Note de synthèse et de propositions option systèmes d'information et de communication :

Métropole de Soigny
Direction de Systèmes d'information à Soigny le,

Note à l'attention de Madame
la Directrice Générale des Services Métropolitains

Objet : La directive européenne NIS 2 et son application au service de la collectivité

Chaque année, le coût des cyberattaques croit de 10 %. Le nombre de structures touchées en France augmente de 70 %. Aucun secteur d'activité ni aucune typologie de structure n'échappe à la croissance de des cyberattaques.
Les collectivités territoriales n'échappent pas à cette recrudescence d'attaques informatiques. Elles sont d'ailleurs particulièrement vulnérables. Elles sont amenées à gérer de nombreux services publics en fonction de leurs compétences, ce qui les rend dépositaires d'un grand nombre de données personnelles des administrés.

En réponse à cette inflation de cyberattaques, les autorités publiques apportent des évolutions normatives.
L'objectif de ces évolutions est de mieux faire face et mieux préparer les structures aux menaces. La nouvelle norme européenne NIS 2 (Network and Information Security) apporte ainsi une réponse en contraignant les entités publiques et privées, et en particulier les collectivités territoriales à mieux faire face aux menaces numériques.

Ces évolutions normatives doivent être regardées comme des opportunités de transformation des organisations et non comme des contraintes réglementaires supplémentaires.
Leur application constitue une opportunité de mieux se protéger mais également d'engager une démarche globale de responsabilisation.

La mise en œuvre de la transposition de la directive européenne NIS 2 s'impose au regard de l'augmentation de menaces (I). Son application au sein des services métropolitains constitue une opportunité de monter collectivement une marche pour mieux se protéger (II).

I. La transposition de la directive RES 2 : un nouveau paradigme qui s'impose face à une cybermenace qui s'accroit.

L'augmentation des cybermenaces (A) justifie la mise en œuvre de la nouvelle directive européenne NIS 2 (B).

A. L'augmentation des cybermenaces rend les collectivités territoriales toujours plus vulnérables.

1. De plus en plus d'attaques informatiques sont recensées en France. Au cours de l'année 2024, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) a recensé 4386 événements de sécurité, qui représentent une augmentation de près de 15 % par rapport à l'année précédente. Les grands événements ou les tensions géopolitiques augmentent l'exposition des entités publiques ou privées aux cyberattaques. Pour les collectivités territoriales, la majorité de ces événements de cybersécurité concernait les communes et / ou les EPCI (Etablissements Publics de Coopération Intercommunale).

2. Plusieurs types d'attaques informatiques peuvent toucher particulièrement les collectivités territoriales. Tout d'abord, les attaques à but lucratif représentent la principale menace. On retrouve les attaques au moyen de rançongiciels, les exfiltrations et ventes de données et d'accès ainsi que d'autres types d'attaques comme les hameçonnages ou les compromissions de messagerie (…). Egalement, des attaques à but de déstabilisation peuvent cibler les collectivités territoriales, notamment des attaques dites « XXX comme les dénis de services distribués ou les sabotages par des acteurs répétés étatiques. Enfin, des attaques à but d'espionnage peuvent compromettre les collectivités territoriales qui gèrent parfois des données sensibles.

3. Les enjeux liés à ces vulnérabilités sont majeurs. En termes de continuité de service. Tout d'abord, les collectivités territoriales assurent des services stratégiques qui peuvent être sensibles : services de distribution d'eau potable, santé, protection des populations (…). Les enjeux d'assurer une continuité de services ne sont pas identiques pour l'ensemble des services rendus mais doivent être mis en avant. Egalement, en termes coûts, les enjeux sont majeurs. Le coût global est estimé à 2 milliards d'euros pour les victimes de cyberattaques, pour les collectivités territoriales, les coûts directs peuvent être de plusieurs millions d'euros auxquels s'ajoutent les coûts indirects (perte d'activité, perte de confiance des usagers…). Enfin, un enjeu de protection des données personnelles doit être mis en avant. Par les services que rendent les collectivités à la population, elles sont détentrices de nombreuses informations d'usagers ou d'agents à caractère personnel.

4. En 2025, la CNIL (Commission Nationale Informatique et Liberté) va concentrer ses contrôles sur la cybersécurité des collectivités territoriales. Elle va contrôler les mesures mises en œuvre par les collectivités territoriales afin de protéger les données des usagers. Elle va également renforcer ses actions de sensibilisation et d'accompagnement en matière de cybersécurité pour préparer les collectivités à l'entrée en application de la directive NES 2.

B. La nouvelle directive NES 2 amène les collectivités territoriales à changer de paradigme en les responsabilisant face aux cybermenaces.

1. Leur corpus de normes s'impose aux organisations pour renforcer leur résilience et leur cybersécurité. En 2022, l'Union Européenne a adopté 3 directives : la directive sur la résilience des entités critiques (REC), la directive NIS 2 qui vise à assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union Européenne et la DORA (Digital Opérationnel Resilience Act) relative au secteur financier bancaire et assurantiel. La transposition de ces directives en droit Français est

portée par la loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

2. L'objectif de la directive NES 2 est donc d'assurer un niveau élevé de cybersécurité en élargissant le périmètre des entités concernées par les mesures de régulation. La transposition amènerait à intégrer notre métropole dans ce périmètre, ainsi que l'ensemble des collectivités de plus de 30 000 habitants. La directive vise à transformer les pratiques de cybersécurité autour d'un nouveau standard et à faire évoluer la gouvernance des organisations qui deviendront responsables de leurs usages numériques. Elle retient une approche proactive de gestion des risques allant en complémentarité d'une vision plus « défensive » de la cybersécurité.

3. De nouvelles obligations vont alors s'imposer aux collectivités territoriales. La cybersécurité devient la responsabilité de l'organisation et non plus seulement de la Direction des Systèmes d'Information. Tout d'abord, l'organisation doit mener une démarche de gestion des risques robuste, en intégrant des protocoles de réponses aux incidents, en sécurisant la chaine d'approvisionnement ou en protégeant les réseaux et les données. Ensuite, la collectivité se doit d'assurer la continuité et la reprise d'activité après une attaque. Elle doit alors planifier la continuité d'activité, les sauvegardes (…). Enfin, la collectivité doit s'engager dans un processus de reporting rapide des incidents en notifiant les évènements aux autorités. Des sanctions plus sévères sont prévues en cas de non-conformité avec ces obligations.

   Ces nouvelles obligations qui s'imposent aux collectivités territoriales sont à mettre en œuvre dans une double perspective : se conformer aux obligations réglementaires mais également ouvrir et engager une réelle démarche d'amélioration de la résilience de la collectivité.

II. La mise en œuvre de la directive européenne est l'opportunité d'engager la collectivité dans une démarche d'amélioration.

L'application de la nouvelle directive doit être menée dans le cadre d'un projet global et partenarial (A).
La priorisation des actions doit répondre à une logique de gestion des risques et de mobilisation des ressources (B).

A. Leur projet global et partenarial qui doit être orienté vers l'amélioration des pratiques.

1. L'opportunité de mettre en œuvre la directive NES 2 dans le cadre d'un projet global favorisera son dimensionnement stratégique. La sécurité informatique n'est pas seulement une question qui intéresse la Direction des Systèmes d'Information puisque désormais, l'ensemble des processus métiers est concerné par la numérisation de tout ou partie de l'activité. La mise en œuvre de la Directive NES 2 va sécuriser l'ensemble de l'organisation mais doit emmener la collectivité, ses acteurs et ses partenaires à contribuer à une amélioration des pratiques et des

outils. Ainsi, un portage du projet par la direction des systèmes d'Information sous couvert par une commande formelle de la direction générale semblerait judicieux.

2. Une association large des acteurs du projet serait un facteur clé de succès. Les usagers internes des services numériques, l'encadrement opérationnel et l'encadrement stratégique doivent être impliqués dans la démarche. Des ressources spécifiques internes vont contribuer à la mise en œuvre des nouvelles actions, ces interventions vont nécessairement s'accompagner de montée en compétence des experts métiers, RSSI (Responsable Sécurité des Systèmes d'Information) mais également des services supports (qualité, juridique). Les exigences et expertises des partenaires extérieurs, notamment les prestataires vont être requestionnées pour qu'on engage une réelle démarche de montée en compétence collective.

3. La méthodologie de gestion de projet doit prévoir deux phases : une phase de préparation et une phase de mise en œuvre. D'autres phases se succèderont lorsque ces premières étapes auront apporté une réelle visibilité sur les opportunités et l'ampleur de la mise en conformité. La phase de préparation va consister à définir les objectifs du projet, identifier précisément le nouveau cadre réglementaire, les délais applicables et les spécificités. En fonction de ce premier cadrage, et de la XXXX des acteurs internes et externes, une proposition de plan d'actions sera formalisée. Les actions seront proposées autour de trois phases de gestion des risques : la sécurisation des systèmes, l'amélioration de la supervision et la réponse aux incidents.

B. La priorisation des acteurs doit tenir compte de la méthodologie de gestion des risques et des ressources associées.

Dans le cadre de ce projet global, la Direction des systèmes d'information devra porter les différentes actions, proposer une priorisation et la soumettre à un arbitrage de la Direction générale – Aussi, à l'appui des premiers éléments portés à notre connaissance, il est possible de mener 3 actions qui vont concourir à la sécurisation globale de notre système d'information et qui s'intègrent pleinement dans les exigences de la directive NES 2.

1. La mise en œuvre d'une démarche globale d'analyse des risques. La DSI peut mener cette analyse qui a pour objectif de cartographier et quotter l'ensemble des risques cyber. Elle mettra en avant les risques les plus sensibles selon une méthodologie classique d'analyse tenant compte de la Fréquence, la gravité et du niveau de maitrise actualisé. Elle distinguera les risques propres à l'organisation et les risques externes. L'analyse sera portée par le RSSI, sous couvert d'une méthodologie travaillée avec le responsable qualité. Certaines directions métiers pourront être associées pour qualifier et identifier des risques numériques dans les process métiers.
   Cette cartographie pourra être menée en lien avec les partenaires, les éditeurs en particulier. Elle doit être formaliser dans un délai de 6 mois et ne nécessite pas de crédits budgétaires spécifiques. Elle sera présentée en comité de direction générale pour décider du plan d'actions à venir.

2. La mise en place d'une démarche de sensibilisation globale doit s'adresser à l'ensemble des agents. Un accompagnement et nécessaire à plusieurs niveaux.

Tout d'abord, les utilisateurs des services numériques de la métropole doivent être sensibilisés aux risques et aux différentes menaces. Des actions de type Formation, campagne de Fishing, articles de blog (…) pourront être menées. Un accompagnement s'adressera aux agents de la DSI ou des directions métiers qui exercent une Fonction d'administrateur fonctionnel.
L'objectif est une montée en compétence générale des agents pour qu'ils contribuent, par leurs actions, à améliorer la sécurité numérique de la collectivité.
Des accompagnements dédiés et ciblés par des structures externes pourront être envisagées. Par exemple, les CSIRT (Centres de Réponse à des Incidents Cyber Territoriaux) peuvent être mobilisés pour des actions de prévention.
Ces actions peuvent débuter sans délai et doivent s'inscrire dans une démarche continue d'amélioration.
Des budgets devront être mobilisés (Formations, partenariat…).

3. La formalisation de plans de continuité et de reprise d'activité (PCA et PRA) devra favoriser l'appréhension des risques par les métiers et clarifier les actions à conduire en cas d'incident. Cette démarche va associer les directions métiers et la DSI en vue de définir une vision partagée des enjeux et des priorités. Elle pourra aboutir à un test de résilience des systèmes d'information de la collectivité.
   Ce test vise à s'assurer que les services et les activités critiques pourront être opérationnels en cas de crise. La formalisation des PCA et PRA nécessite une mobilisation importante des métiers et de la DSI mais pourra être conduite en interne.
   En revanche, les campagnes de test de résilience du système d'information pourront être menées avec l'aide d'un cabinet extérieur, expert en cybersécurité, qui viendra évaluer les capacités techniques de reprises.

La mise en conformité du système d'information en vue de l'application de la directive NES 2 est une obligation. Mais, elle revêt un caractère vertueux qui engage la collectivité dans une démarche globale et partenariale de diminution des risques. Elle permettra des remises à jour de compétences, procédures, documentation (…) et favorisera l'intégration du risques et sa connaissance par les équipes.

A.2. Les limites, freins et risques du développement de l'IA appliquée à la préservation du patrimoine routier

Arriver trop tard avec l'IA sera coûteux et difficilement maîtrisable et il existe un risque de voir le service public obsolète et inadapté.

A cela s'ajoute le sujet majeur de la propriété des données : pour en maîtriser, les usagers, les services publics devront maîtriser la propriété des données.

Un autre frein majeur existe et concerne les ressources humaines. Les agents pourront être inquiets des conséquences de ces outils sur leur emploi. Par ailleurs, un manque de confiance dans la fiabilité freinerait l'usage de l'IA. L'utilisation de l'IA dans l'aide à la prise de décisions nécessite un fort niveau de confiance dans ces nouveaux outils et les données qu'ils produisent.

Ainsi, les freins à l'appropriation ou un manque d'accompagnement des managers pourront limiter le développement de ces nouveaux outils.

D'un point de vue environnemental, l'IA conduit à une consommation importante d'énergie et nécessite le remplacement fréquent des matériels numériques.

D'un point de vue technologique la compatibilité des infrastructures routières existantes avec les nouvelles applications IA n'est pas garantie. De plus, les solutions développées évoluent très vite et sont rendues obsolètes souvent.

Le financement de l'IA peut constituer aussi un frein.

Enfin, le dernier risque est éthique : comment la protection des données est-elle assurée, comment sont garantis les droits fondamentaux, comment sont manipulés et surveillés les flux de données.

C. Perspectives de l'IA appliquée à la préservation du domaine public routier et à l'appui d'exemples.

B.1. Perspectives en plein mouvement

S'agissant des aspects éthiques, l'Europe a coordonné ses moyens pour aligner une réglementation commune au travers de l'ACT – AI. Elle vise à promouvoir un équilibre entre l'innovation et la protection de tous, une gestion éthique et une transparence afin de garantir les droits fondamentaux.

La perspective de confier à une machine la collecte de données, le traitement, la structuration des données et la restituer dans une réponse simple et rapide conduit l'homme à assurer sa valeur ajoutée dans l'analyse et la compréhension du résultat. Cela crée de la valeur.

Une autre perspective amène à diminuer la pénibilité des tâches de certains agents (exemple : gestion de la signalisation routière) et diminuer les coûts.

Expérimenter, prendre en compte les besoins des agents et analyser les retours d'expérience valorise le travail humain.

Dans le domaine de la gestion routière les usages sont très nombreux et donnent des perspectives intéressantes à analyser la circulation, assurer la maintenance

prédictive et préventive, mieux garantir la sécurité avec des données prédictives des accidents.

Plus concrètement, l'auscultation vidéo des chaussées, la réalisation d'inventaires des équipements, l'amélioration de l'information données aux usagers, les méthodes d'acquisition des données, l'aide à la programmation annuelle ou la gestion des moyens sont autant d'exemples de cas d'usage non exhaustifs.

Une autre perspective est organisationnelle : ces technologies vont transformer les métiers et seront source d'optimisation au service des usagers.

L'apprentissage de l'IA et le stockage toujours plus important de données conduira à un développement de la confiance dans ces outils.

Le CEA et le CEREMA développent un outil de prédiction et de la maintenance de 250 000 ponts, l'INRIA et le CEREMA contribuent à un projet collaboratif franco-allemand afin de définir un référentiel dans ce domaine d'application (Road AI).

B.2. Quelques exemples de collectivités

Londres a testé le diagnostic de 400 km de voiries avec des vidéos avec cette technique Road AI.
Cela permet à la ville de tester, calibrer et améliorer la technique en seulement 48 heures alors qu'un travail humain aurait nécessité plusieurs mois.

Le Département du Loiret a participé au projet européen 'Interreg NWE Be-good safer roads » afin d'améliorer et sécuriser ses 3613 km de voiries et réaliser une analyse prédictive des accidents.

L'expérience de la Haute-Garonne depuis 2017 montre maintenant un coût optimisé de 15 euros par kilomètre de voirie auscultée.

La Charente a une expérience similaire et travaille plus finement sur l'analyse des catégories de dégradations des chaussées.

Enfin, le consortium de recherche franco-allemand Renov alte teste l'utilisation de l'IA dans la rénovation des infrastructures routières.

Je vous propose à présent des actions stratégiques et opérationnelles à engager dans notre département Soleil avec dans un premier temps la mise en place de la gouvernance et un diagnostic / structuration des besoins. Dans un second temps, je vous proposerai des actions stratégiques priorisées et je terminerai par un focus sur les moyens d'accompagnement à la démarche.

III. Propositions stratégiques et opérationnelles de renforcement de la préservation du patrimoine routier avec un usage soutenu des outils utilisant l'IA.

A. Mise en place de la gouvernance et proposition d'un diagnostic.

A.1. Mise en place de la gouvernance politique et du projet

Depuis l'accident ayant causé plusieurs décès et blessés je propose d'instaurer un COPIL composé du Vice-Président aux routes, de conseillers départementaux modérés par le sujet et de membres extérieurs comme un représentant national de la sécurité routière faisant autorité. Les principaux directeurs seront présents dans cette instance élue. Je propose une délibération de principe pour le développement de l'IA afin d'optimiser et améliorer la préservation du domaine public routier départemental. La délibération mentionnera les enjeux et objectifs à atteindre : réduire les coûts,

gagner du temps et accélérer la connaissance et l'analyse du patrimoine, développer les outils adaptés d'acquisition, de traitement, d'analyse et d'exploitation des données.

Un CETEC que je propose d'animer sera composé de la DSI, la DRH, la direction juridique mais aussi d'autres directions chargées de diverses politiques publiques centrées sur l'habitat, le social et l'environnement.

A.2. Un diagnostic nécessaire des pratiques actuelles de gestion du patrimoine routier et la structuration des besoins des agents

Compte tenu des besoins limités dans le temps, je recruterai un AMO spécialisé. Il aura pour mission d'organiser des ateliers avec les représentants échantillonnés des différents métiers de la Direction des routes. Il aura pour mission d'auditer les pratiques actuelles et faire ressortir les forces et faiblesses dans le fonctionnement actuel sans utilisation d'IA.

Les thématiques concerneront de façon prioritaire les méthodes de diagnostic des Voiries et ponts et la gestion des données afférentes. Les outils, temps de travaux, coûts et méthodes seront évaluées ainsi que la fréquence de l'état du patrimoine. Les moyens utilisés seront analysés ainsi que les difficultés, les risques et les premières pistes de propositions.

L'AMO aura également pour mission d'auditer les directeurs de l'habitats, de l'action sociale, de l'environnement, de la DSI, la DRH et la direction juridique afin de poser les fondements élargis de la démarche en prenant en compte les observations de chacun : freins, opportunités, éléments de contexte transversaux afin d'assurer une vision globalisée de la problématique à traiter.

B. Actions concrètes et accompagnement de la démarche.

B.1. Actions concrètes priorisées

Je proposerai une première expérimentation de l'IA afin de consolider la connaissance du patrimoine à partir de données existantes à consolider progressivement.

Afin de connaître l'état des routes et des ouvrages d'art, je propose de lancer un diagnostic vidéo en prenant appui sur les expériences consolidées du CEREMA.

La partie outil IA sera aussi consolidée avec le DSI ou son représentant désigné afin de formaliser l'entrepôt des données (où, quand, comment), le stockage, l'analyse et la restitution des résultats. Un avis de la direction juridique sera nécessaire afin de respecter les directives européennes ACT – AI et la réglementation RGPD.

La structuration et la fiabilisation des données au service de l'aide à la décision sera la seconde priorité mais nécessitera un peu de temps pour consolider et vérifier la cohérence des données. L'aide à la décision portera notamment sur les décisions à prendre à partir de

Afin d'augmenter et améliorer les données disponibles, je propose d'expérimenter la pose de capteurs avec l'internet des objets, structurer la remontée de ces informations (et celles disponibles dans les autres équipements existants). Cela permettra de consolider à la fois, la quantité et la qualité des données exploitables.

D'autres actions ultérieures pourront être expérimentées dans la deuxième partie du mandat :

- Analyse des flux de circulation et décisions à prendre pour limiter les impacts environnementaux
- Développement de la maintenance prédictive, catégorisation des dégradations afin d'établir un plan pluriannuel d'investissement cohérent et optimisé en fonction des priorités proposées par les outils IA.

Enfin, dans un mandat ultérieur l'information des usagers ou la gestion des moyens pourront être traitées. La gestion sécurité et optimisée des chantiers sera aussi une des pistes à développer dans un temps un peu plus long.

B.2. Accompagnement organisationnel et humain à la démarche

L'accompagnement humain sera une priorité à traiter dès le début du projet (travail de l'AMO pour établir son diagnostic), pendant toute la durée du projet et enfin pour exploiter tous les retours et expérience. L'accompagnement humain sera à formaliser avec tous les managers de la direction des routes. Les derniers seront formés XXX sensibilisés aux changements induits par l'IA avec l'aide de la DRH, la DSI si nécessaire et moi-même. Les craintes liées aux suppressions de tâches avec l'IA, la réticence à faire confiance aux outils, la transformation des métiers nécessiteront des rencontres évaluées dans le temps pour accompagner toutes les équipes de la direction des routes, afin d'intégrer progressivement les changements.

Afin de favoriser la montée en compétence des équipes, des formations seront dispensées sur l'IA appliquée à la gestion des infrastructures routières.

Pour les agents les plus inquiets, des entretiens individuels pourront être proposés avec leur manager.

La DRH sera associée pour évaluer l'impact sur les fiches de poste des agents et proposer des adaptations en lien avec les propositions de l'encadrement.

Afin d'assurer une amélioration continue, des retours et expériences seront systématiquement organisés avec les encadrants et consolidés au niveau direction.

Pour asseoir et garantir l'éthique et la sécurité de la démarche, la direction juridique sera sollicitée pour vérifier le respect de la réglementation en vigueur (ACT - AI européen et RGPD français).

Le budget aura été consolidé avec la DSI en amont pour permettre d'acheter les outils IA et expérimenter l'internet des objets avec des capteurs.

Des indicateurs seront mis en place pour mesurer les impacts des outils utilisés (exemples : évolution du nombre et accidents, nombre d'incidents sur les ouvrages d'art…).

Utiliser l'IA se construit progressivement et son utilisation doit débuter dès maintenant avec des expérimentations, des améliorations après les retours d'expérience, et des usages à consolider progressivement dans le temps en suivant les priorités données par l'exécutif. Ce domaine nouveau nécessitera à la fois des adaptations mais aussi des données nouvelles à mesurer et à collecter pour développer la confiance dans ces outils et ainsi constituer une véritable aide à la décision efficace qui fera gagner du temps, diminuera les accidents et optimisera la gestion du patrimoine routier départemental.

Domaine en pleine évolution, il nécessitera un questionnement régulier en lien avec les différentes directions transverses afin de garantir un service public de qualité répondant aux besoins des usagers de la route.