Julie-Charlotte FERREIRA

Quels risques cyber pour les collectivités territoriales ?

Université BORDEAUX MONTAIGNE
Cyber criminalités

Promotion 2024-2025

Abstract

À l'heure où la transformation numérique devient un levier essentiel de modernisation des services publics locaux, les collectivités territoriales françaises sont confrontées à une multiplication des cyberattaques, souvent dévastatrices. Cet article propose une analyse approfondie des risques cybernétiques pesant sur ces structures, en s'appuyant sur des données récentes, des études de cas (Marseille, Lille, Sartrouville) et les rapports d'organismes spécialisés (ANSSI, Clusif, cybermalveillance.gouv.fr).

La typologie des menaces (rançongiciels, phishing, exfiltration de données, attaques DDoS) met en évidence une vulnérabilité structurelle aggravée par l'hétérogénéité des moyens humains, financiers et techniques. Les conséquences des attaques, tant techniques qu'organisationnelles, économiques et réputationnelles, soulignent l'urgence d'une réponse systémique.

L'article identifie plusieurs leviers de résilience : renforcement des infrastructures techniques, désignation d'un RSSI, élaboration de plans de continuité d'activité, montée en compétences des agents et mutualisation territoriale des moyens. Il examine enfin les opportunités offertes par la directive européenne NIS2 et les dispositifs nationaux (France Relance, CSIRT régionaux).

En conclusion, la cybersécurité doit être pensée comme un pilier stratégique de la gouvernance territoriale, au service de la continuité démocratique et de la confiance numérique. L'étude ouvre des perspectives de recherche pour mesurer la maturité cyber des collectivités et l'efficacité des politiques publiques de cybersécurité locale.

1. Introduction

La numérisation des collectivités territoriales s'est accélérée depuis plusieurs années avec la digitalisation des services (état civil, urbanisme, eau, éducation…) mais leur protection contre les cybermenaces n'a pas suivi la même cadence. En comparaison avec le secteur privé, seulement 14 % des incidents signalés à l'ANSSI en 2024 concernaient ce secteur. Pour autant le nombre d'attaques qui ont touché les collectivités reste élevé. L'ANSSI alerte sur le fait que ces attaques peuvent bloquer totalement les services publics. Face à cette menace croissante, notre étude tentera de répondre à la question suivante : **quels sont les risques cyber spécifiques aux collectivités et comment renforcer la résilience de ces dernières face aux menaces ?**

2. Méthodologie

Cette recherche adopte une approche qualitative et documentaire afin d'analyser les dangers des cyberattaques ciblant les collectivités territoriales françaises. L'objectif méthodologique est de croiser des données issues de sources variées afin de produire une synthèse analytique rigoureuse et contextualisée.

2.1 Revue de littérature institutionnelle et scientifique

L'étude repose principalement sur une **revue de littérature** (rapports publics, notes techniques, bulletins de veille), et **scientifique**, incluant :

- Les rapports annuels de l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information), notamment celui de 2024-2025, qui fournit des données sur les incidents répertoriés, leur typologie et leur impact.
- Les études de **cybermalveillance.gouv.fr**, en particulier son **Baromètre de la cybersécurité des collectivités territoriales 2024**, mené avec OpinionWay auprès de 1 710 élus et agents de collectivités.
- Des publications de la **CNIL** sur les obligations juridiques des collectivités en matière de protection des données.
- Des analyses de cabinets spécialisés en cybersécurité (Clusif, LockSelf) portant sur les tendances des menaces et les niveaux de préparation.
- Des publications universitaires et des articles scientifiques accessibles via **cairn.info**, **OpenEdition** ainsi que des revues de science politique ou d'administration publique.

Ce corpus documentaire a été sélectionné sur des critères de **pertinence temporelle** (publications 2020-2025), de **fiabilité** (source officielle ou scientifique) et de **spécificité territoriale**.

2.2 Analyse de cas empiriques

Cette étude repose également sur une **analyse comparative de cas** concrets de cyberattaques ayant touché des collectivités françaises entre 2020 et 2024. Les critères de sélection incluent :

- La diversité géographique et démographique (villes, départements, région.
- La variété des types d'attaques (rançongiciel, intrusion, DDoS, phishing).
- La disponibilité d'informations fiables (rapports officiels, presse spécialisée, témoignages publics).

Sont analysés les cas de :

- **La ville de Marseille** (2020) : paralysie de services clés pendant plusieurs semaines à la suite d'un ransomware.
- **Sartrouville** (2022) : vol de données RH par un groupe cybercriminel.
- **Lille** (2023) : attaque massive chiffrant plusieurs serveurs critiques.
- **Mandeure** (2023) : attaque avec demande de rançon de 5 millions de dollars.
- **Département et Région Pays de la Loire** (2024) : cible d'un rançongiciel (LockBit), provoquant une coupure partielle des systèmes.

Ces études de cas permettent d'ancrer l'analyse dans des réalités opérationnelles concrètes.

2.3 Limites de la méthodologie

L'étude est limitée par :

- La **disponibilité partielle des données** : certains incidents ne font pas l'objet de publications détaillées ou ne sont pas signalés officiellement.
- Une **sous-représentation des plus petites communes** dans certaines enquêtes nationales.
- L'absence d'observation directe ou d'entretiens, qui auraient enrichi l'analyse qualitative.

Malgré ces limites, la triangulation des sources (rapports, données statistiques, cas empiriques) permet de proposer une analyse robuste et contextualisée de la menace cyber pesant sur les collectivités.

3. Résultats et discussion

3.1 Typologie des cyberattaques ciblant les collectivités territoriales

Les cybermenaces qui pèsent sur les collectivités s'inscrivent dans un contexte global d'industrialisation des attaques et de spécialisation des groupes cybercriminels. En 2024, l'ANSSI a recensé **218 incidents dans le secteur public** dont **144 visant des mairies, 44 des départements et 29 les régions,** parmi lesquelles **25 attaques par rançongiciel** confirmées (ANSSI, 2025).

a) Rançongiciels (ransomware)

Les rançongiciels sont de loin la menace la plus destructrice et aussi la plus fréquente. Ils consistent à chiffrer les données de la collectivité et à exiger une rançon pour en rétablir l'accès. Exemples notables :

- **Ville de Marseille** (2020) : des milliers de postes de travail paralysés pendant plusieurs semaines, affectant notamment l'état civil, les inscriptions scolaires et la délivrance de documents officiels.
- **Lille** (2023) : attaque par LockBit entraînant un gel complet des systèmes internes, avec des pertes estimées à près de **1 million d'euros**.
- **Mandeure** (2023) : la rançon exigée atteignait **5 millions de dollars**, ce qui constitue un record en milieu territorial (Le Monde, 2023).

- **Département et Région Pays de la Loire** (2024) : cible d'un rançongiciel (LockBit), provoquant une coupure partielle des systèmes.

b) Phishing et ingénierie sociale

Le **phishing** représente une porte d'entrée classique, facilitée par le manque de sensibilisation du personnel. Le **Baromètre Cybermalveillance 2024** indique que **30 % des incidents** déclarés sont liés à une erreur humaine, principalement via des mails frauduleux imitant des prestataires ou des administrations.

c) Intrusions et vols de données

Certaines attaques n'impliquent pas de rançon, mais visent l'**exfiltration silencieuse de données** sensibles : annuaires d'agents, documents de marché public, données RH. En 2023, la ville de **Sartrouville** a ainsi vu publiés sur le dark web des pièces d'identité, bulletins de salaire et courriers internes.

d) Attaques DDoS et défigurations (defacement)

Utilisés principalement à des fins politiques ou idéologiques, les attaques DDoS et les défacements de sites ont été massivement observés en 2023, notamment lors du conflit russo-ukrainien. Des dizaines de mairies ont vu leur site remplacé par des messages prorusses ou bloqué pendant plusieurs jours (CSIRT-CyberCorsica, 2024).

3.2 Vulnérabilités structurelles des collectivités

L'exposition des collectivités est en grande partie due à leur **faible maturité en cybersécurité**, aggravée par des moyens humains, financiers et techniques très hétérogènes.

a) Budget et ressources humaines limitées

Le Baromètre Cybermalveillance révèle que **73 % des communes de moins de 25 000 habitants** disposent d'un **budget cybersécurité inférieur à 5 000 € par an** ; **77 % y consacrent moins de 2 000 €**. En outre, **moins de 15 %** d'entre elles ont un référent ou un responsable de sécurité informatique.

b) Absence de RSSI ou de gouvernance claire

Dans les collectivités de moins de 3 500 habitants, **87 % n'ont pas désigné de RSSI** (Responsable de la sécurité des systèmes d'information), contre 100 % dans les métropoles. Cette absence se traduit par un défaut de politique formelle de sécurité, d'analyse de risques et de suivi des incidents.

c) Manque de sensibilisation des agents

Selon le même baromètre, **47 % des collectivités identifient le manque de culture cyber comme leur principale faiblesse**. 65% ne se sentent pas à l'aise avec les outils numériques, toutes catégories confondues. Or, 90 % des attaques réussies impliquent une erreur humaine à un moment du cycle.

d) Obsolescence technologique et hétérogénéité des systèmes

Les parcs informatiques, très hétérogènes et souvent anciens, comportent de nombreuses failles non corrigées. Un exemple rapporté en 2023 concerne une mairie dont le site web a été compromis via une **extension WordPress non mise à jour depuis 2017**. Tout cela par manque de moyens et de connaissances des risques cyber.

3.3 Conséquences des cyberattaques sur les collectivités

Les conséquences des attaques sont multidimensionnelles, allant bien au-delà des impacts techniques immédiats.

a) Impacts techniques

- **Paralysie des services** : Les villes touchées doivent parfois **isoler complètement leur système** pendant plusieurs semaines.
- **Pertes de données** : En l'absence de sauvegardes déconnectées, certaines collectivités perdent irrémédiablement des archives numériques.

b) Impacts économiques

- Les coûts engendrés par une attaque incluent l'intervention d'experts, la restauration des systèmes, l'achat d'équipements neufs, les frais juridiques, le maintien du salaire des agents malgré l'impossibilité matérielle de poursuivre leurs tâches quotidiennes- sans parler du temps alloué à la remise en activité des services. On pense notamment à la numérisation des travaux réalisés sur papier lors d'un mode dégradé.
- Exemples : **Houilles** a déboursé **350 000 €** après une attaque en janvier 2021 ; la **ville de Lille**, environ **1 million d'euros** en 2023.

c) Impacts juridiques et réputationnels

- La **fuite de données personnelles** peut entraîner des **sanctions de la CNIL** si la RGPD n'est pas respectée.
- La **perte de confiance** des administrés est un impact moins visible mais réel : plusieurs communes rapportent des tensions, notamment sur les réseaux sociaux, après des attaques révélées publiquement.

d) Impacts organisationnels et sociaux

- Les services doivent parfois **revenir temporairement au papier**, ralentissant les délais de traitement et augmentant la charge de travail.
- Les agents subissent une pression accrue, certains témoins évoquant des **retards de paie**, des suppressions d'accès aux outils de travail, voire des arrêts maladie liés au stress post-incident.

3.4 Discussion : une vulnérabilité systémique territoriale

Ces résultats suggèrent que les **collectivités territoriales représentent un maillon faible** de la cybersécurité nationale. Ce constat est renforcé par :

- Une **cyberdéfense encore trop centralisée**, alors que les attaques se multiplient localement ;
- Un **retard de mise en œuvre** de la directive européenne **NIS2**, qui impose des obligations renforcées de cybersécurité aux opérateurs de services essentiels, y compris certaines collectivités dès 2025.

La situation actuelle appelle donc un **changement de paradigme** : la cybersécurité des territoires doit être perçue non comme un coût, mais comme un **investissement stratégique dans la continuité de l'action publique**.

4. Stratégies de prévention et de résilience

Face à la recrudescence et à la sophistication des cyberattaques ciblant les collectivités territoriales, une stratégie de réponse efficace nécessite une approche pluridimensionnelle : **technique, organisationnelle, juridique, humaine et partenariale.** Plusieurs leviers d'action, identifiés à travers les recommandations de l'ANSSI, du SGPI (Secrétariat général pour l'investissement), le CNFPT et de la CNIL permettent de renforcer la résilience des entités locales.

4.1 Renforcement des infrastructures techniques

Le premier pilier de la prévention repose sur la **sécurisation du système d'information** :

a) Cartographie et segmentation du SI

Les collectivités doivent identifier et hiérarchiser leurs actifs critiques : serveurs, bases de données, applicatifs métier. Une **segmentation réseau** permet de limiter la propagation d'une attaque. Mise en place de VLAN séparés, pares-feux internes, journalisation centralisée sont les premières recommandations de l'ANSSI.

b) Sauvegardes régulières, déconnectées et testées

L'une des erreurs courantes est de conserver les sauvegardes dans le même environnement que les systèmes en production. L'ANSSI recommande :

- Des **sauvegardes hors-ligne ou chiffrées**.
- Une **vérification mensuelle** de leur intégrité.

c) Mise à jour des systèmes et audit de sécurité :

De nombreuses attaques exploitent des failles connues mais non corrigées.

- Le recours à des **solutions de supervision (EDR, SIEM)** devient essentiel.
- Des **audits réguliers**, notamment via les CSIRT régionaux, sont encouragés par le plan France Relance.

4.2 Renforcement de la gouvernance cyber locale

Les collectivités doivent adopter une **approche structurée de la gouvernance cyber**, encore trop souvent inexistante.

a) Désignation d'un RSSI ou d'un référent cyber

Selon cybermalveillance.gouv.fr, **seulement 14 % des collectivités ont un RSSI** dédié. Une mutualisation intercommunale ou départementale est parfois nécessaire pour pallier ce manque.

Bien qu'il en existe déjà ou en cours de mise en place, nous n'avons pas encore assez de recul pour en apprécier les retombées positives.

b) Élaboration d'un plan de sécurité des systèmes d'information (PSSI)

Ce document stratégique définit les règles de sécurité, les responsabilités, les procédures d'escalade en cas d'incident. Ce plan n'est malheureusement pas possible à appliquer dans des structures ou il n'y a pas de RSSI ou de DSI.

c) Déploiement d'un Plan de Continuité d'Activité (PCA)

Il s'agit d'un outil essentiel pour anticiper et organiser le redémarrage des services en cas de crise cyber, avec des scénarios d'attaques types et des fiches réflexes. Cela permet aux collectivités touchées de poursuivre leur activité en mode sécurisé ou parfois dégradé. Il évite ainsi une rupture totale de service.

4.3 Sensibilisation et formation des agents

La dimension humaine est centrale : **plus de 90 % des attaques réussies impliquent une erreur humaine** (Clusif, 2024).

a) Formation des agents aux outils numériques

D'après l'étude **du CNFPT, 50% des agents de catégorie A et 27% des agents de catégorie B et C** se disent autonomes avec l'outil informatique. Ce qui signifie que **65%** des agents se disent **ne pas être autonomes avec le numérique**.
Par ailleurs, chaque agent dispose d'au moins **une adresse électronique professionnelle**, associée à **un identifiant et un mot de passe**. Ces éléments constituent bien souvent la **première porte d'entrée des cyberattaques**, soulignant ainsi l'importance de la formation à la cybersécurité au sein des collectivités d'abord, et de la sensibilisation à celle-ci dans un second temps.

b) Sensibilisation continue des agents

Des campagnes de sensibilisation régulières doivent cibler les agents administratifs, élus, mais aussi les prestataires. Ces sessions doivent aborder :

- Les risques de phishing
- Les bonnes pratiques de mot de passe
- La réaction face à un incident

c) Simulations de crise et exercices de phishing

Certaines collectivités comme **Strasbourg**, **Angers ainsi que la Région Nouvelle-Aquitaine et Occitanie** ont mis en place des tests internes d'hameçonnage simulé, avec d'excellents retours. Ces campagnes permettent de corriger les comportements à risque.

d) Formation des Directeurs (DGS, DGA), Elus et des responsables de service.

Les cadres dirigeants doivent être capables de **comprendre les enjeux techniques** et de piloter une réponse rapide en cas d'attaque avec la mise en place de cellules de crise. Sans oublier la dimension humaine, en permettant au responsable de services de pourvoir apporter une réponse bienveillante et un soutien aux victimes ayant été impliquées dans l'attaque. Des modules de formation dédiés sont proposés par le **CNFPT**, l'**INSP**, ou **l'ANSSI**.

4.4 Coopération intercollectivités et dispositifs nationaux

a) Mutualisation régionale des moyens

Certaines régions ou intercommunalités développent des **CERT mutualisés** (équipes d'intervention en cybersécurité). Exemple : le **Campus Cyber Nouvelle-Aquitaine** ou **CyberOCC** (Occitanie) accompagnent les collectivités dans :

- La détection des failles
- L'assistance à la réponse à incident
- L'audit de conformité RGPD.

b) Soutien de l'État et de l'ANSSI

Plusieurs dispositifs publics visent à renforcer la sécurité locale :

- Le **volet cybersécurité du plan France Relance** (2021-2023) a permis à plus de 1 000 collectivités de financer des audits et matériels.
- Le **Fonds interministériel pour la prévention de la délinquance (FIPD)** subventionne les diagnostics cyber.
- La **plateforme cybermalveillance.gouv.fr** propose des outils gratuits de sensibilisation.

c) Application du cadre juridique européen : la directive NIS2

À partir de 2025, certaines collectivités (villes de plus de 50 000 habitants, conseils régionaux, ARS) seront **soumises à des obligations renforcées de cybersécurité** :

- Notification des incidents majeurs sous 24 h.
- Audit de conformité réguliers.
- Responsabilité pénale en cas de négligence.

4.5 Vers une culture cyber territoriale

Au-delà des outils techniques, l'objectif à long terme est l'instauration d'une **véritable culture de la sécurité numérique** dans les collectivités :

- Inclure les enjeux cyber dans les projets de territoire (transition numérique).
- Créer des **réseaux de pairs** entre collectivités (ex. : réseau "Les Territoriaux du numérique").
- Intégrer la cybersécurité comme **critère de gouvernance publique locale**, au même titre que l'environnement ou l'accessibilité.
- **Formation des agents** aux outils du numérique.

5. Conclusion

L'analyse menée met en lumière l'exposition croissante des collectivités territoriales françaises aux cyberattaques, dans un contexte de transformation numérique rapide et de montée en puissance des

menaces numériques globalisées. Si les rançongiciels constituent la forme d'attaque la plus visible et destructrice, d'autres vecteurs, comme le phishing, les intrusions silencieuses ou les défigurations idéologiques participent également à la fragilisation des systèmes d'information locaux.

La vulnérabilité des collectivités tient à des facteurs multiples : hétérogénéité des infrastructures, sous-dotation en ressources humaines et financières, manque de formation des agents, obsolescence des systèmes, manque de gouvernance cyber structurée. Or, les conséquences dépassent largement le périmètre informatique : elles affectent la continuité des services publics, la confiance des usagers, la responsabilité juridique des élus, et plus largement, la stabilité de l'action publique locale.

Face à cela, plusieurs dynamiques positives sont à souligner : multiplication des audits, soutien renforcé de l'État via des dispositifs comme France Relance, développement des CSIRT régionaux, émergence de démarches mutualisées entre collectivités. La transposition imminente de la directive européenne NIS2 constitue également une opportunité pour renforcer le cadre normatif et la responsabilisation des entités locales.

Néanmoins, les efforts actuels restent encore trop ponctuels ou centrés sur les grandes collectivités. Une véritable **culture cyber territoriale** reste à construire, fondée sur la prévention, la coopération intercollectivités, la montée en compétences internes et l'intégration de la cybersécurité dans tous les projets numériques. Il ne s'agit plus seulement de se défendre contre des attaques isolées mais d'**adopter une posture de résilience numérique systémique**, à l'échelle des territoires.

Perspectives de recherche

Pour approfondir ces enjeux, plusieurs axes de recherche complémentaires mériteraient également d'être explorés :

- Études empiriques longitudinales sur l'évolution de la maturité cyber des collectivités depuis la crise COVID ;
- Analyse comparative entre collectivités françaises et européennes soumises aux mêmes obligations NIS2 ;
- Évaluation de l'efficacité des dispositifs mutualisés régionaux (CSIRT, groupements DSI, centrales d'achat cyber) ;
- Enquête sur la perception du risque cyber par les élus et décideurs territoriaux.
- Enquête auprès des agents des collectivités territoriales afin d'estimer leurs niveaux et besoins réels en formation cyber et outils numérique.

Ces pistes permettraient de mieux outiller la décision publique et d'accompagner la montée en compétence du secteur public local face à un défi qui, désormais, engage directement la souveraineté numérique territoriale.

Bibliographie

- *Cybermalveillance.gouv.fr / OpinionWay (2024), Baromètre de la maturité cyber des collectivités françaises (cyber.corsica, cybermalveillance.gouv.fr) consulté le 25/05/2025.*
- *ANSSI (2025), Rapport d'activité 2024 : 218 incidents signalés, 25 rançongiciels (maire-info.com) consulté le 25/05/2025.*
- *CNIL / Cybermalveillance.gouv.fr (2022), Guide obligations cybersécu collectivités (cnil.fr) consulté le 25/05/2025.*
- *Cas locaux (Marseille, Sartrouville, Lille…) : Lockself (blog.lockself.com) consulté le 25/05/2025.*
- *CSIRT CyberCorsica (2025), Synthèse des menaces territoriales. consulté le 25/05/2025.*