2C	Command & Control, indica un sistema centralizzato per coordinare e gestire bootnet e sferrare attacchi soprattutto di tipo DoS/DDoS.
Accesso remoto	Consente di collegare e di far interagire un sistema ICT con un altro, tipicamente un PC con un server e le sue applicazioni (anche in cloud).
Account	Insieme di informazioni di identificazione ed autenticazione di un utente di un sistema informativo. Tipicamente è costituito da un identificativo d'utente e da una password, ma può estendersi a certificati digitali, riconoscimenti biometrici e richiedere l'uso di token quali smart card, chiavette USB, ecc.
ACL	Access Control List: elenco di regole per il controllo degli accessi a risorse ICT.
ACN	Agenzia Cibernetica Nazionale
Active Directory	Sistema di directory della Microsoft, integrato nei sistemi operativi Windows dal 2000 in avanti. Utilizza SSO, LDAP, Kerberos, DNS, DHCP, etc.
Active X Control	File che contengono controlli e funzioni in Active X che "estendono" (eXtension) ed espletano specifiche funzionalità; facilitano lo sviluppo di software di un modulo software dell'ambiente Windows in maniera distribuita su Internet.
Address spoofing	Generazione di traffico (pacchetti IP) contenenti l'indicazione di un falso mittente (indirizzo sorgente IP).
Adware	Codice maligno che si installa automaticamente nel computer, come un virus o lo spyware, ma in genere si limita a visualizzare una serie di pubblicità mentre si è connessi a Internet. L'adware può rallentare sensibilmente il computer e nonostante costringa l'utente a chiudere tutte le finestre pop-up visualizzate, non rappresenta una vera minaccia per i dati, a meno che non nasconda un codice maligno.
AET	Advanced Elusion Techniques: tecniche avanzate di elusione degli strumenti di sicurezza in uso.
AI	Artificial Intelligence, che individua l'ampio campo delle tecniche e delle teorie di intelligenza artificiale. Indicata anche con l'acronimo italiano IA, Intelligenza Artificiale.
AIPSI	Associazione Italiana Professionisti Sicurezza Informatica.
AISE	Agenzia Informazioni e Sicurezza Esterna.
AISI	Agenzia Informazioni e Sicurezza Interna.
Alert	Viene spesso usato il termine inglese di "allarme" per indicare segnalazione di eventi e problemi inerenti la sicurezza informatica; la segnalazione può essere generata sia da dispositivi di monitoraggio e controllo sia dalle persone addette.
API	Application Programming Interface
App	Neologismo ed abbreviazione di "application" (applicazione) per indicare, anche in italiano, le applicazioni operanti localmente sui sistemi mobili, tipicamente su smartphone.
Architettura di un Sistema Informativo (SI)	Insieme strutturato di componenti hardware, software, dati, reti e processi progettato per raccogliere, elaborare, memorizzare e distribuire informazioni a supporto delle attività operative e decisionali di un'organizzazione.
Architettura di sicurezza informatica (o digitale o ICT)	Framework strutturato che definisce politiche, tecnologie e controlli per proteggere risorse IT, reti e dati da minacce. Integra sicurezza su cloud, reti, dispositivi (IoT/Endpoint) e si basa su principi come la triade CIA (Confidenzialità, Integrità, Disponibilità) e il modello Zero Trust.
ASAT	Armi anti satellite informatiche
ATP	Advanced Persistent Threat: attacco persistente e sofisticato, basato su diverse tecniche operanti contemporaneamente e capaci di scoprire e sfruttare diverse vulnerabilità. Usato da organizzazioni con grandi capacità e risorse.
Attacco mirato	O specifico, indicato sovente con il termine inglese targeted attack: attacco portato ad uno specifico sistema obiettivo, o a un gruppo similare di obiettivi, con tecniche sofisticate e specifiche per il sistema target. Viene incluso sovente tra gli ATP.
Attacco massivo	Attacco rivolto ad una grande massa di obiettivi simili, anche dell'ordine di milioni: può essere semplice e non sofisticato, ma nella massa qualche attacco va quasi sempre a buon fine. Tipici esempi i phishing ed i ransomware.
Audit	Per la sicurezza digitale, il risultato di un auditing.
Auditing	Per la sicurezza digitale, il processo documentato di revisione (ossia verifica, controllo e valutazione) della efficacia delle misure in essere e della loro gestione, oltre che della

	conformità di tali misure alle leggi vigenti e alle normative, anche interne, che devono essere seguite.
avvelenamento modelli AI	Chiamato in inglese “data poisoning”, si verifica quando dati di addestramento compromessi deviano il comportamento dell'AI
Backdoor	Interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d’accesso.
BAS	Building Automation Systems: sistemi di controllo, gestione e automazione di dispositivi hardware e software all’interno di un edificio. In Italia si usa più sovente il termine di “domotica”.
BIA	Business Impact Analysis.
Blade server	"Lama", ossia scheda omnicomprensiva di elaborazione di un sistema ad alta affidabilità costituito da più lame interconnesse ed interoperanti.
Blended Threats	Attacco portato con l’uso contemporaneo di più strumenti, tipo virus, worm e trojan horse.
Bluetooth	Protocollo, standard de facto, di collegamento senza fili a brevi distanze. Opera in radio frequenza in campi attorno ai 2,45 GHz.
Bots	Programmi, chiamati anche Drones o Zombies, usati originariamente per automatizzare talune funzioni nei programmi ICR, ma che ora sono usati per attacchi distribuiti.
Botnet	Insieme di computer in rete, chiamati “zombi”, che a loro insaputa hanno agenti (programmi) malevoli dai quali partono attacchi distribuiti, tipicamente DDOS.
Buffer overflow	Consiste nel sovra-scrivere in un buffer o in uno stack del programma dati o istruzioni con i quali il programma stesso può comportarsi in maniera diversa dal previsto, fornire dati errati, bloccare il sistema operativo, ecc.
Bug	Traducibile come “baco”, individua un errore, difetto o guasto nel software o nell'hardware che causa un malfunzionamento, portando il programma a comportarsi in modo inaspettato, errato o a bloccarsi (crash). Spesso derivano da errori umani nella scrittura del codice, che possono variare da lievi anomalie a gravi vulnerabilità di sicurezza.
BYOD	Bring Your Own Device: policy aziendale che consente l'utilizzo di dispositivi mobili di proprietà dell'utente anche nell'ambito dei sistemi dell'azienda/ente. Il fenomeno è chiamato anche “consumerizzazione”.
CAaaS	Cyber Attack as a Service.
CAPTCHA	Completely Automated PublicTuring test to tell Computers and Humans Apart: l'acronimo indica una famiglia di test costituita da una o più domande e risposte per assicurarsi che l'utente sia un essere umano e non un programma software.
CASB	Cloud Access Security Brokers.
C&C	Command&Control: Sistema centrale di commando e controllo di una botnet.
CED	Centro Elaborazione Dati: centro di calcolo ove risiedono tutti i sistemi centralizzati di elaborazione, archiviazione e trasmissione dei dati.
CER	Critical Entities Resilience: Direttiva UE 2022/2557, recepita in Italia dal D. Lgs 134/2024, sulla resilienza dei soggetti critici.
CERT	Computer Emergency Response Team.
Chatbot	Programma software realizzato per interagire con gli umani via voce e/o scambi di testi. Hanno numerose applicazioni, tipicamente l’assistente virtuale digitale, ma possono essere programmati per agire in maniera malevola e costituire un componente di un attacco digitale.
Cybersquatting	Acquisto e/o registrazione di un nome di dominio web identico o simile a un dominio esistente, con l'intento illegale e truffaldino di trarre profitto illegalmente da un marchio, da un nome di azienda o da un nome di persona famosa cui il dominio fa di fatto riferimento.
Churn rate	Tasso di abbandono a favore della concorrenza, tipicamente dopo un attacco.
CIO	Chief Information Officer: il responsabile dell’intero sistema informatico.
CISA	Cybersecurity and Infrastructure Security Agency negli US
CISA	Certified Information Systems Auditor di ISACA.
CISO	Chief Information Security Officer: il responsabile della sicurezza digitale dell’intero sistema informativo.
CISR	Comitato interministeriale per la sicurezza della Repubblica.

CISSP	Certified Information Systems Security Professional.
Cyber warfare	Guerra cibernetica, chiamata anche guerra informatica o guerra elettronica.
Cluster	Insieme di computer e/o di schede (es lame di un sistema blade) cooperanti per aumentare l'affidabilità complessiva del sistema; il termine è anche usato per identificare un insieme contiguo di settori in un disco rigido.
CNA	CVE Numbering Authority
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, all'interno della Polizia Postale e per la Sicurezza Cibernetica.
COBIT	Control Objectives for Information and related Technology: consolidata best practice per il governo (governance) di un SI ed il suo audit.
Consumerizzazione	Si veda BYOD.
Container	Istanza di un ambito virtualizzato di applicazioni, che isola le risorse hardware e software in uso da ognuna di esse, pur sempre all'interno di un solo e unico sistema operativo.
COPASIR	Comitato parlamentare per la sicurezza della Repubblica: è l'organo di controllo parlamentare sulle agenzie italiane di intelligence.
COR	Comando Operazioni in Rete (Ministero Difesa).
CPS	Cyber-Physical System (in ambiti OT).
CRAMM	CCTA Risk Analysis and Management Method
Crash	Blocco di un software o di un intero sistema ICT per un suo malfunzionamento, il più delle volte causato da errori nel software, ma che può anche essere causato da errori degli utenti finali o privilegiati.
CRM	Customer Relationship Management: applicativo di gestione dei clienti, anche potenziali, che normalmente viene integrato o è parte di un sistema ERP.
Cryptojacking	Utilizzo di capacità elaborativa di un inconsapevole sistema ICT target da parte di un cybercriminale per creare criptovaluta.
CSIRT	Computer Security Incident Response Team, italiano, ora sotto ACN
Crowdturfing	Combinazione di "crowdsourcing" e "astroturfing", indica un attacco basato su recensioni scorrette e false per danneggiare la reputazione di un prodotto o di una azienda/ente.
CSaaS	Cyber Security as a Service
CSO	Chief Security Officer; responsabile della sicurezza dell'intera azienda/ente, prevalentemente per la sicurezza fisica di edifici e del personale. In alcune organizzazioni il CISO riporta a questa figura.
CSSLP	Certified Secure Software Lifecycle Professional.
CTO	Chief Technology Officer: è il direttore tecnico di più alto livello, tipicamente per aziende che producono prodotti e servizi ICT. In talune organizzazioni il CIO riporta a questa figura.
CTTA	Central Computer and Telecommunications Agency del Governo UK, ora chiamato Cabinet Office.
CVE	Common Vulnerabilities and Exposures: l'acronimo indica sia il programma di identificazione e classificazione delle vulnerabilità tecniche di ogni sistema e servizio ICT, sia l'elenco dei record delle vulnerabilità identificate.
CVSS	Common Vulnerability Scoring System: metrica internazionale di valutazione della gravità di una vulnerabilità di un sistema ICT.
CWE	Common Weakness Enumeration
DAC	Discretionary Access Control.
Darknet	Rete virtuale privata nella quale gli utenti si connettono solamente con persone di cui si fidano.
Dark web	Siti web che si raggiungono via Internet ma attraverso specifici software, configurazioni e accessi autorizzativi, e non sono indicizzati, e quindi ritrovabili, dai motori di ricerca. Molti dark web contengono informazioni criminali, dalla pedopornografia a strumenti informatici di attacco e da account e identità digitali rubate che sono poste in vendita.
Data Breach	Letteralmente "violazione dei dati", spesso è usato come sinonimo di furto di dati. Tecnicamente è usato per indicare l'accesso a banche dati o a file system contenenti identità digitali ed informazioni personali.
Data Center	Centro Dati: si veda CED.
Data poisoning	Si veda Avvelenamento dati AI.

DB	Data Base: banca dati.
DBMS	Data Base Management System.
DCS	Distributed Control System (ambiti OT). Sistema di automazione industriale in cui le funzioni di controllo non sono centralizzate, ma distribuite su più controllori autonomi dislocati vicino alle macchine. Collegati in rete, gestiscono complessi processi produttivi continui, offrendo alta affidabilità, facile manutenzione e supervisione centralizzata (HMI/SCADA)
Deadlock	Condizione in cui due o più processi non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.
Deamon	Software di base operante in back-ground in un ambiente multi-tasking.
Defacement o Defacing	In inglese significa deturpare, e nel gergo della sicurezza digitale indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
DES	Data Encryption Standard.
DevHub	Centro risorse Cisco per sviluppatori che fornisce strumenti, codice e documentazione per la creazione e l'integrazione di applicazioni con le tecnologie Cisco.
DoS/ DDoS	Denial of Service e Distributed Denial of Service: attacco per saturare sistemi e servizi ed impedire la loro disponibilità.
Dialer	Programma software che connette il sistema ad Internet, ad una rete o ad un computer remoto tramite linea telefonica (PSTN o ISDN); può essere utilizzato per attacchi e frodi.
DKIM	Domain Keys Identified Mail: in ambito DMARC, chiavi di crittografia asimmetrica per l'autenticazione di ogni messaggio di posta elettronica. Il messaggio viene firmato dal server e il destinatario controlla i messaggi con la chiave pubblica DKIM, che viene fornita nel DNS del dominio.
DMARC	Domain-based Message Authentication, Reporting, and Conformance: sistema standard di autenticazione dei messaggi di posta elettronica, che aiuta gli amministratori della posta a impedire che hacker e altri malintenzionati eseguano lo spoofing dell'organizzazione e del dominio
DNS	Domain Name System.
Docker	Software per la creazione di container.
DLP	Data Loss Prevention: sistemi e tecniche per prevenire la perdita e/o il furto di dati nel corso del loro trattamento, archiviazione inclusa.
DMZ	DeMilitarized Zone: isola del sistema informatico costituita da sottoreti locali, fisiche o virtuali, ove sono allocati i server esposti ad Internet.
DNS	Domain Name System: sistema gerarchico di nomi (naming) di host su Internet che vengono associati al loro indirizzo IP di identificazione nella rete.
DORA	Digital Operational Resilience Act: regolamento europeo UE 2022/2554 che stabilisce un quadro unificato per la gestione dei rischi informatici nel settore dei servizi finanziari dell'Unione Europea.
Download	Azione di scaricare file, tipicamente via Internet
Drive-by Downloads	Attacchi digitali causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
Drones, Droni	Si veda bots.
ECDL	European Computer Driving Licence,è il patentino europeo di conoscenza di vari aspetti dell'ICT soprattutto nell'ottica dell'utente finale. Ideato, realizzato e gestito da AICA, da più di venti anni, ha recentemente cambiato nome in ICDL
eCF	European Competence Framework: quadro europeo standardizzato sulle competenze digitali e sui ruoli ICT che espletano professionalmente tali competenze.
ECSF	European Cybersecurity Skills Framework, emanato a fine 2022 da ENISA: considera 10 ruoli per la sicurezza digitale, tra cui il CISO.
EDGE	Enhanced Data rates for GSM Evolution.
EDR	Endpoint Detection and Response. Sistema di sicurezza informatica che monitorizza in tempo reale gli Endpoint di un sistema informativo, per rilevare, analizzare e bloccare automaticamente comportamenti sospetti e/o attacchi digitali.
eIDAS	electronic IDentification Authentication and Signature: fornisce la normativa di base a livello UE sull'identità digitale per i servizi fiduciari e l'identificazione elettronica degli

	Stati membri. Il precedente Regolamento UE n. 910/2014 è stato aggiornato e superato dal nuovo Regolamento UE n. 1183/2024.
ENISA	European Union Agency for Cybersecurity.
End Point, EndPoint, endpoint	Punto finale. Indica i dispositivi finali che includono PC, server e smartphone.
ERP	Enterprise Resource Planning: software gestionale integrato che pianifica e automatizza i processi aziendali chiave (finanza, risorse umane, produzione, logistica, vendite) in un unico database centrale.
ETACS	Extended TACS.
ETL	ENISA Threat Landscape.
Ethical hacking	Attività di provare attacchi ai fini di scoprire bachi e vulnerabilità dei programmi, e porvi rimedio con opportune patch/fix.
EUCIP	European Certification of Informatics Professionals: ora sostituito da eCF.
Exploit	Attacco ad una risorsa ICT utilizzando sue vulnerabilità.
Extranet	Intranet accessibile anche da utenti esterni all'azienda/ente.
FIMI	Foreign Information Manipulation Interference.
FIRST	Forum of Incident Response and Security Teams, che attualmente ha in carico la gestione della metrica CVSS.
Fix	Software di correzione di un programma software, in particolare di una o più sue vulnerabilità. E' un tipo di patch, ma è usato spesso come suo sinonimo.
FTP	File Transfer Protocol: protocollo per il trasferimento di file.
Flash threats	Tipi di virus in grado di diffondersi molto velocemente.
Flooding	Letteralmente significa "allagamento" ed è un termine associato a varie tecniche per attacchi DoS/DDoS.
Form	In informatica indica il campo generato da una applicazione visibile su una schermata, nel quale l'utente deve inserire dei caratteri per interagire con l'applicazione stessa; è l'elemento base per l'interfaccia tra utente e applicazione per l'inserimento dei dati (data entry).
Framework	Struttura di supporto, tecnica o concettuale, che fornisce una base predefinita (librerie, strumenti, linee guida) per sviluppare software o gestire processi complessi in modo efficiente.
FSD	Fornitori di Servizi Digitali, così come definiti da NIS.
FTP	File Transfer Protocol: protocollo per il trasferimento di file.
FTPS	File Transfer Protocol Secure: per il trasferimento di file crittati
FW	FireWall generico, normalmente di rete. E' un sistema di sicurezza informatica che funge da barriera tra una rete fidata (come la LAN aziendale o domestica) e reti non fidate (Internet). Analizza il traffico dati in entrata e in uscita basandosi su regole preimpostate per bloccare accessi non autorizzati e minacce.
FWA	FireWall Applicativo. A differenza dei firewall di rete, analizza il contenuto effettivo dei pacchetti dati (Deep Packet Inspection), bloccando minacce specifiche per applicazioni e siti web, come SQL injection o cross-site scripting (XSS).
GDPR	General Data Protection Regulation: Regolamento 2016/679 UE per la protezione dei dati personali delle persone fisiche (privacy).
GenAI	AI generativa: una branca dell'intelligenza artificiale che si concentra sulla creazione di nuovi contenuti originali, come testo, immagini, musica, audio e video
GPRS	General Packet Radio Service.
GSM	Global System for Mobile communications.
Hactivism	Termine derivato dalla combinazione di hack e di activism, indica un uso sovversivo dell'ICT per promuovere un'ideologia politica/religiosa e la sua agenda o un cambiamento sociale.
Hijacking	Tipico attacco in rete "dell'uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding).

HMI	Human-Machine Interface, Interfaccia Uomo-Macchina. E' un software che consente agli operatori di interagire con macchine e sistemi industriali, tipicamente tramite pannelli video.
Hoax	In italiano "bufala" o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
Honeynet	Rete di honeypot.
Honeypot	Sistema "trappola" su Internet per farvi accedere con opportune esche possibili attaccanti e poterli individuare.
Hosting	Servizio che "ospita" risorse logiche ICT del Cliente su hardware del fornitore del servizio.
Housing	Concessione in locazione di uno spazio fisico, normalmente in un Data Center già attrezzato, ove riporre, funzionanti, le risorse ICT di proprietà del Cliente.
HSDPA	High Speed Downlink Packet Access.
HTTPS	HyperText Transfer Protocol Secure: protocollo sicuro per le transazioni crittate tra browser e sito web, e viceversa.
Hypervisor	Elemento di base di un sistema virtualizzato, che crea e gestisce sistemi virtuali.
IA	Intelligenza Artificiale, si veda AI
IAA	Identificazione - Autenticazione – Autorizzazione: per il controllo degli accessi ai sistemi ICT.
IaaS	Infrastructure as a Service.
IAM	Identity & Access Management.
ICDL	International Certification of Digital Literacy. Nuovo nome dato alle precedenti certificazioni ECDL di AICA, portate a livello europeo ed internazionale e che rappresentano lo standard riconosciuto per la computer literacy.
ICS	Industrial Control System (in ambienti OT).
IDS	Intrusion Detection System.
Information Leakage	Diffusione-dispersione non autorizzata di informazioni.
Info stealer (anche infostealer)	Malware progettati per carpire informazioni, tipicamente quelle di un utente mentre effettua un login
Intranet	Rete e server operanti in http/https ed accessibili solo ad utenti interni ad una data azienda/ente.
IoT	Internet of Things (Internet delle Cose): componenti/sistemi intelligenti ed interoperanti su Internet, tipici di ambienti OT.
IIoT	Industrial IoT.
IPS	Intrusion Prevention System
ISACA	Information Systems Audit and Control Association.
ISSA	Information Systems Security Association: AIPSI è il suo capitolo italiano
ISTAT	Istituto Nazionale di Statistica
ITIL	Information Technology Infrastructure Library: consolidata best practice per la gestione operativa (management) di un SI.
Jailbroken	Sistema AI in cui sono state aggirate le restrizioni di sicurezza imposte dagli sviluppatori, solitamente attraverso l'uso di specifici "prompt" o comandi ingannevoli per farla agire in modi che normalmente non le sarebbero permessi, ad esempio generando contenuti inappropriati o aggirando le sue linee guida etiche.
Jamming	In informatica è un attacco che consiste nell'interferire o bloccare intenzionalmente i segnali wireless di un sistema, solitamente tramite un dispositivo chiamato "jammer"
Jammer	Dispositivo "disturbatore" che emette segnali sulla stessa frequenza dei dispositivi bersaglio per sovraccaricarli, diminuire il rapporto segnale-rumore e impedire o degradare la comunicazione wireless, compromettendo sistemi di navigazione, reti cellulari, allarmi di sicurezza e altri dispositivi connessi.
Key Logger	Sistema di tracciamento dei tasti premuti sulla tastiera per poter carpire informazioni quali codici, chiavi, password.
Kerberos	Metodo sicuro per autenticare la richiesta di un servizio, basato su crittografia simmetrica. Utilizzato da Active Directory.
KEV	Known Exploited Vulnerabilities, catalogo basato su CVE e gestito dalla agenzia statunitense CISA

Kubernets	Sistemi per la gestione di carichi di lavoro e servizi containerizzati, in grado di facilitare sia la configurazione dichiarativa che l'automazione.
LDAP	Lightweight Directory Access Protocol: protocollo standard per la gestione e l'interrogazione dei servizi di directory che organizzano e regolano in maniera gerarchica le risorse ICT ed il loro utilizzo da parte degli utenti. Il termine LDAP indica anche il sistema di directory nel suo complesso.
Log bashing	Operazioni tramite le quali un attaccante cancella le tracce del proprio passaggio e attività sul sistema attaccato. Vengono ricercate e distrutte le voci di registri, log, contrassegni e file temporanei, ecc. Possono operare sia a livello di sistema operativo (es. deamon sui server Unix/Linux), sui registri dei browser, ecc. Esistono innumerevoli programmi per gestire le registrazioni, ma sono tecnicamente complessi.
LTE	Long Term Evolution.
MAC	Mandatory Access Control.
MAC	Codice indirizzo assegnato in modo univoco ad ogni scheda di rete.
MAC	Media Access Control: sub strato del livello datalink del modello ISO/OSI.
MAC flooding	Tecnica di attacco tipo DoS/DDoS ad un dispositivo con indirizzo MAC per saturarlo e bloccarne il corretto funzionamento.
Malicious insider	Attaccante interno all'organizzazione cui viene portato l'attacco.
Malvertising	Contrazione di "malicious advertisements": pubblicità malevola, con pagine web che nascondono un codice maligno o altre tecniche di attacco, come il dirottamento su siti web mascherati e fraudolenti.
Malware	Termine generico che indica qualsiasi tipo di programma software di attacco.
MaaS	Malware as a Service: fornitura in cloud di malware (a pagamento).
Media sintetici	Qualsiasi tipo di video, immagini, oggetti virtuali, suoni o parole prodotti dall'intelligenza artificiale (o con l'aiuto di essa).
MEHARI	MEthod for Harmonized Analysis of RIsk
MFA	Multi-Factor Authentication: autenticazione con più fattore, ad esempio con certificati, token diversi e identificazioni biometriche
Microservizi	Approccio allo sviluppo ed all'organizzazione dell'architettura dei software, evoluzione dell'architettura SOA e dell'object orientation. I microservizi sono moduli software autonomi, specializzati, indipendenti di piccole dimensioni che comunicano tra loro tramite API ben definite. Le architetture dei microservizi permettono di scalare e sviluppare le applicazioni in modo rapido e semplice.
Mirroring	termine inglese per indicare la replica e la sincronizzazione di dati su due o più dischi.
MSS	Managed Security Service.
MSSP	Managed Security Service Provider: fornitore di servizi per la sicurezza digitale.
NAC	Network Access Control: termine usato con più significati, che complessivamente indica un approccio architetturale ed un insieme di soluzioni per unificare e potenziare le misure di sicurezza a livello del punto di accesso dell'utente al sistema informativo.
NCA	National Crime Agency del Regno Unito
NCS	Nucleo per la cybersicurezza ora operante in ambito ACN.
NFT	Non Fungible Token: è un gettone non riproducibile nell'ambito di una blockchain. Gli NFT sono associati a beni virtuali, da un documento a un'opera d'arte, e come tali hanno un mercato mondiale.
NIS	Network and Information Security: direttiva UE 2016/1148, recepita in Italia con il D. Lgs. n. 65 del 18/5/2018, che definisce le misure di sicurezza digitale necessarie a livello di ogni paese membro per le infrastrutture ICT critiche, chiamate anche "servizi essenziali".
NIS2	Aggiornamento ed ampliamento della NIS con direttiva UE 2022/2555, recepita in Italia dal D. Lgs. 138/2024.
NIST	National Institute of Standards and Technology
NSTPFT	Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy.
NVD	National Vulnerability Database statunitense, gestito da NIST

OASIS	Consorzio di aziende ICT no profit che fornisce norme implementative per alcuni standard, tra i quali la SOA e la sua sicurezza (SALM SPML, XACML).
OLE	Object Linking and Embedding.
OPC	OLE for Process Control (ambito OT).
OPS	Open Platform Communications. Standard de facto per la comunicazione tra sistemi OT
OPS UA	Open Platform Communications Unified Architecture.
OSA	Open Security Architecture.
OT	Operational Technology. Il termine indica l'insieme di sistemi ICT che monitora, controlla e gestisce dispositivi, processi e infrastrutture fisiche, come macchinari industriali, robot, reti elettriche, sistemi di anali medica quali TAC.
OTP	One Time Password: logica e/o dispositivo che genera password da usarsi una sola volta per sessione/transazione.
Outsourcer	Fornitore di servizi digitali terziarizzati.
Outsourcing	Utilizzo di Servizi terziarizzati
OWASP	Open Web Application Security Project
PaaS	Platform as a Service.
PAC	Pubblica Amministrazione Centrale.
PAC	Programmable Automation Controller (ambiti OT)
PAL	Pubblica Amministrazione Locale.
PAM	Privileged Access Management.
Patch	Traducibile in italiano come “toppa”, è un software per aggiornare, correggere bug o migliorare un programma.
Payload	“Carico utile” di informazioni all’interno di un programma, di un protocollo, ecc.; tipicamente è il codice maligno da attivare sul sistema attaccato dopo esservi penetrati.
PEC	Posta Elettronica Certificata.
Pharming	Attacco digitale per carpire informazioni riservate di un utente basato sulla manipolazione dei server DNS o dei registri del sistema operativo del PC dell’utente.
Phishing	Attacco digitale di social engineering per carpire informazioni riservate di un utente, basato sull’invio di un falso messaggio in posta elettronica che fa riferimento ad un ente primario, che richiede di collegarsi ad un server (trappola) per controllo ed aggiornamento dei dati.
PID	Proportional-Integral-Derivative (in ambito OT)
Ping of death	Invio di pacchetti di ping di grandi dimensioni (ICMP echo request), che blocca la pila di protocolli TCP/IP: è un tipo di attacco DoS/DDoS.
PLC	Programmable Logic Controller (ambiti OT).
PMI	Piccole e Medie Imprese: sotto i 250 dipendenti.
PNRR	Piano Nazionale di Ripresa e di Resilienza.
Port scanner	Programma software che esplora una fascia di indirizzi IP sulla rete per verificare quali porte, a livello superiore, sono accessibili e quali vulnerabilità eventualmente presentano. È uno strumento di controllo della sicurezza, ma è anche uno strumento propedeutico ad un attacco.
Provisioning	Attività grazie alle quale vengono fornite le opportune risorse ICT e la loro configurazione, in particolare i diritti d’accesso, ad utenti di un SI
PUP	Potentially Unwanted Programs: programma che l’utente consente di installare sui suoi sistemi ma che, a sua insaputa, contengono codici maligni o modificano il livello di sicurezza del sistema. Tipici esempi: adware, dialer, sniffer, port scanner.
QR	Quick Response: è un codice a barre bidimensionale, ossia a matrice, che è impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.
Race condition	Termine che indica le situazioni derivanti da condivisione di una risorsa comune, ad esempio un file o un dato, ed in cui il risultato viene a dipendere dall'ordine in cui vengono effettuate le operazioni.
Ransomware	Codice maligno che restringe e/o blocca i diritti d'accesso e tramite il quale viene chiesto un riscatto (ransom) per far funzionare correttamente il sistema.
RBAC	Request Based Access Control.
RBAC	Role Based Access Control.

RDoS	Ransom Denial of Service: gli attaccanti ricattano minacciando un attacco DoS/DDoS.
RFID	Radio-Frequency Identification: tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti oggetti, animali o persone, basata su un tag intelligente identificativo dell'entità oggetto dell'identificazione ed un dispositivo in grado di riconoscere l'entità se in sua prossimità, scambiando in radio frequenza delle informazioni.
Ricatto	L'attacco digitale perpetrato viene poi usato per ricattare l'attaccato perché paghi per non subirne di altri, magari più perniciosi. Il malware ransomware ha come tipica motivazione il ricatto, che è un tipo della più generale frode informatica.
Ritorsione	L'attacco digitale è stato portato come "vendetta" verso torti subiti, o come tali ritenuti: tipico il caso di un dipendente cui è stata negata una sua richiesta, o di ex dipendente licenziato. L'attaccante intende "colpire" con un attacco digitale l'Azienda/Ente che ritiene "colpevole" dei (presunti) torti subiti.
Robot	Un sistema in grado di svolgere, più o meno indipendentemente, un lavoro al posto dell'uomo
Robotica	La disciplina dell'ingegneria che studia e sviluppa metodi che permettano a un robot di eseguire dei compiti specifici riproducendo in modo automatico il lavoro umano.
Rogueware	Falso antivirus che a sua volta è un codice maligno che infetta il sistema.
Rootkit	Programma software di attacco che consente di prendere il completo controllo di un sistema, alla radice come indica il termine.
RPU	Remote Processor Unit (in ambiti OT).
SaaS	Software as a Service.
SALM	Security Assertion Markup Language.
SASE	Secure Access Service Edge.
SCADA	Supervisory Control And Data Acquisition: sistema informatico distribuito per il controllo ed il monitoraggio di processi, ed in parte per la loro automazione, in ambiti OT.
Scam	Tentativo di truffa via posta elettronica. A fronte di un millantato forte guadagno o forte vincita ad una lotteria, si chiede di versare un anticipo o pagare una tassa.
Scammer	Chi effettua uno scam.
SCAP	Security Content Automation Protocol.
SCC	Security Command Centre.
Scareware	Software d'attacco che finge di prevenire falsi allarmi, e diffonde notizie su falsi malware o attacchi.
Scraping	Letteralmente significa "raschiando", è il termine usato per indicare l'attività di ricerca e raccolta, in maniera automatica, di determinate informazioni dai sistemi connessi in Internet.
SD-WAN	Software Defined WAN (Wide Area Network)
SGSI	Sistema Gestione Sicurezza Informatica.
SIEM	Security Information and Event Management: sistemi e servizi per la gestione in tempo reale di informazioni ed allarmi generati dalle risorse ICT di un sistema informativo, inclusi i log.
Sinkhole	metodo per reindirizzare specifico traffico Internet per motivi di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
Sistema Informatico	Insieme dei sistemi e dei servizi ICT, dalle reti ai server ed agli applicativi, anche terziarizzati e in cloud, organizzato in una specifica architettura e che una azienda/ente usa a supporto delle proprie attività. Il sistema informatico può includere anche i dispositivi d'utente fissi e mobili (PC, smartphone, tablet, etc.), i sistemi di automazione e controllo industriale (DCS, PLC, robot, ecc.) ed i dispositivi IoT. Il termine indica quindi l'insieme dei sistemi ICT che lo costituiscono
Sistema Informativo	Indica il Sistema Informatico con tutte le informazioni che vi sono trattate.
Sniffing-snooping	Tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
Slack	Servizio di messaggistica per le aziende che collega le persone alle informazioni di cui hanno bisogno, creando e gestendo gruppi di lavoro.

Smart city	Città “intelligente” largamente dotata di infrastrutture e soluzioni ICT sia per i suoi abitanti e per interagire con loro, sia per migliorare il controllo del territorio, della sua sicurezza, dell’ambiente, della viabilità, ecc.
Smart grid	Grid è la rete elettrica di distribuzione di energia, che affiancata da una rete informatica che la gestisce diviene “smart”.
Smishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato sull’invio di SMS. E’ l’analogo del phishing con la posta elettronica.
SMS	Short Message Service.
Smurf	Tipo di attacco per la saturazione di una risorsa, avendo una banda trasmissiva limitata. Si usano tipicamente pacchetti ICMP Echo Request in broadcast, che fanno generare a loro volta ICMP Echo Replay.
SOA	Service Oriented Architetture.
SOAR	Security Orchestration, Automation and Response: sistemi di automazione ed integrazione dei vari strumenti e processi di sicurezza digitale.
SOC	Security Operation Centre
Social Engineering	Ingegneria sociale: con questo termine vengono considerate tutte le modalità di carpire informazioni, quali l’user-id e la password, per accedere illegalmente ad una risorsa informatica.
Spamming	Invio di posta elettronica “indesiderata” all’utente.
SPF	Sender Policy Framework: in DMARC, un record di testo DNS nel dominio considerato, che indica ai servizi di posta e ai ricevitori di ricevere l'e-mail dall'IP del server fornito nel record SPF.
SPID	Sistema Pubblico di Identità Digitale: è attualmente obbligatorio per accedere on line ai servizi digitali delle Pubbliche Amministrazioni.
SPML	Service Provisioning Markup Language.
Spoofing	Attacco digitale che falsifica l'indirizzo nell'intestazione Da: di un messaggio email. Un messaggio contraffatto mediante lo spoofing sembra provenire dall'organizzazione o dal dominio la cui identità è stata rubata.
Spyware	Codice maligno che raccoglie informazioni riguardanti l’attività online di un utente (siti visitati, acquisti eseguiti in rete, etc.) senza il suo consenso, utilizzandole poi per trarne profitto, solitamente attraverso l’invio di pubblicità mirata.
SQL	Structured Query Language: linguaggio per interazione con un DB relazionale.
SQL injection	Tecnica di inserimento di codice in un programma che sfrutta delle vulnerabilità sul database con interfaccia SQL che viene usata dall’applicazione.
SSCP	Systems Security Certified Practitioner.
SSO	Single Sign On: autenticazione unica per avere accesso a diversi sistemi e programmi.
Stealth	Registrazione invisibile.
Stuxnet	Uno dei primi e più noti attacchi ATP, portato ai sistemi di controllo delle centrifughe delle centrali nucleari iraniane.
SYN Flooding	Invio di un gran numero di pacchetti SYN a un sistema per intasarlo (DoS/DDoS).
Supply Chain	Catena di approvvigionamento o di fornitura. Questo termine indica l'insieme complesso di processi, attività, persone, organizzazioni e risorse coinvolte nella creazione e vendita di un prodotto, dal fornitore di materie prime al cliente finale. Include pianificazione, approvvigionamento, produzione, logistica e distribuzione. L’interazione informatica tra i vari attori di una supply chain può rappresentare u serio rischio d’attacco, che pate sempre dall’interlocutore con un sistema informativo con minori livelli di sicurezza digitale, e quindi più vulnerabile.
TA	Targeted Attacks: attacchi mirati, talvolta persistenti, effettuati con più strumenti anche contemporaneamente; rientrano in questa categoria APT e Watering Hole.
TACS	Total Access Communication System.
Telegram	Servizio di messaggistica istantanea e di broadcasting criptato e gratuito.
TLC	Telecomunicazioni.
Trojan Horse	Cavallo di Troia: codice maligno che realizza azioni indesiderate o non note all’utente. I virus fanno parte di questa categoria.

TOR	The Onion Router: sistema di comunicazione anonima in Internet basato sul protocollo onion router e su tecniche di crittografia.
Troll	Utenti di Internet, e in particolare di social net, che pubblicano messaggi provocatori, irritanti o fuori tema.
Troll net	Gruppo organizzato di troll.
Trouble ticketing	Processo e sistema informatico di supporto per la gestione delle richieste e delle segnalazioni da parte degli utenti; tipicamente in uso per help-desk e contact center.
UE	Unione Europea.
UEBA	User and Entity Behavioral Analytics.
UOSI	Unità Organizzativa Sistemi Informativi.
UMTS	Universal Mobile Telephone System.
URL	Uniform Resource Locator: sequenza di carattere che identifica in maniera nome univoca una risorsa ICT in rete; esempio: www.oadweb.it.
Utente finale	Utente di un sistema d'utente e/o di una o più applicazioni con i diritti di accesso relativi al suo ruolo, ma non di tipo privilegiato.
Utente privilegiato	Utenti con diritti d'accesso privilegiati: includono operatori, manutentori ed amministratori di sistema di un sistema informativo, che hanno i più elevati diritti per poter accedere e gestire le risorse ICT del sistema informatico sulle quali debbono operare. Rientrano in questa categoria anche gli sviluppatori di software. Le attuali tendenze di forte terziarizzazione di queste funzioni portano a personale esterno dei fornitori dell'azienda/ente cliente tali diritti, con la necessità di maggiori controlli su di loro per assicurarsi l'adeguate livello di sicurezza digitale.
Vishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato su chiamate telefoniche. E' l'analogo del phishing con la posta elettronica.
VoIP	Voice over IP.
VPN	Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "privata" e sicura per i soli utenti abilitati.
XACML	eXstensible Access Control Markup Language.
XSS	Cross - site scripting: una vulnerabilità di un sito web che consente di inserire a livello "client" dei codici maligni via "script", ad esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
Watering Hole	Famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine, traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona o un'azienda target accede periodicamente.
Wiper	Malware distruttivo che manipola e/o cancella il driver di un hard disk, eliminando tutti i dati archiviati e non consentendo più il suo utilizzo.
Worm	Tipo di virus che non necessita di un file eseguibile per attivarsi e diffondersi, dato che modifica il sistema operativo del sistema attaccato in modo da essere eseguito automaticamente e tentare di replicarsi sfruttando per lo più Internet.
Zero-day	Attacchi basati su vulnerabilità ancora non note e/o a cui non è ancora stato trovato rimedio.
Zero Trust	Modello di sicurezza informatica che elimina la fiducia implicita all'interno di una rete di sistemi ICT.
Zombies, zombi	Si veda bots.