ENS DE LYON MINES PARIS | PSL

L’opportunité d’intégration des outils d’IA générative au SGDSN

Antoine Sérandour

SGDSN

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

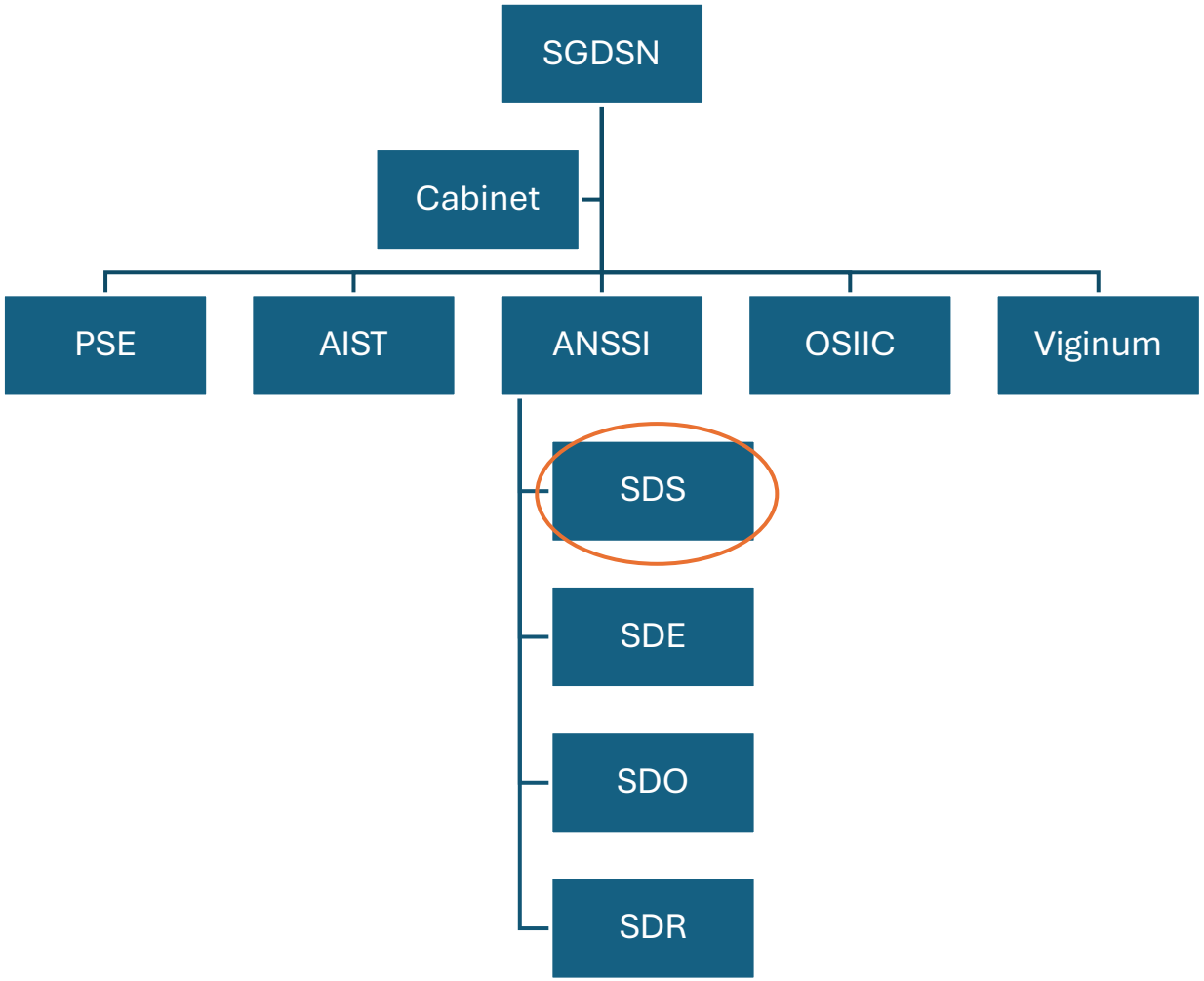
Ce dont on va parler !

Présentation du contexte de l'IA et du SGDSN

Conceptions de l'IA générative chez les agents du SGDSN

Questions posées par ces outils et l'organisations des agents

Le SGDSN aux missions de sécurisation

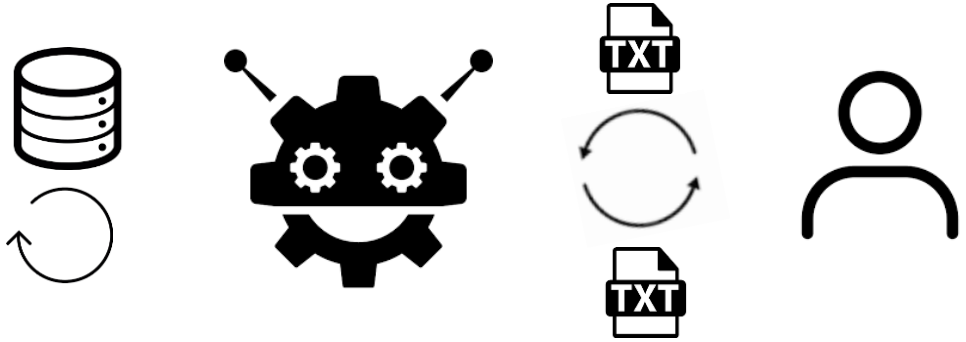


Secrétariat Général de la Défense et de la Sécurité Nationale

- Cybersécurité
- Protection du Secret
- Manipulation de l'information
- Exportation de matériel de guerre
- Gestion des communications du Président
- Secrétariat du Conseil de défense
- …

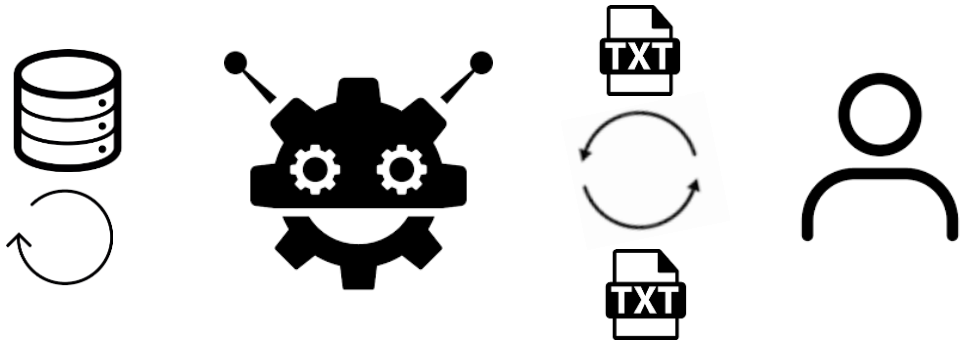
Contexte de l’IA au SGDSN

Fonctionnement d’une IA générative (IAG)



Contexte de l’IA au SGDSN

Fonctionnement d’une IA générative (IAG)



L’IAG au SGDSN

Premiers travaux sur l’IAG	Création du Groupe de Travail IA	Mise à jour de la charte des usages	Entrée en vigueur du RIA	Mise en place de Chap Albert	AI Action Summit
Nov 2022	Nov 2023	Avr 2024	Aout 2024	Sept 2024	Fev 2025

Augmentation des sollicitations

Pas d’expertise structurée

} Comment piloter les projets d’outillage ?

Projets d’outillage au SGDSN

Questions et décisions

- Choix de technologie en cohérence avec les objectifs
- Intégration dans les **outils professionnels**
- Hébergement de la puissance **d’inférence**
- Réalisation **d’entraînements**
- **Expertise interne ou partenariat** public/privé
- **Pluralité** d’outils
- **Promotion et encadrement** (formation, appareil légal)
- …

Contexte de l'étude

Comment **piloter** les projets d'**outillage** d'une administration avec une **diversité de directions** et **sans expertise structurée** ?

Méthode

- 15 entretiens avec des agents de toutes les directions, dont 7 ANSSI
- 7 réunions d'information
- 3 mois d'observation
- Article scientifique pour les Mines et note de synthèse pour le SGDSN

Partir des enquêtés pour qualifier leurs conceptions de l'IAG et les confronter au pilotage des projets d'outillage par les observations

Deux conceptions de l’IA...

Le cas d’usage, une conception de l’IAG

Cas d’usage : une **tâche élémentaire**, réalisable par un **agent** et **contextualisée** dans un environnement professionnel, avec un **référentiel d’évaluation** de la qualité de la tâche

Rédaction de comptes rendus ou notes

Production d’éléments de langage

Traduction

Génération de courriers administratifs

Rédaction de code

Gestion du niveau de classification

Propriétés :

- Utilisation plurielle, segmentée et sélective de l’IAG
- Adapter la technologie à l’administration
- Boîte noire qui dissimule les enjeux techniques et politiques

Autre conception : le levier technologique

Les projets d'outillage organisent :

- De l'expertise
- De ressources informatiques
- Des financements
- Des agents
- Des partenariats

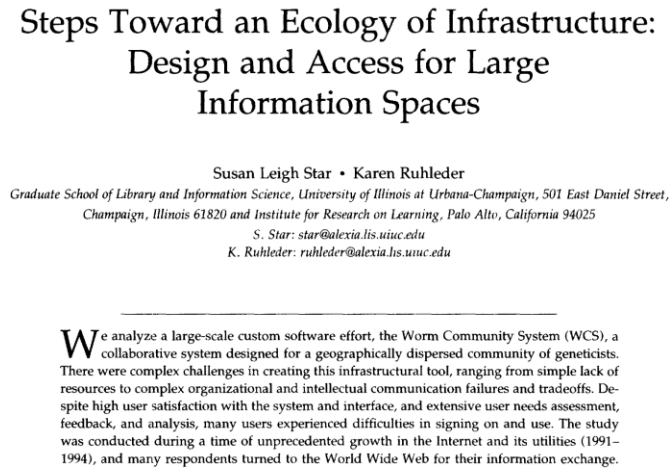
→ Opportunités pour les bénéfices de l'IAG et au-delà

Propriétés :

- Parier sur les gains au-delà de l'utilisation
- Adapter l'administration à la technologie
- Infrastructure globale aux contours flous

Le levier et la dimension infrastructurelle

Dimensions des infrastructures	Exemple pour l'IAG
Embeddedness	Systèmes d'information, budget
Transparency	Conception en boite noire
Reach or scope	Multiples accès
Learned as part of membership	Accès restreint à la fonction publique, aux personnes habilitées
Links of convention of practice	Entrainement pour des productions administratives
Embodiment of standards	Respect des contraintes de sécurité
Built on an installed base	SI existant, intégration dans des logiciels
Becomes visible upon breakdown	*Pas encore lancé*



Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces

Susan Leigh Star • Karen Ruhleder
Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign, 501 East Daniel Street, Champaign, Illinois 61820 and Institute for Research on Learning, Palo Alto, California 94025
S. Star: star@alexia.lis.uiuc.edu
K. Ruhleder: ruhleder@alexia.lis.uiuc.edu

We analyze a large-scale custom software effort, the Worm Community System (WCS), a collaborative system designed for a geographically dispersed community of geneticists. There were complex challenges in creating this infrastructural tool, ranging from simple lack of resources to complex organizational and intellectual communication failures and tradeoffs. Despite high user satisfaction with the system and interface, and extensive user needs assessment, feedback, and analysis, many users experienced difficulties in signing on and use. The study was conducted during a time of unprecedented growth in the Internet and its utilities (1991–1994), and many respondents turned to the World Wide Web for their information exchange.

Deux conceptions de l'IAG

Cas d'usage :
opportunités pour les utilisations de l'IAG

Propriétés :

- Utilisation plurielle, segmentée et sélective
- Adapter la technologie à l'administration
- Boîte noire qui dissimule les enjeux techniques et politiques

Levier technologique :
opportunités pour les bénéfices infrastructurels de l'IAG

Propriétés :

- Parier sur les gains au-delà de l'utilisation
- Adapter l'administration à la technologie
- Infrastructure globale aux contours flous

Comment ces conceptions influencent les questions posées par l'IAG ?

Deux conceptions de l’IA…

… Qui orientent les questionnements

Les questionnements

Qualité des productions :
Les gains attendus de l'IAG permettent-ils de satisfaire le cahier des charges du SGDSN ?

Coût matériel de l'IAG :
Les capacités financières de l'administration sont-elles suffisantes pour outiller le SGSN ?

Evolution des compétences:
Quels effets long terme sur l'administration peut-on attendre de l'utilisation étendue d'outils d'IAG ?

Sécurité de l'utilisation de l'IAG :
L'implémentation et l'utilisation d'IAG peuvent-elles garantir la sécurité des activités sensible du SGDSN ?

…

Les questionnements

Qualité des productions :
Les gains attendus de l'IAG permettent-ils de satisfaire le cahier des charges du SGDSN ?

Coût matériel de l'IAG :
Les capacités financières de l'administration sont-elles suffisantes pour outiller le SGSN ?

Evolution des compétences:
Quels effets long terme sur l'administration peut-on attendre de l'utilisation étendue d'outils d'IAG ?

Sécurité de l'utilisation de l'IAG :
L'implémentation et l'utilisation d'IAG peuvent-elles garantir la sécurité des activités sensible du SGDSN ?

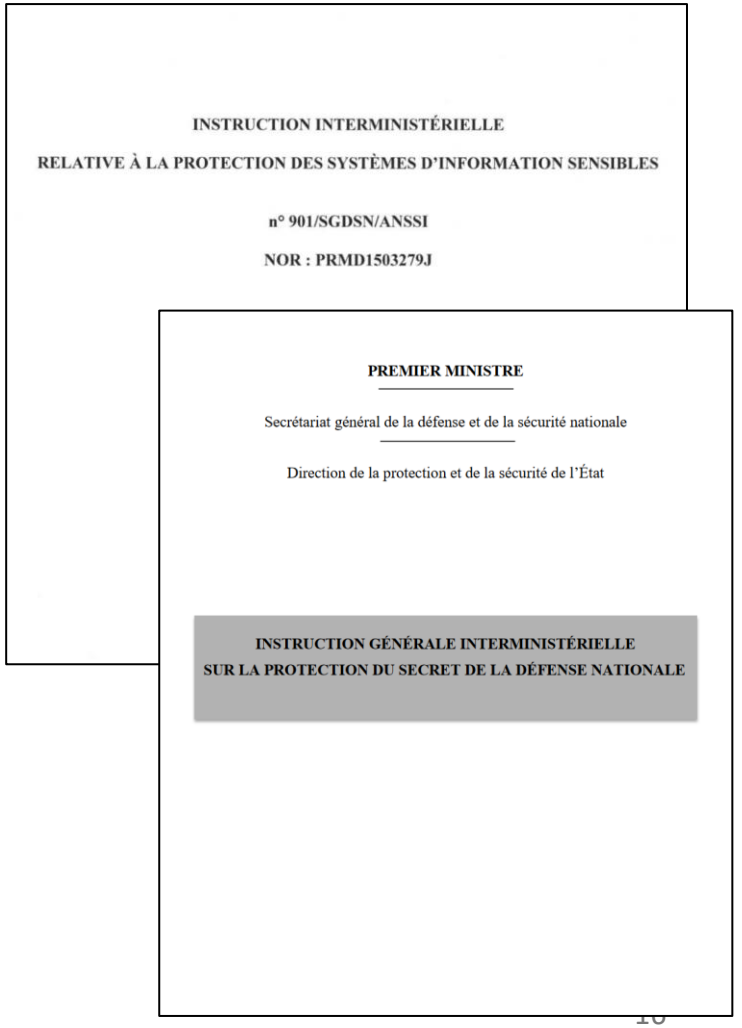
…

La PSDN

Protection du secret de la défense nationale

PSE

Niveau de protection	Risque pour un agent si diffusion
Non protégé	Aucun
Diffusion restreinte	Sanctions disciplinaires
Classifié	Sanctions pénales



Remise en cause de l'IAG

Risques envisagés :

- Fuite d'informations
- Accès à des informations pour des agents sans besoin d'en connaitre
- Génération d'informations sensibles à partir de données publiques

Solutions techniques
Expertise, développement, homologation

Solutions sensibilisation
Formations

Des agents remettent en cause la capacité d'adapter la technologie aux contraintes de l'administration

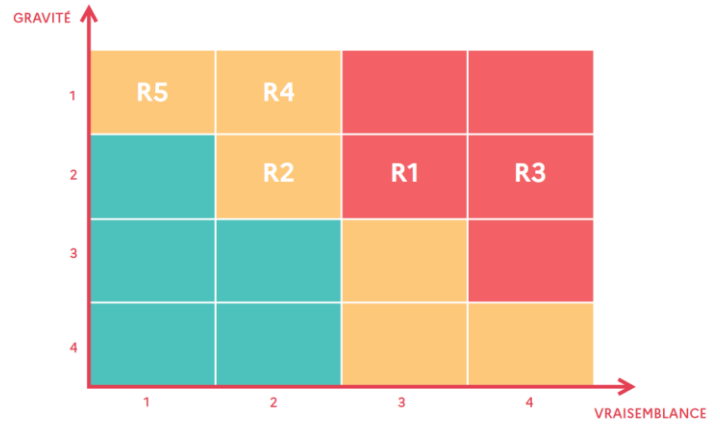
Remise en cause de l’administration

- **Déjà un règlement intérieur** sur les usages numériques
- **Mauvaises pratiques** de certains agents dans la gestion d’informations sensibles
- **Impossibilité d’évaluer** le degré de sensibilité d’un agrégat d’informations

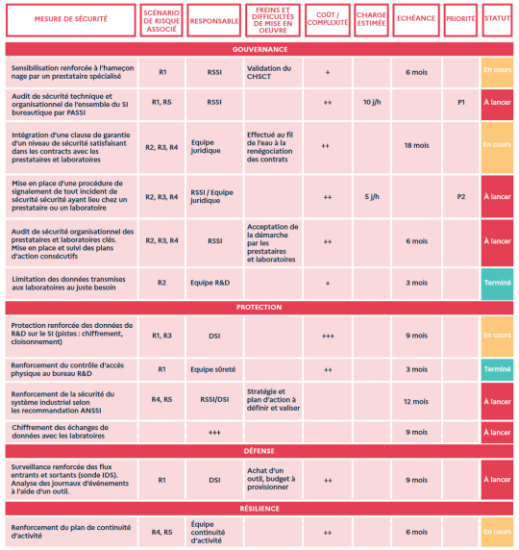
Les discussions remettent en cause la capacité de l’administration à respecter ses propres contraintes

Une méthode de décision ?

⇒ Analyse de risques



- Identifier et évaluer les risques
- Décider de l'acceptation du risque



MESURE DE SÉCURITÉ	SCÉNARIO DE RISQUE ASSOCIÉ	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN OEUVRE	COÛT / COMPLEXITÉ	CHARGE ESTIMÉE	ÉCHÉANCE	PRIORITÉ	STATUT
GOUVERNANCE								
Sensibilisation renforcée à l'hameçonnage par un prestataire spécialisé	R1	RSSI	Validation du CHSCT	+		6 mois		En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par PASSI	R1, R5	RSSI		++	10 j/h		P1	À lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contracts avec les prestataires et laboratoires	R2, R3, R4	Equipe juridique	Effectué au fil de l'eau à la renégociation des contrats	++		18 mois		En cours
Mise en place d'une procédure de signalement de tout incident de sécurité sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / Equipe juridique		++	5 j/h		P2	À lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires	++		6 mois		À lancer
Limitation des données transmises aux laboratoires au juste besoin	R2	Equipe R&D		+		3 mois		Terminé
PROTECTION								
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI		+++		9 mois		En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Equipe sûreté		++		3 mois		Terminé
Renforcement de la sécurité du système industriel selon les recommandation ANSSI	R4, R5	RSSI/DSI	Stratégie et plan d'action à définir et valider			12 mois		À lancer
Chiffrement des échanges de données avec les labratoires		+++				9 mois		À lancer
DÉFENSE								
Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'événements à l'aide d'un outil.	R1	DSI	Achat d'un outil, budget à provisionner	++		9 mois		À lancer
RÉSILIENCE								
Renforcement du plan de continuité d'activité	R4, R5	Équipe continuité d'activité		++		6 mois		En cours

Mobiliser les méthodes de décision

Rédaction d'une charte pour encadrer
les usages numériques de l'IAG

Conception par **cas d'usage :**

- Informer des risques pour les cas d'usages

⇒ Inscrire dans la charte les risques associés

⇒ Encadrer les usages en précisant les mesures de contrôle par cas d'usage

Conception par **levier technologique :**

- Sensibiliser sur la technologie au global

⇒ Ne pas prescrire de cas d'usages mais avertir sur les risques globaux

⇒ Encadrer l'utilisation par des modules de formations

Les questions sans méthode de décision

Risques envisagés :

- **Changement des méthodes** de travail sur le long terme : valider plutôt que produire
- **Evolution de la communication interne** comme mobilisation des expertises et des compétences
- **Orientation des productions** sans identifier les qualités (créativité, probabilité ou uniformité)

Peu de visibilité technique et de l'écosystème

Pas d'outil de décision technique consensuel

Pas de dynamique collective dans l'exploration de ces questions

Conclusion

- Sans expertise, l'administration ouvre les discussions à l'ensemble des directions
- Les outils traditionnels de décisions sont prolongés sur les nouveaux enjeux, adaptés et réinterrogés
- Les débats moins structurés (enjeux de transformation globale de l'administration, long terme) prennent moins de place dans la conduite des projets

⇒ L'IAG est envisagée comme un moyen **d'améliorer la réalisation des missions** du SGDSN **sans anticiper les transformations** plus globales de ses activités en raison d'un **manque d'outils techniques dédiés et consensuels**