Intitulé de l'épreuve : Note de synthèse

Nombre de copies : 2

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Sujet : Point de situation sur la souveraineté numérique et ses possibles mises en oeuvre au sein du ministère.

Le conflit en Ukraine depuis 2022 et la recrudescence d'actes cybers ces dernières années contre des structures publiques (hôpitaux, aéroports...) illustrent l'importance de stratégies hybrides visant l'espace cyber, avec comme enjeu clé pour la France sa souveraineté numérique.

Le concept de souveraineté numérique peut se définir comme la capacité des Etats à agir dans le cyberespace et à faire respecter leurs règles par les différents acteurs du monde virtuel. Elle implique ainsi une maîtrise par l'Etat des technologies numériques et du droit qui leur est applicable. Dans ce domaine, l'Union européenne (UE) apparaît en retard, alors que 80 % des infrastructures et technologies numériques utilisées en Europe sont importées, mais agit pour faire émerger une souveraineté numérique (IA Act, RGPD). Au niveau français, plusieurs initiatives sont en cours en faveur de la souveraineté numérique.

Dans ce contexte, cette note vise à faire un point de situation sur la souveraineté numérique et ses possibles mises en oeuvre au sein du ministère de l'Europe et des Affaires Etrangères, en matière de maîtrise des matériels (I) des logiciels (II) et des données sensibles (III).

I Sous

N° 1 / 2.

I. Souveraineté numérique et maîtrise des matériels

Au niveau du matériel informatique, l'UE et la France reposent sur des équipements étrangers alors que peu d'industries sont présentes en Europe, que ce soit dans les semi-conducteurs, les équipements réseaux ou les composants électroniques.

Si le droit européen ne prévoit pas de règles spécifiques concernant le matériel informatiques, l'Etat s'assure au niveau français que le matériel utilisé soit fiable et sans risque sécuritaire. Ainsi, l'Agence nationale de sécurité des systèmes d'information (Anssi), créée en 2009, prévoit des exigences spécifiques en matière de marchés publics, tandis que leur mutualisation au niveau interministériel facilite ce contrôle.

En parallèle, la résilience des communications intergouvernementales est assurée par le réseau interministériel de l'Etat (RIE) créé en 2015 et s'appuie sur des fibres optiques sous-marines dont la protection a été renforcée depuis le début de la guerre en Ukraine. Pour prévenir les risques en cas de défaillance, la Direction interministérielle du numérique (Dinum) ~~développe~~ prépare de son côté un plan de continuité (PCA) et de reprise d'activité (PRA).

Au niveau du ministère, si l'infrastructure est connectée à celle des RIE et respecte des spécificités particulières, le développement d'une capacité de connexion satellitaire s'appuyant par exemple sur Eutelsat, en attendant le déploiement du projet européen IRIS², permettrait de renforcer la résilience numérique au niveau matériel (notamment pour les emprises du ministère à l'étranger).

> Piste n°1 : Etudier le développement d'une capacité de connexion satellitaire souveraine pour améliorer la résilience du réseau du ministère.

Au niveau français et européen, le renforcement de la sécurité des approvisionnement en matières premières et composants clés est une piste majeure pour renforcer la souveraineté numérique concernant le matériel, via par exemple du recyclage ou la constitution de stocks

stratégiques.

II. Souveraineté numérique et maîtrise des logiciels

Concernant les logiciels informatiques, le droit européen ne prévoit pas de règles spécifiques et les contraintes de concurrence peuvent entraver la sélection des logiciels utilisés. La maîtrise des logiciels suppose de différencier leur développement de leur hébergement, qui est lié aux questions de données et de cloud.

Au niveau français, deux modèles existent : certaines administrations développent leurs applications métier en interne et l'héberge également sur des structures de l'État, assurant la souveraineté en la matière. D'autres recourent à des logiciels de marché, avec un risque de dépendance vis-à-vis des éditeurs de logiciels. En particulier, ces éditeurs peuvent décider de passer de logiciels installés sur les postes personnels à des logiciels hébergés dans le cloud, comme pour la suite Microsoft Office. Dans ce cas, les administrations concernées sont confrontées à des risques en matière de souveraineté.

Enfin, certains logiciels sont développés pour un usage interministériel par la Dinum, en s'appuyant sur des projets open source et en intégrant des règles strictes en matière de souveraineté. C'est notamment le cas d'une suite bureautique (La Suite), de la messagerie Tchap ou du projet d'identité numérique France Connect, renforcée au niveau de sa sécurité par l'outil France Connect +.

Pour le ministère, des pistes de renforcement de la souveraineté numérique seraient alors d'adopter ces outils interministériels. Si Tchap est déjà préconisé, sa coexistence avec l'usage par les agents d'autres messageries diminue son utilité. En parallèle, l'adoption de La Suite permettrait de bénéficier d'une suite bureautique souveraine en s'appuyant sur l'expertise et le support de la Dinum.

Piste n° 2 : Renforcer l'usage de Tchap comme messagerie interne par les agents du ministère.

Piste n° 3 : Evaluer et préparer l'adoption de La Suite comme suite bureautique du ministère

III. Souveraineté numérique et maîtrise des données

Le domaine de la maîtrise des données est celui où la France et l'UE sont les plus actives, notamment en matière de réglementation. Outre le cadre global posé par le règlement général sur la protection des données (RGPD), l'UE a adopté en 2024 le règlement sur l'IA, qui classifie les risques des systèmes d'IA et les exigences associées, et prévoit l'adoption d'un règlement sur le cloud. ~~Au niveau~~

Au niveau français, la création d'une certification SecNumCloud par l'Anssi, régulièrement réévaluée, permet de définir un cadre pour le niveau de sécurité attendue pour qu'un service cloud soit adapté aux usages sensibles de l'Etat et des entreprises françaises. L'usage de tels services cloud, appelés "cloud de confiance", est encouragé par la doctrine de "Cloud au centre" définie par le Premier ministre.

Par ailleurs, tout la France que des entreprises européennes du numérique, regroupée au sein de l'European Sovereign Tech Industry Alliance (ESTIA), souhaitent l'adoption par la Commission européenne d'une définition juridique de ce qu'est un ~~cloud~~ "cloud souverain" dans le futur règlement cloud. Une définition claire, garantissant la localisation des données hébergées dans l'UE et une protection contre les lois extraterritoriales, serait à même de renforcer la souveraineté numérique de l'UE en matière de données.

Enfin, la France promeut l'intégration de la certification ~~de~~ SecNumCloud dans le schéma de certification des fournisseurs de services de cloud (EUCS4) européen, sans succès pour le moment. En parallèle de SecNumCloud, une certification "Hébergeur de données de santé" spécifique a été élaborée par l'Anssi.

D'un point de vue opérationnel, l'Etat peut s'appuyer sur les clouds certifiés pour assurer la souveraineté numérique en matière de données. En effet, SecNumCloud apporte des garanties de cybersécurité, un hébergement des données en Europe, contrôlé par un prestataire européen et avec une autonomie suffisante vis-à-vis de sous-traitants non-européen (protection contre le kill switch). Ces règles permettent une protection contre les lois extraterritoriales. Toutefois, certaines données considérées comme "non-sensibles" par des administrations françaises sont hébergés sur des clouds non-certifiés, avec un risque en matière de souveraineté.

N° 4.1.B

Intitulé de l'épreuve : Note de synthèse

Nombre de copies : 2

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

En outre, certains ministères ont développé leur propre solution cloud en interne, comme le ministère des finances (cloud Nubo) ou de l'Intérieur (cloud Pi). Au niveau du MEAE, deux data centers propres au ministères assurent également une souveraineté numérique sur les données et services qui y sont stockés. C'est notamment le cas d'une solution IA interne, Diplo IA.

Pour gagner en souveraineté, le ministère pourrait renforcer les moyens de son cloud interne, voire le mutualiser ~~avec d'au~~ ou le fusionner avec ceux d'autres ministères pour gagner en efficacité et réduire les coûts liés. Enfin, le ministère devrait recenser les données qu'il utilise et leur lieu d'hébergement afin de s'assurer d'un niveau de protection adéquat.

Piste 4 : Renforcer le cloud interne du ministère

Piste 5 : Cartographier les données utilisées par le ministère et leur lieu d'hébergement

Piste 6 : Etudier la mutualisation des clouds ministériels

N° 5 16

N°

6.1.6

N°

N°

8 I.8