List of terms and definitions

(UK National Cyber Security Strategy)

Active Cyber Defence (ACD) – the principle of implementing security measures to strengthen the security of a network or system to make it more robust against attack.
Anonymisation – the use of cryptographic anonymity tools to hide or mask one's identity on the Internet.
Authentication – the process of verifying the identity, or other attributes of a user, process or device.
Automated system verification – measures to ensure that software and hardware are working as expected, and without errors.
Big data – data sets which are too big to process and manage with commodity software tools in a timely way, and require bespoke processing capabilities to manage their volumes, speed of delivery and multiplicity of sources.
Bitcoin – a digital currency and payment system.
Commodity malware – malware that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors.
Computer Network Exploitation (CNE) – cyber espionage; the use of a computer network to infiltrate a target computer network and gather intelligence.
Cyber Crime marketplace – the totality of products and services that support the cyber crime ecosystem.
Cryptography – the science or study of analysing and deciphering codes and ciphers; cryptanalysis.
Cyber attack – deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.
Cyber crime – cyber-dependent crime (crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber–enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach).
Cyber ecosystem – the totality of interconnected infrastructure, persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.
Cyber incident – an occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.
Cyber-physical system – systems with integrated computational and physical components; 'smart' systems.
Cyber resilience – the overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them.
Cyber security – the protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Cyberspace – the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controllers.

It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.

Cyber threat – anything capable of compromising the security of, or causing harm to, information systems and internet-connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.

Data breach – the unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.

Domain – a domain name locates an organisation or other entity on the Internet and corresponds to an Internet Protocol (IP) address.

Domain Name System (DNS) – a naming system for computers and network services based on a hierarchy of domains.

Doxing – the practice of researching, or hacking, an individual's personally identifiable information on the Internet, then publishing it.

e-commerce – electronic commerce. Trade conducted, or facilitated by, the Internet.

Encryption – cryptographic transformation of data (called 'plaintext') into a form (called 'cipher text') that conceals the data's original meaning, to prevent it from being known or used.

Horizon scanning – a systematic examination of information to identify potential threats, risks, emerging issues and opportunities allowing for better preparedness and the incorporation of mitigation and exploitation into the policy-making process.

Incident management – the management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

Incident response – the activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

Industrial Control System (ICS) – an information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.

Industrial Internet of Things (IIoT) – the use of Internet of Things technologies in manufacturing and industry.

Insider – someone who has trusted access to the data and information systems of an organisation and poses an intentional, accidental or unconscious cyber threat.

Integrity – the property that information has not been changed accidentally, or deliberately, and is accurate and complete.

Internet – a global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

Internet of Things – the totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

Malware – malicious software, or code. Malware includes viruses, worms, Trojans and spyware.

Network (computer) – a collection of host computers, together with the sub-network or inter-network, through which they can exchange data.

Offensive cyber – the use of cyber capabilities to disrupt, deny, degrade or destroy computers networks and internet-connected devices.

Patching – patching is the process of updating software to fix bugs and vulnerabilities
Penetration testing – activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.
Phishing – the use of emails that appear to originate from a trusted source, to deceive recipients into clicking on malicious links or attachments that are weaponised with malware, or share sensitive information, with an unknown third party.
Ransomware – malicious software that denies the user access to their files, computer or device until a ransom is paid.
Reconnaissance – the phase of an attack where an attacker gathers information on, and maps networks, as well as probing them for exploitable vulnerabilities in order to hack them.
Risk – the potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.
Router – devices that interconnect logical networks by forwarding information to other networks based upon IP addresses.
Script kiddie – a less skilled individual who uses ready-made scripts, or programs, that can be found on the Internet to conduct cyber attacks, such as web defacements.
Secure by default – the unlocking of the secure use of commodity technologies whereby security comes by default for users.
Secure by design – software, hardware and systems that have been designed from the ground up to be secure.
SMS spoofing – a technique which masks the origin of an SMS text message by replacing the originating mobile number (Sender ID) with alphanumeric text. It may be used legitimately by a sender to replace their mobile number with their own name, or company name, for instance. Or it may be used illegitimately, for example, to fraudulently impersonate another person.
Social engineering – the methods attackers use to deceive and manipulate victims into performing an action or divulging confidential information. Typically, such actions include opening a malicious webpage, or running an unwanted file attachment.
Trusted Platform Module (TPM) – an international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
User – a person, organisation entity, or automated process, that accesses a system, whether authorised to, or not.
Virus – viruses are malicious computer programs that can spread to other files.
Vishing – vishing or ‘voice phishing’ is the use of voice technology (landline phones, mobile phones, voice email, etc) to trick individuals into revealing sensitive financial or personal information to unauthorised entities, usually to facilitate fraud.
Vulnerability – bugs in software programs that have the potential to be exploited by attackers.