- Adversar - O entitate (inclusiv un insider) care acționează rău intenționat pentru a compromite un sistem.
- Securitate - O condiție care rezultă din stabilirea și menținerea măsurilor de protecție care permit unei organizații/sistem să își îndeplinească misiunea sau funcțiile critice, în ciuda riscurilor reprezentate de amenințări.
- Risc - O măsură a gradului în care o entitate este amenințată de o eventuală circumstanță sau eveniment.
- Vulnerabilitate - Slăbiciune într-un sistem informațional, proceduri de securitate ale sistemului, controale interne sau implementare care ar fi putea fi exploatate sau declanșate de o sursă de amenințare.
- Securitate Cibernetica - Capacitatea de a proteja / apăra spațiul cibernetic de atacuri cibernetice.

- malware - software care este conceput special pentru a perturba, a deteriora sau a obține acces neautorizat la un sistem informatic
- virus - fragment de cod capabil să se copieze singur și să corupă / distrugă date dintr-un sistem, fără permisiunea sau cunoștința utilizatorului
- dropper - un tip de Trojan care a fost proiectat pentru a "instala" malware (virus, backdoor, etc.) pe un computer. Codul malware-ului poate fi conținut în interiorul dropper-ului.
- downloader - un tip de Troian care se instalează pe sistem și așteaptă până când o conexiune la internet devine disponibilă pentru a se conecta la un server sau site web de la distanță în scopul descărcării de programe suplimentare.
- trojan - un tip de cod sau software rău intenționat care pare legitim, dar poate prelua controlul asupra computerului
- spyware - software care permite unui utilizator să obțină informații ascunse despre activitățile computerului altcuiva prin transmiterea secretă a datelor de pe hard disk-ul lor.
- riskware - definește orice programe legitime care prezintă potențiale riscuri datorate vulnerabilităților de securitate, incompatibilității software sau încălcărilor legale.
- ransomware - un tip de software rău intenționat proiectat pentru a bloca accesul la un sistem informatic până când o sumă de bani este plătită.
- adware - software care afișează sau descarcă automat materiale publicitare, precum bannere sau pop-up-uri, atunci când un utilizator este online.
- worm - tip de malware care se răspândește prin copierea de sine de pe un computer pe altul.

- obfuscare - a face ceva dificil de înțeles. Codul de programare este adesea obfuscat pentru a proteja proprietatea intelectuală sau secretele comerciale și pentru a împiedica un atacator să facă reverse engineering unui program software.

- Criptologie - Știința care se ocupă de criptanaliză și criptografie.
- Criptografie - Disciplina care studiază principiile, mijloacele și metodele de transformare a datelor pentru a ascunde conținutul lor semantic, a preveni utilizarea lor neautorizată sau a preveni modificarea lor nedetectată.
- Criptanaliza - Încercarea de a înfrânge protecția criptografice fără o cunoaștere inițială a cheii utilizate în furnizarea protecției.

- Inginerie socială - O încercare de a păcăli pe cineva să dezvăluie informații (de exemplu, o parolă) care pot fi folosite pentru a ataca sisteme sau rețele.
- Phishing - O tehnică pentru încercarea de a achiziționa date sensibile, cum ar fi numerele de cont bancar, printr-o solicitare frauduloasă prin e-mail sau pe un site web, în care făptuitorul se maschează ca o afacere legitimă sau o persoană de încredere.
- Whaling - Un tip specific de phishing care vizează membrii de rang înalt ai organizațiilor.
- Pharming - Utilizarea mijloacelor tehnice pentru a redirecționa utilizatorii către accesarea unui site Web fals, mascat drept unul legitim și divulgarea informațiilor personale.
- Spear phishing - Un termen colocvial care poate fi folosit pentru a descrie orice atac de phishing foarte vizat.
- Spoofing - Falsificarea adresei de trimitere a unei transmisii pentru a obține intrarea ilegală într-un sistem securizat.

- **Confidentialitate**: păstrarea secretului informației, accesul la informația sensibilă fiind disponibilă doar persoanelor autorizate.
- **Integritate** (a datelor): eliminarea posibilității de modificare (schimbare, inserare, stergere) sau distrugere neautorizată a informației.
- **Disponibilitate**: permiterea entitatilor autorizate sa acceseze în timp util si fiabil informatia.
- **Autentificare**: identifica o entitate sau atestă sursa datelor.
- **Non-repudiere**: previne negarea unor evenimente anterioare.