Partie 1

COMPRENDRE les défis numériques actuels et futurs

« En matière cyber, nulle entreprise, ni aucun internaute ne peuvent affirmer ne jamais avoir fait l'objet d'une cyberattaque. Ainsi, pour la première fois dans l'histoire de l'utilisation d'un système, 100 % de ses utilisateurs ont été victimes, a minima *d'une tentative d'attaque (généralement de fraude, d'escroquerie ou de rançongiciel). »*

X. Leonetti, magistrat

***

La cybersécurité est devenue un enjeu stratégique majeur pour les collectivités territoriales. **Cette première partie a pour objectif d'offrir aux décideurs une compréhension claire des enjeux et des menaces auxquels leurs organisations font face**, sans pour autant les transformer en experts techniques.

Dans un environnement numérique en constante évolution, la maîtrise des concepts fondamentaux constitue un prérequis indispensable pour piloter efficacement les politiques de sécurité.

Cette partie vise avant tout à construire un socle de connaissances solide, permettant aux dirigeants d'appréhender sereinement les défis cyber de leur collectivité et de dialoguer en confiance avec les experts techniques. Ils seront ainsi mieux armés pour agir et porter les projets stratégiques de leur organisation.

Elle s'articule en deux chapitres.

Le premier chapitre, « **Vulnérabilités du service public local face aux cyberattaques** », dresse un état des lieux détaillé des menaces actuelles, des fragilités structurelles des collectivités, des principales formes d'attaques et de leurs impacts sur le service public.

Le second chapitre, « **Cadre légal et réglementaire de la cybersécurité des collectivités** », analyse les obligations qui encadrent aujourd'hui la cybersécurité des collectivités territoriales, en détaillant notamment leur adaptation selon la taille des structures et leur niveau de risque.

Si vous êtes **pressé et souhaitez passer directement à l'action**, vous pouvez tout à fait **lire le chapitre I pour bien cerner les enjeux, puis avancer directement à la partie 2**, où vous trouverez la méthode concrète pour construire votre PCA-cyber en 100 jours. Vous pourrez revenir au chapitre II à tout moment pour vérifier vos obligations légales et approfondir votre compréhension réglementaire lorsque vous en aurez besoin.
L'essentiel est d'avancer à votre rythme, en fonction de vos priorités et de vos contraintes locales.

Chapitre I

Vulnérabilités du service public local face aux cyberattaques

Dans un monde où la numérisation des services publics s'accélère, les collectivités territoriales se trouvent en première ligne face à des cybermenaces de plus en plus sophistiquées.

Ce premier chapitre propose une analyse globale de ces menaces. Il débute par un état des lieux des risques numériques qui pèsent sur le secteur public local (A), puis met en lumière les vulnérabilités propres aux collectivités, liées notamment à la diversité des structures et au manque de ressources (B). Un scénario illustratif d'attaque informatique visant une mairie et une intercommunalité (C) permet d'appréhender concrètement les mécanismes d'intrusion. Le chapitre passe ensuite en revue les principales formes d'attaques (D) observées dans ce contexte, ainsi que les techniques utilisées. Enfin, il analyse les impacts de ces cyberattaques sur la continuité des services publics (E), tant du point de vue opérationnel que financier, sans oublier les effets sur la confiance des usagers envers les institutions locales.

A - État des lieux de la menace cyber dans le secteur public

1. L'évolution des cyberattaques

La menace cyber est aujourd'hui une réalité omniprésente, touchant tous les secteurs de la société. Elle s'intensifie au rythme des avancées technologiques et des transformations numériques, avec l'émergence de techniques d'attaque toujours plus sophistiquées et difficiles à détecter. Le ministère de l'Intérieur souligne ainsi que *« la persistance des cybermenaces représente une tendance de fond, avec une augmentation constante du nombre d'infractions liées au numérique enregistrées ces dernières années en France »*[1].

1. *Rapport annuel sur la cybercriminalité du ministère de l'Intérieur*, 2024.

Cette évolution s'inscrit dans un contexte global complexe, où les enjeux géopolitiques, économiques et sociaux s'entremêlent avec le domaine numérique. Les acteurs malveillants, qu'il s'agisse de groupes criminels organisés, d'États hostiles ou de hacktivistes[2], exploitent ces interconnexions pour maximiser l'impact de leurs actions. Selon l'Enisa (Agence de l'Union européenne pour la cybersécurité), *« à mesure que les tensions géopolitiques et économiques augmentent, la cyberguerre s'intensifie avec l'espionnage, le sabotage et les campagnes de désinformation devenant des outils clés pour les nations afin de manipuler les événements et sécuriser un avantage stratégique »*[3].

La France, comme de nombreux pays développés, fait face à une menace qui dépasse désormais les entreprises et les institutions gouvernementales. Dans la *Revue nationale stratégique 2025*[4], les services du Premier ministre confirment que *« la cybercriminalité s'est développée massivement : elle touche désormais tous les pans de la société (hôpitaux, collectivités territoriales, PME, etc.). [...] Cette menace pèse sur le développement économique de la France et porte atteinte à la confiance des populations dans le numérique »*. Les collectivités territoriales, les petites et moyennes entreprises, et même les particuliers sont devenus des cibles potentielles, nécessitant une sensibilisation et une protection accrues à tous les niveaux de la société. Jules Veyrat[5], expert européen en couverture du risque cyber, estime d'ailleurs que *« face à une telle menace, et en particulier dans un contexte géopolitique aussi incertain, il faut faire front commun, car la réponse ne peut qu'être collective »*[6].

Le directeur de l'Anssi[7], Vincent Strubel, a rappelé cette vulnérabilité des plus petites structures dans son discours d'ouverture du FIC[8] en avril 2025. À ses yeux, *« la directive européenne NIS 2 arrive à point nommé et c'est une nécessité [...] Ces textes vont être l'occasion de parler de cybersécurité à des petites structures et cela avant que des attaquants ne leur en parlent de manière moins agréable »*[9].

2. L'impact sur les collectivités territoriales

« Une collectivité sur dix déclare avoir déjà été victime d'une ou plusieurs attaques au cours des douze derniers mois. »(1)

(1) *Baromètre de la maturité cyber des collectivités*, Cybermalveillance.gouv.fr, 2024.

2. Hacktivistes : individus ou groupes qui utilisent des techniques de piratage informatique pour promouvoir des causes politiques, sociales ou idéologiques.
3. *Rapport annuel d'activité Enisa*, 2024.
4. *Revue nationale stratégique 2025*, secrétariat général de la Défense et de la Sécurité nationale, 14 juillet 2025.
5. Jules Veyrat est président et cofondateur de Stoïk, premier acteur de l'assurance cyber pour les PME et entreprises de taille intermédiaire (ETI).
6. *Rapport Stoïk 2024 sur la sinistralité cyber*, 20 mars 2025.
7. Agence nationale de la sécurité des systèmes d'information (https://cyber.gouv.fr).
8. Le forum InCyber (FIC) est un événement annuel majeur dédié à la cybersécurité, réunissant des experts, des décideurs et des professionnels pour discuter des enjeux et des innovations dans le domaine.
9. Article *Le Monde informatique* : « FIC 2025 : Mobiliser pour muscler la cybersécurité des petites structures », 2 avril 2025.

Les collectivités sont devenues des cibles privilégiées pour les cybercriminels. En effet, elles gèrent à la fois des données sensibles (état civil, données fiscales, informations personnelles des usagers) et des services essentiels (eau, voirie, écoles, gestion des déchets, etc.), ce qui en fait des points névralgiques du bon fonctionnement de la société.

La plupart des collectivités ne disposent que de moyens limités pour se protéger efficacement contre les cybermenaces. Cette faiblesse crée un écart préoccupant entre la sensibilité des actifs à protéger et les moyens disponibles pour les défendre. Les motivations des cybercriminels sont variées : extorsion financière, vol de données stratégiques ou volonté de perturber les services publics.

Rapport d'activité de l'Anssi[7]

Sur l'année 2024, l'Anssi a traité un total de 4 386 événements de sécurité[(1)], marquant une augmentation de 15 % par rapport à 2023. Sur ces incidents, 219 concernaient spécifiquement les collectivités territoriales[(2)], soit environ 5 % du total des incidents traités. Cette proportion significative souligne la vulnérabilité particulière du secteur public local, avec une moyenne de 18 incidents par mois touchant les collectivités. L'analyse détaillée montre que toutes les strates de collectivités sont concernées, avec une majorité d'incidents affectant les communes et EPCI[(3)], suivis par les départements (44 incidents) et les régions (29 incidents). Cette répartition suggère que la menace cyber ne fait pas de distinction en termes de taille ou de type d'organisation publique.

(1) Rapport Anssi : *Panorama de la cybermenace 2024*, mars 2025.

(2) Rapport Anssi : *Synthèse de la menace – Collectivités territoriales*, février 2025.

(3) Un établissement public de coopération intercommunale (EPCI) : communautés de communes, communautés d'agglomération, communautés urbaines, métropoles.

3. La transformation numérique du secteur public

La transformation numérique du secteur public, accélérée ces dernières années avec les nouvelles technologies, a profondément modifié le fonctionnement des collectivités territoriales. Elles se trouvent désormais au cœur d'un écosystème numérique complexe, gérant une multitude de services en ligne, de données sensibles et d'infrastructures connectées.

Cette numérisation croissante élargit la surface d'attaque, rendant la protection des systèmes d'information plus cruciale que jamais. La cybersécurité devient ainsi un élément de la gouvernance locale, au même titre que la gestion financière ou l'aménagement du territoire.

Les élus et dirigeants territoriaux sont confrontés à un double défi : assurer la qualité des services publics tout en garantissant la sécurité des données et des systèmes. Cela exige une prise de conscience à tous les niveaux de l'administration et une intégration systématique des considérations de cybersécurité dans tous les projets et processus.

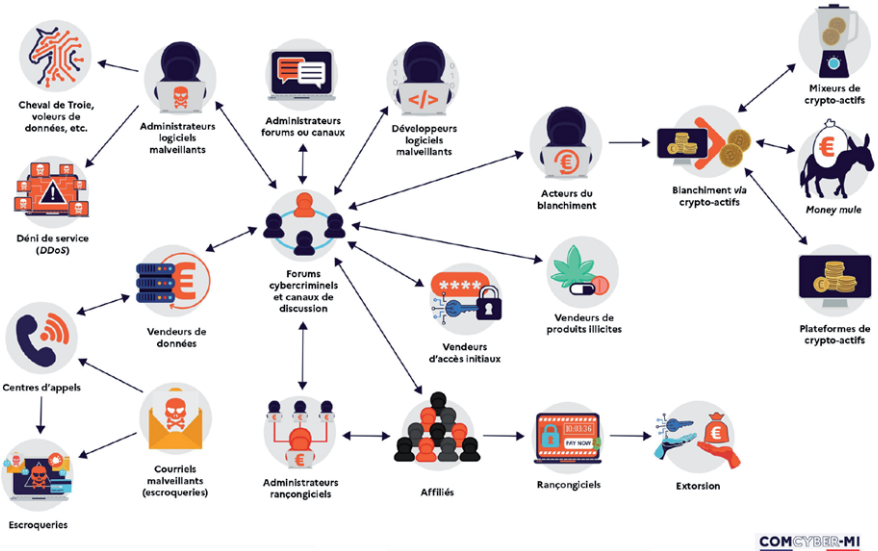
4. L'évolution rapide des menaces

L'évolution des cybermenaces et la capacité d'adaptation des collectivités territoriales s'inscrivent dans des temporalités radicalement différentes. Alors que les menaces se transforment à une vitesse fulgurante, les institutions publiques peinent à suivre ce rythme effréné.

a) Professionnalisation des cybercriminels

Le paysage des cybermenaces évolue sous l'effet d'une professionnalisation croissante du cybercrime, qui se traduit par l'émergence d'un véritable écosystème facilitant l'accès à des outils d'attaque sophistiqués. Désormais, même des individus peu qualifiés techniquement peuvent lancer des offensives élaborées.

Exemple de modélisation d'un écosystème cybercriminel



Exemple de modélisation d'un écosystème cybercriminel

COMCYBER-MI
Rapport annuel sur la cybercriminalité 2024