

RESUME SUR

LE ROLE COMBINE DE L'OSINT, DU COMMUNITY MANAGEMENT, ET DE LA CYBER SÉCURITÉ DANS LA GUERRE INFORMATIONNELLE MODERNE.

INTRODUCTION

La guerre informationnelle moderne encore appelée guerre de L'information, est un type de conflit qui utilise les technologies de l'information et de la communication pour influencer, manipuler, s'approprié ou détruire les systèmes d'information adverse tout en protégeant les siens. Plusieurs techniques telles que l'OSINT du Community Management et de la cybersécurité sont utilisées pour réduire cette guerre informationnelle à sa plus simple expression.

A : L'OSINT

L'Open source intelligence (OSINT) est une technique de recherche de l'information à partir des sources accessibles, l'OSINT permet dans un premier temps de **Détecter les campagnes de désinformation** en analysant les réseaux sociaux et en identifiant les fausses sources d'informations et dans second temps de les **contrés** en retrouvant de vraies informations tout en retraçant les influenceurs à l'origine de fausses informations **Surveillance des réseaux sociaux. Les outils OSINT (Open Source Intelligence) couramment utilisés pour détecter, analyser et suivre les campagnes de désinformation, notamment sur les réseaux sociaux et le web**

- **Hoaxy**
Permet de visualiser la propagation de fausses informations et de comparer leur diffusion avec des sources fiables.
- **TweetDeck**
Suivi en temps réel de mots-clés, hashtags et comptes suspects.
- **CrowdTangle**
Analyse de la diffusion de contenus sur Facebook, Instagram et Reddit (souvent utilisé par journalistes et chercheurs).

B : LE COMMUNITY MANAGEMENT

Le Community management est une technique qui consiste à administrer une communauté en ligne en créant des contenus et en produisant des publicités pour pouvoir avoir une plus grande audience et avoir une plus grande influence publique. Le Community management joue un rôle crucial dans la guerre informationnelle, car il permet de gérer et d'influencer les communautés en ligne pour obtenir des objectifs stratégiques à travers, la création de contenu, la gestion de crise et la surveillance des réseaux sociaux. **Les outils et techniques de Modération & gestion des crises**

Techniques

- Modération proactive (avant que ça dérape)

- Séparer débat / troll / désinformation
- Réponse factuelle + calme
- Ne pas nourrir les provocations
- Documentation des incidents

👉 Outils :

- **CrowdTangle / Tweet Deck** : surveiller les conversations
- **Mod tools natifs** (Facebook, Discord, Reddit)
- **Perspective API** : détection de toxicité
- **Bot de modération (MEE6, Dyno)**

C : LA CYBERSECURITE

La **cybersécurité** est l'ensemble des moyens techniques, humains et organisationnels mis en place pour **protéger les systèmes informatiques, les réseaux et les données** contre les cyberattaques, les intrusions, les vols ou les dommages. La cybersécurité dans le cadre de la guerre informationnelle moderne consiste à protéger les systèmes d'information, les données, les réseaux et les informations contre les attaques cybernétiques et les menaces visant à compromettre la confidentialité, l'intégrité et la disponibilité des informations, elle a pour objectif la protection des informations sensibles et confidentielles contre les accès non autorisés, la prévention des attaques cybernétiques telle que les piratages, les virus, les malwares à travers la mise en place des mécanismes d'authentification et d'autorisation ainsi que l'application des pare-feu pour protéger les systèmes. **Pare-feu nouvelle génération (NGFW)**

- Inspection profonde (DPI)
- Détection d'intrusions (IDS/IPS)

🔧 Outils pare-feu

Open-source

- pfSense
- OPNsense
- Snort / Suricata (IDS/IPS)

D : RÔLE COMBINÉ ET AVANTAGES DE L'OSINT DU COMMUNITY MANAGEMENT ET DE LA CYBERSÉCURITÉ DANS LA GUERRE INFORMATIONNELLE MODERNE

L'OSINT, le Community management et la cybersécurité jouent un rôle complémentaire.

L'OSINT permet de collecter et d'analyser des informations issues de sources ouvertes pour détecter les campagnes de désinformation, comprendre les narratifs dominants et identifier les acteurs malveillants.

Le **Community management** agit ensuite sur le terrain de l'influence en diffusant des messages stratégiques, en gérant les communautés en ligne et en contrant les rumeurs ou manipulations.

La **cybersécurité**, enfin, protège les systèmes, les données et les comptes contre le piratage, les fuites d'informations et les attaques numériques.

E : DÉFIS ET LIMITE DE L'OSINT DE LA CYBERSÉCURITÉ ET DU COMMUNITY MANAGEMENT DANS LA GUERRE INFORMATIONNELLE MODERNE

Dans le cadre de la guerre informationnelle moderne le Community management et l'OSINT font face à de nombreux défis à l'exemple de :

- **Volume de données** : le volume de donnée qui doit être analysé dans le cadre d'une recherche est très souvent énorme ce qui constitue un véritable défi pour les chercheurs
- **Qualité de données** : la qualité de données peut être variable ce qui peut affecter la précision et l'analyse

En ce qui concerne la cybersécurité elle également fait face à d'important défi c'est notamment le cas de :

- **Le manque de ressource** : les organisations peuvent manquer de ressource pour mettre en place des mesures de cybersécurité efficace.
- **La complexité des systèmes** : les systèmes d'informations sont de plus en plus complexes ce qui rend la protection plus difficile.

CONCLUSION

La guerre informationnelle moderne tend nos jours à reposer sur **la maîtrise d'information** que sur **la force militaire**. L'alliance entre la cybersécurité l'OSINT et le Community management est devenu indispensable pour comprendre, influencer et protéger un environnement numérique. Le rôle combiné de ces notions offre plusieurs avantages. Entre autres, on peut noter une meilleure protection des informations et des systèmes d'informations, une meilleure compréhension des cibles et des menaces et une influence accrue sur les communautés en ligne.