Analyse PESTEL

Armée de Terre Française : pôle cybersécurité

I. Le Facteur **P**olitique

Premièrement, l'environnement international est marqué par des conflits comme en Ukraine, ce type de conflit a transformé la **cyberguerre** en une réalité quotidienne. Ce qui nécessite donc un renforcement continu des défenses.

Ensuite, la **Loi de Programmation Militaire (LPM)** est la concrétisation des choix politiques : elle garantit le budget et les moyens humains alloués au **COMCYBER** (Commandement de la cyberdéfense) pour assurer la souveraineté numérique.

- **Opportunité (Politique) :** La LPM assure un **investissement massif et pérenne** (plusieurs milliards d'euros) dans le domaine cyber, garantissant des postes et des projets d'avenir.
- **Menace (Politique) :** L'instabilité géopolitique persistante signifie que le **niveau de menace est en hausse constante** et ne permet aucun relâchement dans les défenses informatiques.

II. Le Facteur **É**conomique

Sur le plan Économique, la cybersécurité militaire est soumise à deux contraintes majeures.

D'une part, le coût des systèmes de pointe est très élevé, faisant de l'Armée un acteur économique qui investit dans les solutions nationales.

D’autre part, une cyberattaque réussie représente un **risque financier immense**, au-delà de la simple perte de données. Puisque, comme dit précédemment, les infrastructures et systèmes sont onéreux.

- **Menace (Économique) :** La **compétition féroce pour les talents** avec le secteur privé fait monter les salaires, ce qui représente un coût élevé pour l'Armée et rend difficile la rétention des experts.
- **Opportunité (Économique) :** L'Armée peut jouer un rôle de **locomotive économique** en soutenant les **PME/start-ups françaises** de la cybersécurité, favorisant ainsi l'innovation souveraine.

III. Le Facteur **S**ocio-culturel

Abordons la dimension humaine et sociale. Le facteur Socio-culturel est un atout de différenciation.

L'**image de l'Armée** doit être moderne et experte pour attirer entre guillemets les citoyens Français. Elle mise sur la **mission** et le **service public**.

Les informaticiens militaires eux, sont soumis à une **éthique forte** et à des règles strictes de **secret défense**. Ces valeurs sont un filtre pour le recrutement et un pilier de la confiance au sein de l'organisation. De plus, la **formation continue** est un enjeu permanent pour maintenir les compétences à jour.

- **Opportunité (Socio-culturel) :** L'**attractivité unique de la mission** (défendre la Nation) permet d'attirer des profils que le secteur privé ne peut pas séduire, garantissant un personnel très motivé.
- **Menace (Socio-culturel) :** La **méconnaissance** par le public des métiers de la cyberdéfense peut freiner le recrutement si l'image n'est pas suffisamment moderne et technologique.

IV. Le Facteur **T**echnologique

Passons au point Technologique qui est au cœur de l'innovation et des menaces. Sur ce plan, on parle d’une course permanente.

La **Course à l'armement** signifie que les défenses doivent évoluer au même rythme que les outils offensifs, notamment avec l'émergence de l'**Intelligence Artificielle** et la future **menace quantique**.

Pour rester au niveau, l'Armée est obligée d'intégrer des innovations civiles comme les Cloud (stockées sur des serveurs situés hors site), mais elle doit le faire en assurant une sécurité maximale, en s'appuyant sur la **R&D** (partir d’une recherche et assurer sa faisabilité) via l'AID.

- **Opportunité (Technologique) :** L'Armée, grâce à sa R&D (AID), peut devenir **pionnière** dans le développement d'outils de **cyberdéfense souveraine** que le secteur civil pourra ensuite utiliser.
- **Menace (Technologique) :** Le risque de **dette technique** est élevé ; la rigidité et l'ampleur des systèmes militaires rendent l'intégration rapide des nouvelles technologies difficile et coûteuse.

V. Le Facteur **É**cologique (Environnemental)

Parlons d’un facteur moins évident mais de plus en plus pertinent, le point Écologique (Environnemental).

Premièrement, par l'**Impact Numérique** : l'Armée est attentive à la **consommation énergétique** de ses grands systèmes d'information, s'alignant sur le **Green IT** (une démarche d'amélioration qui vise à réduire les impacts sur l'environnement, sociaux et économiques du numérique).

Deuxièmement, les capacités cyber sont de plus en plus intégrées à la **gestion de crises** (comme les catastrophes naturelles) qui ont un impact environnemental direct.

- **Opportunité (Écologique) :** L'alignement sur le **Green IT** permet d'améliorer l'image de l'Armée et d'optimiser les coûts opérationnels à long terme (meilleure gestion de l'énergie).
- **Menace (Écologique) :** L'importance croissante des préoccupations environnementales pourrait générer une **pression publique** sur les activités militaires dont l'empreinte carbone est historiquement élevée.

VI. Le Facteur Légal

Enfin, le dernier pilier, celui du Légal. Le facteur Légal impose un cadre très strict.

Tout est régi par un **cadre réglementaire strict** lié à la défense nationale et à la protection du secret. Les systèmes sont classés comme **SIIV** (Systèmes d'Information d'Importance Vitale).

L'Armée doit également prendre en compte le droit européen, notamment la **directive NIS 2** (directive qui vise à renforcer la sécurité informatique dans l’UE), cette directive impacte l'ensemble de ses fournisseurs et partenaires critiques.

L'ensemble des activités, y compris le renseignement, est très fermement encadré par la loi pour garantir la sécurité de l'État dans le respect du droit.

- **Opportunité (Légal) :** L'existence d'un **cadre juridique clair** pour la cyberdéfense (LPM, lois sur le renseignement) sécurise les opérations et donne une **légitimité** forte aux actions menées.
- **Menace (Légal) :** La nécessité d'homologuer les systèmes selon des **normes de sécurité très strictes** (Secret Défense, SIIV) peut entraîner des **délais d'intégration longs** et une complexité administrative importante.

SOURCES :

https://fr.wikipedia.org/wiki/Arm%C3%A9e_de_terre_(France)

https://www.defense.gouv.fr/terre

https://www.sgdsn.gouv.fr/nos-missions/proteger/assurer-la-cybersecurite-et-coordonner-la-cyberdefense

https://www.welcometothejungle.com/fr/companies/commandement-de-la-cyberdefense-comcyber/missions-2

https://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-defensive-lid