Cyberspace : Le terme "cyberespace" désigne un concept abstrait représentant l'environnement virtuel où se déroulent les activités liées à l'informatique, à l'Internet et aux communications électroniques. Il s'agit d'un espace numérique non physique où les données, les informations, les communications et les interactions électroniques ont lieu.

Attaque ciblée : Dans le contexte de la cybersécurité, une attaque ciblée est une méthode d'attaque informatique soigneusement planifiée et exécutée, visant spécifiquement une personne, une organisation, un système ou un réseau particulier. Contrairement aux attaques génériques ou automatisées qui visent un large éventail de cibles potentielles, une attaque ciblée est conçue pour être précise et adaptée à sa cible.

Livre blanc de la défense : Un "livre blanc de la défense" est un document officiel publié par un gouvernement, détaillant les politiques, orientations et stratégies liées à la défense nationale. Ces documents fournissent souvent des informations sur les menaces perçues, les priorités en matière de sécurité, les capacités militaires, les alliances internationales, et d'autres aspects clés de la politique de défense.

Identité numérique : L'identité numérique englobe toutes les informations permettant de décrire et d'identifier une entité (personne, organisation, appareil, etc.) dans le contexte numérique. Cela inclut les données personnelles, les attributs spécifiques, les interactions en ligne, les activités numériques, et d'autres éléments contribuant à la représentation numérique d'une identité.

Donnée : Le terme "donnée" fait référence à des faits, des informations ou des éléments bruts qui peuvent être collectés et stockés. Les données peuvent prendre différentes formes, notamment des nombres, des textes, des images, des vidéos, des enregistrements audio, etc. Elles sont souvent utilisées comme matière première pour générer des informations significatives et prendre des décisions.

Authentification : L'authentification est le processus de vérification de l'identité d'une entité, telle qu'une personne, un appareil ou un système informatique, afin de garantir l'accès à des ressources, des données ou des services. L'objectif principal de l'authentification est de s'assurer que l'entité prétendant être ce qu'elle prétend être est effectivement légitime. Ce processus implique généralement l'utilisation de facteurs d'authentification, classés en trois catégories principales : facteurs de connaissance, facteurs de possession et facteurs biométriques.

Attaques directes et indirectes : Ces termes décrivent différentes approches ou méthodes d'attaque, que ce soit dans le contexte militaire, informatique, ou d'autres domaines. Les attaques directes se produisent lorsque l'attaquant cible spécifiquement une entité ou un objectif sans utiliser d'intermédiaire, tandis que les attaques indirectes impliquent souvent l'utilisation d'intermédiaires ou de moyens détournés pour atteindre l'objectif final.

Chiffrement symétrique et asymétrique : Ces méthodes de cryptographie sont utilisées pour sécuriser les données en les rendant inintelligibles sans la clé appropriée. Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données, tandis que le chiffrement asymétrique utilise une paire de clés (publique et privée) pour chiffrer et déchiffrer, offrant des avantages tels que l'échange sécurisé de clés sur des canaux non sécurisés.

Cryptographie : La cryptographie est l'art et la science de sécuriser les communications et les informations en les transformant de manière à ce qu'elles soient incompréhensibles pour des personnes non autorisées. Elle repose sur l'utilisation de techniques mathématiques et informatiques pour encrypter (chiffrer) et décrypter (déchiffrer) des données.