from `sites.google.com` instead of `support.google.com` or `accounts.google.com`

Fake Zoom:

"Once the potential victim has joined the call, they are prompted to share their screen to present their work. At this point, ELUSIVE COMET will use Zoom to request control over the potential victim's computer. If the potential victim is not paying close attention, they may accidentally grant remote access, which allows ELUSIVE COMET to install their malware to the victim's device. This malware may either be an infostealer which immediately exfiltrates relevant secrets, or a RAT which allows for exfiltration at a later time."

Link to view this article: 2025-06-24 Internet Threats Update