

## Cyberguerre

La cyberguerre désigne l'utilisation du numérique comme arme par un État (ou un groupe soutenu ou non par un État) pour : Perturber un pays, l'espionner, affaiblir ses infrastructures ou influencer sa population.

Contrairement à une guerre classique, il n'y a pas de bombes, mais des attaques informatiques.

Dans une cyberattaque visant un pays ou une ville sont but est multiple comme saboter les infrastructures essentielles de celle-ci : l'électricité, l'eau, transports, hôpitaux, télécommunication.

L'espionnage est aussi un des objectifs : vol de données diplomatiques, recherches scientifique, secrets militaires...

Ces attaques conduisent à l'affaiblissement d'un pays, les données collecter donnent un avantage stratégique aux attaquant et permet de plonger les habitants dans la panique, la désinformation, la manipulation.

Une Cyberguerre nécessite de fort dispositifs d'attaques très couteuses et souvent impossible à réaliser sans un Etat allié.

Selon Yimou Lee source Reuters, en 2025 la Chine aurait lancé par jours environ 2.6 millions de cyberattaques par jours contre Taiwan sur des secteurs critiquent telle que l'énergie et les hôpitaux.

Selon les rapports Taiwanais les attaques lancées par la Chine serait des Distributed Denial-of-Service (DDoS) visant à perturber le quotidien des Taiwanais ainsi que des attaques MITM (Man-In-The-Middle) afin de collecter les informations circulant sur les réseaux de télécommunication de l'île.

Dans un monde constamment en évolution vers le numérique les risques de cyberguerre restent un sujet important, données militaires, données personnelles de la populations, ressources essentiels, tous ces éléments tomber entre de mauvaises mains mettrais un pays entier en faiblesse.

Pour lutter contre les attaquant les analystes Forensics ont pour mission d'enquêter après une cyberattaque, analyser les disques, serveurs, logs pour retrouver comment l'attaque a eu lieu et qui en est responsable.

Les analystes SOC eux surveillent les systèmes 24h/24 7j/7, ils d'détecent les attaques et réagissent pour limiter les dégâts.

La Blue team a pour rôle de défendre les systèmes contre les attaques travaillant avec la SOC.

La Red team est constituée de pentester, ils attaquent les systèmes légalement, simule des cyberattaques ennemies et identifie les failles de sécurité.

La Purple team combinant la Blue (défense) et Red (attaque) team améliore la sécurité globale, très utilisé dans les stratégies cyber militaires

Les Threat Intelligence Analyst étudie les groupes de hackers et États adverses, analyse les menaces mondiales, anticipe les futures cyberattaques.

Les cyberguerres sont combattues par des spécialistes comme les analystes SOC, forensics, threat intelligence, red team et blue team, qui surveillent, enquêtent, anticipent et défendent les systèmes numériques.