Note / 20	Correcteur

Épreuve de Note de Synthèse

N° d'anonymat (4)
5335

Feuille n° 1 / 1 (5)

Nombre de mots : 959.

Ministère des armées — Le 3 mars 2021

DGNUM

Note à l'attention du directeur général du numérique et des systèmes d'information et de communication

OBJET : La stratégie du ministère des armées pour la cybersouveraineté de la France.

Annexe 1 : Propositions d'actions 2021-2026.

La souveraineté nationale repose de nos jours sur la souveraineté numérique. L'État a par conséquent le devoir de contrôler la manière dont Internet est utilisé au sein de ses frontières et de gérer les données qui en résultent. Par là, il s'agit d'une nouvelle prérogative régalienne mettant en jeu des questions éthiques, sécuritaires et d'indépendance. Néanmoins, la France ne dispose pas encore de cette cybersouveraineté, comme en témoignent les risques de cyberattaques dont elle fait régulièrement l'objet et sa dépendance aux technologies étrangères, en particulier pour la collecte des données. Dans ce contexte, le ministère des armées a développé une stratégie pour développer sa cybersouveraineté, notamment en lançant sa transition numérique (TN) grâce au DGNUM qui a conduit la restructuration de son système d'information (SI) depuis 2018.

Dès lors, comment le ministère des armées contribuera-t-il à la cybersouveraineté de la France ?

Cette présente note établit donc le bilan des avancées en matière de souveraineté numérique (I) et la stratégie mise en place pour lutter contre la dépendance technologique de l'État (II). Enfin, des propositions concrètes seront formulées pour le ministère des armées (Annexe 1).

(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).

EDIACA SAINT-ÉTIENNE - 2013060041

SGA/SPAC/PGT Impressions

I- Le bilan des avancées en matière de souveraineté numérique.

A. Une transition numérique (TN) récente...

Depuis le Livre Blanc de 2008 le rôle des armées dans la cyberdéfense s'avère majeur. Le développement de son système d'information (SI) permet ainsi la modernisation des métiers mais aussi l'exploitation de données, dans une démarche de « numérisation des champs de bataille ». La TN des armées permet ainsi de protéger la France des attaques virtuelles de ses potentiels ennemis : grâce à l'Unité de management cyber numérique (UM SNUM), travaillant avec la DGA et la DIRISI, le ministère des armées est passé à une « logique produit/service » afin de mettre en œuvre des outils répondant aux besoins.

B. ... afin d'être en permanence dans la course à la supériorité opérationnelle.

La France connaît un retard technologique important en ce qui concerne la protection de ses données puisque de facto elle doit recourir à des hébergeurs étrangers, principalement américains (GAFAM). Malgré tout, le ministère des armées a mis en fonctionnement son propre réseau interne, reposant notamment sur 220 000 machines, et dispose de son propre système de communication afin de garantir son indépendance. En outre, grâce à l'ANSSI, une doctrine de décourager et de répondre dans le cyberespace guide aujourd'hui l'action de l'État face aux menaces virtuelles. De même, un fonds de souveraineté, géré par la BPI France et s'élevant à 500 millions d'euros en 2021, a été créé afin de protéger les start-up françaises, développant des technologies de pointe, des rachats étrangers.

II- La stratégie pour lutter contre la dépendance technologique de l'État.

A. Face à la fuite des données personnelles...

En 2019, le Sénat défend l'idée d'une loi d'orientation et de

suivi de la souveraineté numérique (LOSSN) afin d'inscrire la souveraineté numérique dans la durée, rendant possible la protection des données personnelles. De fait, cette protection est à ce jour quasi-inexistante et, pour se réaliser, nécessiterait une interopérabilité entre les entreprises et l'État. De même, l'Union européenne (UE) a un rôle majeur à jouer, en particulier en développant la coopération entre États membres. Le « cloud » franco-allemand Gaia-X, issu de la fusion des entreprises OVH cloud pour la France (1% du marché mondial) et de T-systems pour l'Allemagne, est une initiative allant en ce sens mais encore trop timide.

B. — La nécessité de développer une véritable coordination

Face à un marché de la donnée qui s'élèvera à 82,5 milliards d'euros en 2025, il s'avère primordial pour l'État d'opérer une « nationalisation de ses données » afin de les protéger de l'étranger. Aussi, il est du ressort du ministère des armées de participer à cette dynamique ; son fonds, « Def Invest » participe déjà à conserver nos pépites françaises. Les entreprises analysant des données. La start-up Preligens, qui s'appuie sur des images collectées par satellite grâce à l'intelligence artificielle (IA) et au « machine learning » a ainsi été achetée pour partie par ce fonds. De même la plateforme Gallia permet à l'État de fédérer tous les acteurs de la cybersécurité et d'organiser leur coordination. Enfin, les forums, tels le Forum international de la cybersécurité (FIC) ou le Forum national du numérique (FNH), permettent de donner l'impulsion nécessaire à l'éclosion de ces projets.

Conclusion : Le défi pour le ministère des armées consiste aujourd'hui à protéger ses données, véritables clés de voûte de la cybersouveraineté. Ses initiatives, permises par sa TIV, sont désormais bien lancées et méritent désormais d'être consolidées. De l'indépendance technologique des armées dépend en effet la souveraineté de la France.

Annexe 1 : Propositions d'actions 2021-2026.

• Proposition 1 : Encourager les démarches de rachats de start-up françaises, notamment via le fonds DefInvest, permettrait de préserver les talents français des convoitises étrangères et créerait les bonnes conditions de leur développement, au service de la France.

• Proposition 2 : Investir dans la formation et le recrutement des spécialistes de la cybersécurité. L'objectif de 1500 postes supplémentaires d'ici 2025 par la Loi de Programmation militaire (LPM) 2019-2025 doit ainsi être tenu et maintenu pour la prochaine LPM. Pour ce faire, les salaires devraient être augmentés afin que le ministère des armées soit compétitif vis-à-vis du secteur privé.

• Proposition 3 : Créer un Hébergeur de données national de grande ampleur. Le cloud Gaia-X pourrait ainsi servir de point de départ pour créer une plateforme capable de rivaliser avec celles des GAFAM et ainsi permettre l'indépendance de la France en matière de cybersécurité.