DEFINITION



Katie Terrell Hanna

## What is cyberterrorism?

Cyberterrorism is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population. Attackers often do this by damaging or disrupting critical infrastructure.

Various security organizations view cyberterrorism and the parties involved differently. The U.S. Federal Bureau of Investigation (FBI) defines cyberterrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs and data, which results in violence against noncombatant targets by subnational groups or clandestine agents."

The FBI views a cyberterrorist attack as different from a common virus or denial of service (DoS) attack. According to the FBI, a cyberterrorist attack is a type of cybercrime explicitly designed to cause physical harm. However, there is no consensus among governments and the information security community on what qualifies as an act of cyberterrorism.

Other organizations and experts have said that less harmful attacks can be considered acts of cyberterrorism. When attacks are intended to be disruptive or to further the attackers' political agenda, they can qualify as cyberterrorism, according to these other groups. In some cases, the differentiation between cyberterrorism attacks and ordinary cybercrime lies in the intention: The primary motivation for cyberterrorism attacks is to disrupt or harm the victims, even if the attacks do not result in physical harm or cause extreme financial harm.

In other cases, the differentiation is tied to the outcome of a cyber attack. Many cybersecurity experts believe an incident should be considered cyberterrorism if it results in physical harm or loss of life. This can be either direct or indirect harm through damage to or disruption of critical infrastructure.

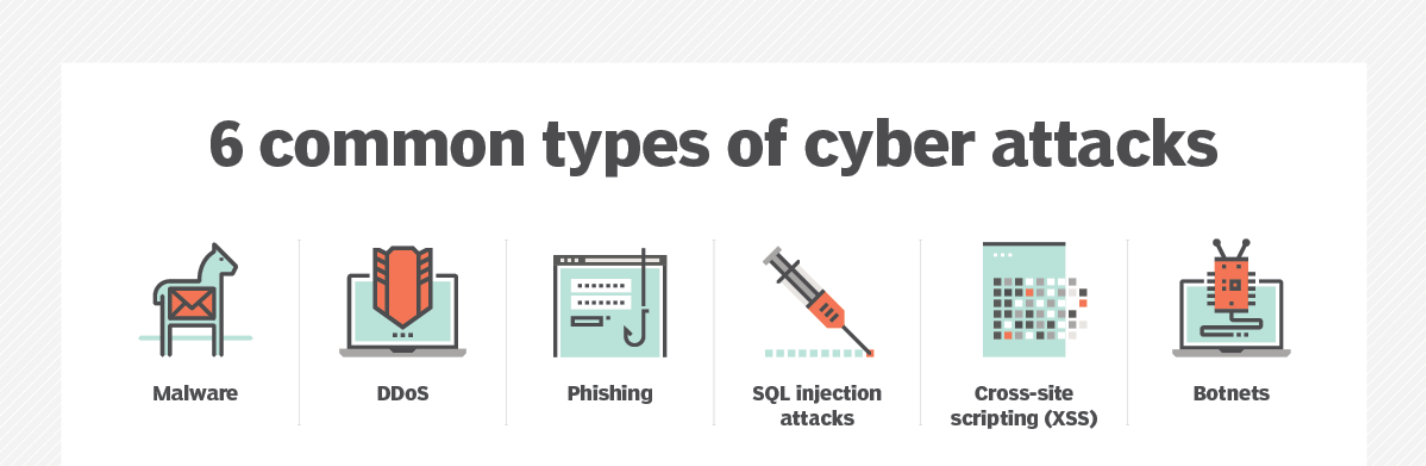
Physical harm is not always considered a prerequisite for classifying a cyber attack as a terrorist event. The North Atlantic Treaty Organization, known as NATO, has defined cyberterrorism as a cyber attack that uses or exploits computer or communication networks to cause "sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."

According to the U.S. Commission on Critical Infrastructure Protection, possible cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers and water systems.

## Methods used for cyberterrorism

The intention of cyberterrorist groups is to cause mass chaos, disrupt critical infrastructure, support political activism or hacktivism, or inflict physical damage and even loss of life. Cyberterrorism actors use various methods. These include the following types of attacks:

- Advanced persistent threat (APT) attacks use sophisticated and concentrated penetration methods to gain network access. Once inside the network, the attackers stay undetected for a period of time with the intention of stealing data. Organizations with high-value information, such as national defense, manufacturing and the financial industry, are typical targets for APT attacks.
- Computer viruses, worms and malware target IT control systems. They are used to attack utilities, transportation systems, power grids, critical infrastructure and military systems.
- DoS attacks attempt to prevent legitimate users from accessing targeted computer systems, devices or other computer network These attackers often go after critical infrastructure and governments.
- Hacking, or gaining unauthorized access, seeks to steal critical data from institutions, governments and businesses.
- Ransomware, a type of malware, holds data or information systems hostage until the victim pays the ransom. Some ransomware attacks also exfiltrate data.
- Phishing attacks attempt to collect information through a target's email, using that information to access systems or steal the victim's identity.




Cyberterrorists employ a variety of attack methods, including the six most common pictured here.

## What are examples of cyberterrorism?

Cyberterrorist acts are carried out using computer servers, other devices and networks visible on the public internet. Secured government networks and other restricted networks are often targets.

Examples of cyberterrorism include the following:

- **Disruption of major websites.** The intent here is to create public inconvenience or stop traffic to websites containing content the hackers disagree with.
- **Unauthorized access.** Attackers often aim to disable or modify communications that control military or other critical technology.
- **Disruption of critical infrastructure systems.** Threat actors try to disable or disrupt cities, cause a public health crisis, endanger public safety or cause massive panic and fatalities. For example, cyberterrorists might target a water treatment plant, cause a regional power outage or disrupt a pipeline, oil refinery or fracking operation.
- **Cyberespionage.** Governments often carry out or sponsor cyberespionage attacks. They aim to spy on rival nations and gather intelligence, such as troop locations or military strategies.

## Is cyberterrorism a real threat?

The threat of cyberterrorism is greater than ever. In 2021, the Center for Strategic and International Studies (CSIS), a bipartisan, nonprofit policy research group, identified 118 significant cyber attacks that either occurred during that time or were acknowledged to have occurred earlier. Significant attacks, as the CSIS defines them, include those that target government agencies, defense and high-tech companies, as well as economic crimes with losses over $1 million.

Here are examples of 2021 attacks that CSIS identified:

- **January.** Hackers with ties to the Chinese government deployed ransomware attacks against five major gaming companies. They demanded over $100 million in ransom.
- **February.** Hackers tried to contaminate the water supply of Oldsmar, Fla., by exploiting a remote access system to increase the amount of sodium hydroxide present.
- **March.** The Polish government said it suspected Russian hackers had taken control of Poland's National Atomic Energy Agency and Health Ministry websites for a short time. They tried to spread alarms about a radioactive threat that didn't exist.
- **May.** North Korea carried out a cyber attack against South Korea's state-run Korea Atomic Energy Research Institute by taking advantage of a virtual private network vulnerability.
- **July.** Iran used Facebook to target U.S. military personnel, posing as recruiters, journalists and nongovernmental organization personnel. The hackers sent files with malware and used phishing sites to trick victims into providing sensitive credentials.
- **September.** Hackers stole 15 terabytes of data from 8,000 organizations working with Voicenter, an Israeli company. The hackers offered the data online for $1.5 million.
- **October.** Brazilian hackers attacked a website belonging to Indonesia's State Cyber and Password Agency.
- **December.** A Russian group claimed responsibility for a ransomware attack on CS Energy, an Australian utility company.


## Defending against cyberterrorism

The key to countering cyberterrorism is to implement extensive cybersecurity measures and vigilance.

Cyberterrorism has mostly targeted government entities. However, that is changing, and businesses are becoming targets as well. As a result, businesses and other organizations must ensure that all internet of things devices are secured and inaccessible via public networks. To protect against ransomware and similar types of attacks, organizations must regularly back up systems, implement continuous monitoring techniques, and use firewalls, antivirus software and antimalware.

Companies must also develop IT security policies to protect business data. This includes limiting access to sensitive data and enforcing strict password and authentication procedures, like two-factor authentication or multifactor authentication.

The National Cyber Security Alliance is a public-private partnership to promote cybersecurity awareness. It recommends training employees on safety protocols and how to detect a cyber attack and malicious code. The Department of Homeland Security coordinates with other public sector agencies and private sector partners. It shares information on potential terrorist activity and how to protect national security, as well as counterterrorism measures.

On a global level, 66 countries, including the United States, participate in the Council of Europe's Convention on Cybercrime. It seeks to harmonize international laws, improve investigation and detection capabilities, and promote international cooperation to stop cyberwarfare.

*Want to protect your IT infrastructure and data from cyberterrorists and other attackers? Check out our guide to successful cybersecurity planning.*

This was last updated in January 2022

## Continue Reading About cyberterrorism

- The nation state threat to business
- Nation-state hacker indictments: Do they help or hinder?
- How to prevent cybersecurity attacks using this 4-part strategy
- 6 common types of cyber attacks and how to prevent them
- What is the future of cybersecurity?

## Related Terms

### antivirus software (antivirus program)

Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other ...

See complete definition

### cyberwarfare

The generally accepted definition of cyberwarfare is a series of cyber attacks against a nation-state, causing it significant ...

See complete definition

## quantum supremacy

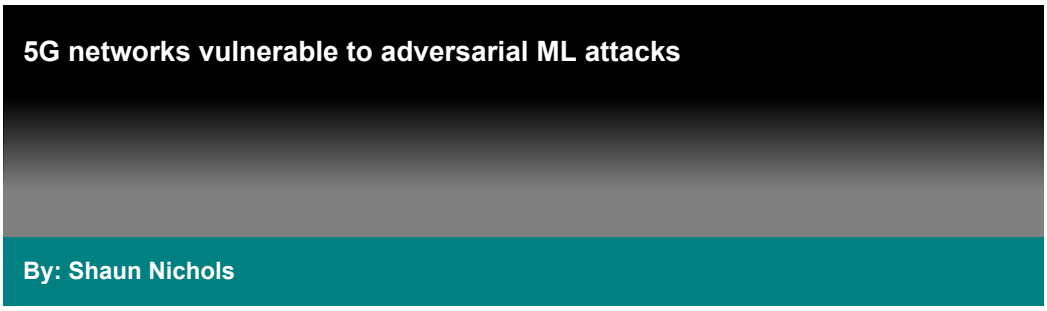
Quantum supremacy is the experimental demonstration of a quantum computer's dominance and advantage over classical computers by ... See complete definition

## Dig Deeper on Threats and vulnerabilities


By: Alexander Gillis


By: Rahul Awati


By: Alex Scroxton




By: Shaun Nichols



## Networking

### Top 9 SD-WAN benefits for businesses

Make the case for an SD-WAN implementation, and explore the benefits and main use cases for SD-WAN in enterprises, beyond ...

### White box networking use cases and how to get started

Rising cloud costs have prompted organizations to consider white box switches to lower costs and simplify network management. ...