Office of the Director of National Intelligence

Cyber Threat Intelligence Integration Center

Cyber Threats to Elections

A LEXICON

Cyber Threats to Elections

A LEXICON

Office of the Director of National Intelligence

Cyber Threat Intelligence Integration Center

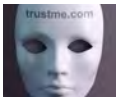
Contents


Scope Note **9**


Describing What's Happened: Common Terms **11**


Election-Specific Terms **15**


Common Cyber Terms **21**



Often Misused or Confusing Terms **29**


CYBER
SECURITY
EMAIL
BUSINESS
DESIGN
COMPUTER
DATA
MANAGER
ANALYSIS DESIGN
PRODUCTS
RESEARCH COMPUTER
TECHNOLOGY
INFORMATION
DATABASE
COMPUTER
CLIENT
STRATEGY
ANALYSIS
PROJECT
PLANNING
KNOWLEDGE
MANAGEMENT
SYSTEM
PROFESSIONAL
INTERNET LAPTOP MOBILE MOBILITY NETWORK
COMPUTING WORKSTATION WORLD DESKTOP
PROCESS
ACCESS

Scope Note

This reference aid draws on CTIIC's experience promoting interagency situational awareness and information sharing during previous significant cyber events—including cyber threats to elections. It provides a guide to cyber threat terms and related terminology issues likely to arise when describing cyber activity. The document includes a range of cyber-specific terms that may be required to accurately convey intelligence on a cyber threat event and terms that have been established by relevant authorities regarding technical infrastructure for conducting elections.

CTIIC will adhere to this terminology guide in future documents related to cyber threats to US elections and recommends use by others in the interest of consistency and clear communication.

Please note that this reference aid is not intended to address terminology related to political or other noncyber aspects of influence or interference involving elections, nor is it intended to be a comprehensive guide to cyber threat terminology.

Targeted/Targeting : A cyb
ctor's targeting of a particular
an refer to any aspect of the a
tempts to select a system to c

Describing What's Happened: Common Terms

The following terms are central to accurately describing cyber threat activity but are often used differently. CTIIC recommends their use be accompanied by definitions and any necessary context for nontechnical readers.

Attacked

Indicates that a cyber actor has attempted to degrade, destroy, disrupt, manipulate, or otherwise detrimentally affect the operation of a system or network. However, manipulation or deletion of data solely for the purpose of hiding one's tracks is not considered an attack. Some reports use "attack" and "exploit" synonymously, drawing in part on the cryptanalysis sense of "attack"—the use of a technical approach to defeat a security measure. The dual usage can cause confusion, especially for nontechnical readers, if the context does not fully explain the type of malicious cyber activity that occurred.

Compromised

Indicates that a victim system has installed malware, connected to a malicious Internet Protocol address, or provided a cyber actor unauthorized access to collect data or execute commands.

Exploited

Indicates that a malicious actor has conducted additional activities on a compromised system, such as collecting data, deploying more malware, or establishing persistent access. Some documents—within both the IC and the private sector—use exploited and compromised synonymously. In practice, however, cyber actors may compromise more accounts and systems than they exploit, in part because of the availability of tools to automate the process of compromising vulnerable systems. Distinguishing whether and how an actor has made use of a compromised system—whenever available intelligence allows—aids in understanding the impact and implications of the malicious cyber activity.

Scanned/Scanning

Scanning a system involves attempting to identify the security vulnerabilities the system may have by sending it specific network traffic and observing its responses. The definition is reasonably specific but can cause confusion—and potentially undue alarm—if it is assumed to include follow-on attempts to exploit any vulnerabilities discovered. Scanning is extremely common on the Internet but may have only a modest success rate, and cyber actors therefore scan far more systems than they actually affect.

Targeted/Targeting

A cyber actor's targeting of a particular victim can refer to any aspect of the actor's attempts to select a system to conduct operations against, learn about, find vulnerabilities, gain access, or conduct other malicious activities. The term also connotes an attempt at conducting malicious cyber activity, without indicating the degree of success an actor achieved. We recommend greater specificity and clarification of the specific usage whenever available intelligence allows.

Voting Machine : The mec
ectromechanical and electric
omponents of a voting system
oter uses to view the ballot, in

Election-Specific Terms

These terms have been defined by the US Election Assistance Commission (EAC), a bipartisan commission charged with developing voting system guidelines.

Audit

Systematic, independent, documented process for obtaining records, statements of fact, or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled.

Ballot

The official presentation of all of the contests to be decided in a particular election.

Central Count Voting System

A voting system that tabulates ballots from multiple precincts at a central location. Voted ballots are placed into secure storage at the polling place. Stored ballots are transported or transmitted to a central counting place, which produces the vote count report.

Claim of Conformance

Statement by a vendor declaring that a specific product conforms to a particular standard or set of standard profiles; for voting systems, National Association of State Election Directors (NASED) qualification or EAC certification provides independent verification of a claim.

Direct Recording Electronic (DRE) Voting System

System that uses electronic components for the functions of ballot presentation, vote capture, vote recording, and tabulation that are logically and physically integrated into a single unit. A DRE produces a tabulation of the voting data stored in a removable memory component and in printed hardcopy.

Election Databases

Data file or set of files that contain geographic information about political subdivisions and boundaries, all contests and questions to be included in an election, and the candidates for each contest.

Electronic Voting System

One or more integrated devices that use an electronic component for one or more of the following functions: ballot presentation, vote capture, vote recording, and tabulation.

Independent Testing Authority (ITA)

Replaced by “accredited testing laboratories” and “test labs.” Previous usage referred to independent testing organizations accredited by NASED to test voting system qualifications.

Internal Audit Log

A human-readable record, residing on the voting machine, used to track all activities of that machine. This log records every activity performed on or by the machine, indicating the event and when it happened.

Precinct Count Voting System

A system that tabulates ballots at the polling place, typically as they are cast, and prints the results after the close of polling. For DREs, and for some paper-based systems, these systems electronically store the vote count and may transmit results to a central location over public telecommunication networks.

Security Analysis

An inquiry into the potential existence of security flaws in a voting system. Includes an analysis of the system's software, firmware, and hardware, as well as the procedures associated with system development, deployment, operation, and management.

Security Controls

Management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Voting System

The total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information; and the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes to be made to a system after the initial qualification of the system; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

The following terms, which reflect the changing technology used at election polling stations, have been defined by organizations other than the EAC.

Ballot on Demand (BOD)

A dedicated application that prints out a dedicated ballot as each voter checks in. BODs may also be used by polling stations to print additional ballots in emergency situations.

Election Management System

Set of processing functions and databases within a voting system that defines, develops, and maintains election databases; performs election definitions and setup functions; formats ballots; counts votes; consolidates and reports results; and maintains audit trails.

Election Reporting System (ERS)

A web-based election management system that includes the following functionalities: candidate filing and ballot question entry; election night reporting (ENR) of results and statistics; post-election review module for statutorily required manual results review following state general elections; recount module for Federal, state, or county-level recounts; and numerous reports related to above functionalities.

Electronic Pollbook (e-Pollbook)

Hardware, software, or a combination of the two that allows election officials to review and/or maintain voter register information for an election but does not actually count votes. The functions of an e-pollbook often include voter lookup, verification, identification, precinct assignment, ballot assignment, voter history update, name change, address change, and/or the redirection of voters to correct voting location.

E-Voting

The act of casting any ballot in a public election or referendum on an electronic voting machine.

Internet Voting

The act of casting any ballot in a public election or referendum via the Internet.

Operational Environment

All software, hardware (including facilities, furnishings, and fixtures), materials, documentation, and the interface required for voting equipment operations used by the election personnel, maintenance operators, poll worker, and voters.

Remote Accessible Vote by Mail System

A mechanical, electromechanical, or electronic system and its software that is used for the sole purpose of marking an electronic vote by mail ballot remotely, outside a polling location, for a voter with disabilities or a military or overseas voter who would then be required to print the paper-cast vote record to be submitted to the elections official.

Voting Machine

The mechanical, electromechanical, and electric components of a voting system that voters use to view the ballot, indicate their selections, and verify those selections. In some instances, the voting machine also casts and tabulates the votes.

Cyberspace : A global doma
he information environment c
f the interdependent network
nformation technology infrast

Common Cyber Terms

The terms in this section are commonly used in cyber intelligence, investigations, operations, security, and general technology discussions. These terms will probably be encountered in finished intelligence and reporting on election issues.

Attribution

A determination of the perpetrators and/or sponsors of a cyber operation.

Availability

A guarantee of reliable access to the information by authorized people.

Beaconing

A process through which a system or program sends a message announcing its presence online. This term is typically used in a cyber threat context to indicate a compromised system communicating with an actor's command-and-control infrastructure to indicate its availability.

Confidentiality

A set of rules that limits access to information.

Cyber Deterrence

The prevention of cyber action by credibly demonstrating the ability and willingness to deny benefits or impose costs to convince the adversary that restraint will result in better outcomes than will confrontation.

Cyber Defense

A set of processes and measures to detect, monitor, protect, analyze, and defend against network infiltrations. *See Cyber Security.*

Cyber Disruption

Activities initiated by the threat actor that temporarily negatively alter or prevent the operation of the victim's network.

Cyber Effect

The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Cyber Espionage

The intentional clandestine acquisition of information from targeted networks without altering the information or affecting users' access.

Cyber Influence

The use of cyber operations to shape the perceptions or behavior of targeted audiences while maintaining plausible deniability.

Cyber Operation

An umbrella term to describe cyber attack, cyber espionage, cyber influence, or cyber defense, and intrusions or activities with unknown intent.

Cyberspace

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Security

The protection of information systems against unauthorized access to or modification of information contained therein, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. Also known as network security. *See Cyber Defense.*

Cyber Threat

Cyber operations or noncyber actions (intentional or accidental) that compromise the confidentiality, integrity, reliability, or availability of digital devices, systems, networks, or data.

Cyber Threat Intelligence

The collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, operational activities and indicators, and their impact or potential effects on US national security interests. Cyber threat intelligence also includes information on cyber threat actor information systems, infrastructure, and data; and network characterization or insight into the components, structures, use, and vulnerabilities of foreign cyber program information systems.

Data Integrity

A performance measure or service that ensures data has not been accidentally or maliciously modified, altered, or destroyed.

Database

A structured collection of data that is organized to provide efficient retrieval.

Destroy (Hardware/Software/Data)

Permanently, completely, and irreparably damage a victim's physical or virtual computer or information system(s), network(s), and/or data stores; for example, system administrators discover permanent unexplained damage to portions of the information system, or system users discover that data or files have been inappropriately corrupted or deleted.

Digital/Electronic Signature

Any mark in electronic form associated with an electronic document, applied with the intent to digitally sign the document.

Distributed Denial-of-Service (DDoS) Attack

A type of cyber attack designed to prevent users from accessing a network-connected service by sending simultaneous illegitimate requests from numerous sources. Data is sent to overload a network's resources.

Encoding

The process of translating binary characters into representing characters (e.g., letters and numbers).

Encryption

The conversion of plaintext, by means of a defined system (e.g., a "cipher"), so that it is unintelligible to an unauthorized recipient.

Exfiltration

The transfer, either electronically or physically, of information from a victim system by a threat actor without the data owner's permission.

Exploitation

The act of extracting and gathering intelligence data, often from a cyber attack or cyber espionage.

Hop Point

A compromised or commercially purchased intermediary system that is used as a proxy to disguise the attacker's true point of origin.

Information Security

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Insider Threat

The risk that one or more individuals with the access to and/or internal knowledge of a company, organization, or enterprise would exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

Intrusion Set

A group of cyber security incidents that share similar cyber actors, methods, or signatures.

Intrusion

A computer system or network compromise; may describe a broad range of activities used to support cyber attacks, cyber influence, or cyber espionage. *See also: Compromise, Penetration.*

Malicious Cyber Activity

Activities, other than those authorized by or in accordance with US law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Network

An information system comprising a collection of interconnected computers or devices.

Penetration

The unauthorized access or compromise of an electronic system, computer, or network by a cyber actor. *See also: Compromise, Intrusion.*

Persistence

The ability of malware (malicious software) to maintain access to a compromised system even after mitigation steps have been taken. Achieving some degree of persistence eliminates the need to reinfect a machine.

Personally Identifiable Information (PII)

Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Reconnaissance

The act of determining vulnerabilities in a targeted system or network. (Common examples include port scanning and open network traffic analysis.)

Remote Access (noun) or Remote-Access (modifier)

The ability to gain access to targeted systems or networks from a distance, such as over the Internet.

Router Operation

A method for compromising midpoint network infrastructure—such as routers—rather than specific computers or networks, to illicitly observe, redirect, tamper with, impede, or in some other way adversely affect network communications.

Server

A machine that provides services (for instance a web server, e-mail server, proxy server, file server, or print server) to other machines. In general, all machines on the Internet fall into two categories: clients and servers. Where the available intelligence permits, specify the type of server involved (e.g., an e-mail server).

Vulnerability

An exploitable flaw that can undermine a system's security. (This term is often used to describe the overall strategic perception of susceptibility to a given threat actor. It should only be used to describe a cyber-system issue.)

Zero Day (noun) or Zero-Day (modifier)

A cyber capability that relies on a vulnerability in the design or implementation of a system and can be used to violate its security. Neither the system designers, cyber security community, or general public are aware of the vulnerability.

Spoofing : Using a counterfe
nternet Protocol (IP) address o
n attempt to mislead the recip
e origin of the original comm

Often Misused or Confusing Terms

The terms in this category are commonly used in several contexts, including cyber security, intelligence, and election vernacular. We recommend against their use in finished analytic production because the terms lack necessary specificity or because they have been replaced with other terms in the common lexicon of the cyber community.

Advanced Persistent Threat (APT)

An industry term used to describe suspected offensive cyber activity in which the cyber actor occupies the network for an extended period while continuously penetrating systems and avoiding detection. *See Intrusion Set.*

Operational Relay Box (ORB) *See Hop Point.*

Proxy

A service that relays users' Internet traffic while hiding the link between users and their activity.

Spoofing

The use of a counterfeit domain, Internet Protocol (IP) address, or e-mail in an attempt to mislead the recipient as to the origin of the original communication or as a means of malicious redirection.