| Note / 20 | Correcteur |
|---|---|
| | |

Épreuve de Synthèse de dossier

| N° d'anonymat (4) |
|---|
| 5725 |

Feuille n° 1 / 2 (5)

Ministère des Armées

Direction générale du numérique et des systèmes d'information et de communication (DGNUM)

Rédacteur : Commissaire XX Paris, le YY

NOTE à l'attention du directeur général de la DGNUM

Objet : Avancées nationales et perspectives pour le ministère des Armées en matière de cybersouveraineté

Michel Paulin, directeur général d'OVH cloud, exprimait en 2020 sa crainte que la France ne devienne « une colonie numérique de la Chine ou des États-Unis », mettant en évidence les faiblesses françaises et européennes en matière de cybersouveraineté.

La cybersouveraineté se traduit par la capacité d'un pays à réguler l'usage des outils numériques sur son territoire, ainsi que la gestion des données qui y sont générées. La France et l'Union européenne accusent, cependant, un retard considérable en matière numérique, les rendant vulnérables et dépendantes vis-à-vis de puissances étrangères. Pour pouvoir assurer la cybersouveraineté de la France, le ministère des Armées devra pouvoir s'appuyer sur des outils numériques et des infrastructures nationales et indépendantes de toute ingérence contraire aux intérêts de la Nation.

La présente note reviendra sur les menaces posées par l'absence de cybersouveraineté (I), les avancées

(1) Indiquer la nature du concours.
(2) Précisez le niveau : CME - CM1 - CM2 - CTE - CT1 - CT2 - CT1/VE - CAT2 - BSAT - BSTAT.
(3) Pour les examens de langues, préciser : active, réserve, service détaché.
(4) Ne rien inscrire dans cette case.
(5) Le candidat porte au numérateur le numéro d'ordre de la feuille et au dénominateur le nombre total de documents constituants sa composition (ex. : 1/3 puis 2/3 et 3/3).

ÉDIACA SAINT-ÉTIENNE - 2013060041
SGA/SPAC/PGT Impressions

nationale et européenne sur la question (II) et sur les besoins et recommandations du ministère des Armées pour atteindre cet objectif (III).

## I. Menaces d'un manque de cybersouveraineté

La domination du monde numérique par la Chine et les Etats-Unis rend la France dépendante et vulnérable vis-à-vis d'acteurs privés et/ou étrangers et diminue sa capacité à assumer sa puissance régalienne.

• Le secteur du stockage de données est dominé par des entreprises américaines (Amazon, Microsoft, Google) et chinoises (Alibaba, Tencent). La première entreprise européenne sur le secteur, OVHcloud, représente moins d'1% du marché mondial, 11% en France. Seul un centre de données sur cinq est localisé en Europe, contre plus d'un tiers aux Etats-Unis. La France ne gère elle-même que très peu de ses propres données, qui sont en grande partie stockées à l'étranger, vulnérables à des utilisations malveillantes par leurs dépositaires.

• L'Etat est concurrencé dans ses fonctions régaliennes : sur le secteur monétaire (cryptomonnaies), celui de l'identification (Facebook Connect), voire celui de la violence légitime (ripostes à des attaques numériques coordonnées par des acteurs privés). Ceci fait courir le risque d'une perte de contrôle par l'Etat du secteur numérique et d'une prédominance du secteur privé sur des missions régaliennes.

• L'offre française et européenne pour remplacer ces outils étrangers est très lacunaire. L'Assurance Maladie doit ainsi utiliser les services de Microsoft pour les données patient, et EDF envisage, par praticité, d'y héberger ses espaces coopératifs. Le manque d'alternatives privées à placer des données sensibles pour la sécurité

nationale entre les mains d'entreprises étrangères, ouvrant la possibilité de leur usage à but lucratif ou malveillant.

## II. Avancées françaises en matière de cyber souveraineté

La France souffre d'un grand retard matériel. Elle poursuit toutefois une stratégie de résilience et émancipation, pouvant s'appuyer sur ses partenaires européens.

• Pour répondre à l'initiative sur la cybersécurité, les moyens de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ont été augmentés, notamment en matière de surveillance des flux et attaques informatiques, l'évaluation des outils numériques susceptibles d'être utilisés par l'administration, et le développement des capacités de cyberdéfense des données hébergées sur le territoire.

• Pour un meilleur hébergement des données, le développement d'infrastructures nationales et européennes a été lancé. Ce processus comprend notamment la création d'un cloud franco-allemand, Gaia-X, porté par le français OVH cloud et l'allemand T. Systems. Thierry Breton, commissaire européen, a annoncé un investissement de 2 milliards d'euros pour son développement en « sphère publique européenne », sous le nom de Gaia-EU.

• Pour encourager le développement de solutions nationales de cybersécurité, des filières collaboratives, telles que GALLIA, ont été lancées pour favoriser la création d'une filière française de cybersécurité. Celle-ci viennent s'ajouter à un plan de financement de près de 1,2 milliard d'euros projeté par le Gouvernement, visant à investir dans les entreprises numériques françaises novatrices et empêcher leur rachat par des intérêts étrangers.

## III. Perspectives et enjeux pour le ministère des Armées

Pour remplir les objectifs de cyber souveraineté, le ministère des Armées a lancé en 2017 une démarche de transformation numérique, sous l'égide de la DGNUM, afin d'atteindre une supériorité opérationnelle en matière de cybersécurité.

- Pour pouvoir acquérir des outils numériques souverains, l'initiative Défense Connect du ministère, visant à développer et promouvoir les initiatives fournissant ces outils de transformation numérique, doit être renforcée. Son action d'attractivité vis-à-vis des acteurs nationaux du numérique doit être poursuivie, et les entreprises y participant défendues contre une prise de contrôle étrangère de leurs capitaux, à l'image de la nationalisation de l'entreprise d'analyse de données Palantir vis-à-vis d'un fonds d'investissements gouvernemental américain.
- Le ministère doit pouvoir également se doter de structures de stockage de données sûres, efficaces et souveraines. Ceci doit passer par la création d'infrastructures de type "cloud" confiées à des prestataires de confiance, ayant à cœur l'autonomie stratégique de la Nation.
- Enfin, le ministère doit accélérer la formation de ses agents à la transformation numérique, afin que celle-ci passe du statut de projet à celui d'outil opérationnel. Dans ce cadre, des outils d'acculturation tels que le Passeport numérique ou le réseau Combattantes@Numériques doivent être étendus et intégrés à la formation initiale et continue des personnels de Défense.

La cyber souveraineté est un enjeu crucial pour

| Note / 20 | Correcteur |
| --- | --- |
| | |

Épreuve de Synthèse de dossier

| N° d'anonymat (4) |
| --- |
| 5725 |

Feuille n° 2 / 2 (5)

la France, afin d'assurer son indépendance et sa résilience vis-à-vis d'acteurs étrangers et privés, et de faire de la transition numérique un atout pour la Nation et sa sécurité.

L'impératif de souveraineté s'inscrit dans un processus général de résilience dépassant le seul ministère des Armées, qui a pour objectif de pallier aux problèmes d'interdépendance excessive tels que mis en évidence par la crise du Covid-19. La France doit trouver dans l'autonomie un nouvel atout de réponse aux crises.

900 mots

(1) Indiquer la nature du concours.
(2) Précisez le niveau : CME - CM1 - CM2 - CTE - CT1 - CT2 - CT1/VE - CAT2 - BSAT - BSTAT.
(3) Pour les examens de langues, préciser : active, réserve, service détaché.
(4) Ne rien inscrire dans cette case.
(5) Le candidat porte au numérateur le numéro d'ordre de la feuille et au dénominateur le nombre total de documents constituants sa composition (ex. : 1/3 puis 2/3 et 3/3).

ÉDIACA SAINT-ÉTIENNE - 2013060041
SGA/SPAC/PGT Impressions

35

40

45

50

55

60

65