N° 283

SÉNAT

SESSION ORDINAIRE DE 2021-2022

Enregistré à la Présidence du Sénat le 9 décembre 2021

RAPPORT D'INFORMATION

FAIT

au nom de la délégation aux collectivités territoriales et à la décentralisation (1) et de la délégation aux entreprises (2) relatif à la **cybersécurité** *au sein des* **collectivités territoriales**,

Par M. Serge BABARY et Mme Françoise GATEL,

Sénateurs

(1) Cette délégation est composée de : Mme Françoise Gatel, *présidente* ; MM. Rémy Pointereau, Guy Benarroche, Jean-Pierre Corbisez, Bernard Delcros, Mmes Corinne Féret, Michelle Gréaume, MM. Charles Guené, Éric Kerrouche, Antoine Lefèvre, Mme Patricia Schillinger, M. Pierre-Jean Verzelen, *vice-présidents* ; M. François Bonhomme, Mme Agnès Canayer, M. Franck Montaugé, *secrétaires* ; Mmes Nadine Bellurot, Céline Brulin, MM. Bernard Buis, Laurent Burgoa, Thierry Cozic, Mmes Chantal Deseyne, Mme Catherine Di Folco, MM. Thomas Dossus, Jérôme Durain, Mme Dominique Estrosi Sassone, MM. Fabien Genet, Hervé Gillet, Jean-Michel Houllegatte, Mmes Muriel Jourda, Sonia de La Provôté, Christine Lavarde, Anne-Catherine Loisier, MM. Pascal Martin, Hervé Maurey, Franck Menonville, Jean-Marie Mizzon, Philippe Mouiller, Olivier Paccaud, Philippe Pemezec, Didier Rambaud, Mme Sylvie Robert, MM. Jean-Yves Roux, Laurent Somon, Lucien Stanzione, Cédric Vial, Jean Pierre Vogel.

(2) Cette délégation est composée de : M. Serge Babary, *président* ; M. Stéphane Artano, Mmes Martine Berthet, Florence Blatrix Contat, MM. Gilbert Bouchet, Emmanuel Capus, Mme Anne Chain-Larché, MM. Gilbert-Luc Devinaz, Thomas Dossus, Fabien Gay, Jacques Le Nay, Dominique Théophile, *vice-présidents* ; MM. Rémi Cardon, Jean Hingray, Sébastien Meurant, Vincent Segouin, *secrétaires* ; Mmes Cathy Apourceau-Poly, Annick Billon, Nicole Bonnefoy, MM. Michel Canevet, Daniel Chasseing, Alain Chatillon, Mme Marie-Christine Chauvin, M. Pierre Cuypers, Mme Jacky Deromedi, M. Alain Duffourg, Mme Pascale Gruny, MM. Christian Klinger, Daniel Laurent, Martin Lévrier, Didier Mandelli, Jean-Pierre Moga, Albéric de Montgolfier, Claude Nougein, Mme Guylène Pantel, MM. Georges Patient, Sebastien Pla, Mmes Émilienne Poumirol, Frédérique Puissat, MM. Christian Redon-Sarrazy, Olivier Rietmann, Daniel Salmon.

S O M M A I R E

Pages

LISTE DES PRINCIPALES CONCLUSIONS TIRÉES DE LA TABLE RONDE DU 28 OCTOBRE 2021 SUR « *LES COLLECTIVITÉS TERRITORIALES FACE AU DÉFI DE LA CYBERSÉCURITÉ* »

1. **Sensibiliser les élus** communaux et intercommunaux ainsi que leurs services aux enjeux de la cybersécurité.

Un travail d'information doit être mené en particulier, sur :

- **l'ampleur des menaces numériques**, lesquelles sont accentuées par trois facteurs :
  - ✓ le développement des services publics numériques et des territoires connectés ;
  - ✓ le recours grandissant au télétravail dans la fonction publique territoriale ;
  - ✓ la formation insuffisante des élus et des agents.

- **l'existence de lourdes conséquences** en cas d'attaques :
  - ✓ dysfonctionnement des services publics locaux (mise à l'arrêt de parkings, de piscines, de musées, de stations d'épuration, graves perturbations de l'état civil empêchant, par exemple, la délivrance de permis d'inhumer pendant une semaine…) ;
  - ✓ perte irrémédiable de données informatiques, de ressources humaines et financières ;
  - ✓ conséquences financières : mise au chômage technique d'employés de mairie, pertes de ressources liées à la mise à l'arrêt de certains services payants, éventuel paiement de rançons…
  - ✓ conséquences humaines : altération du lien de confiance avec les citoyens et impact psychologique sur les agents territoriaux.

2. **Appliquer le principe de subsidiarité en matière de politique de sécurité numérique**.

Deux critères doivent être pris en compte pour apprécier le niveau **pertinent** d'intervention : la soutenabilité financière et la technicité requise. Ce principe permettrait aux petites collectivités, identifiées comme des « *maillons faibles* », de bénéficier, par l'effet de la **mutualisation**, d'une protection numérique renforcée. L'échelle de pertinence doit être appréciée *in concreto* selon les réalités territoriales. Il peut s'agir du niveau soit intercommunal soit départemental. Cette recommandation suppose toutefois de lever les freins psychologiques tenant à la sensibilité des données des communes et à la crainte corrélative du transfert de ces dernières.

3. Mettre en place des **plans ou des procédures de continuité et de reprise d'activité** en cas de survenance d'une crise d'origine numérique (mesures

d’urgence à prendre, prestataires à contacter, notification aux autorités publiques telles que la CNIL et l’ANSSI…).

4. **Revaloriser les fonctions de RSSI (responsable de la sécurité des systèmes d'information) dans les collectivités** d’une certaine taille.

   Il d’en faire un véritable « *directeur de la Sécurité numérique* » dont les fonctions ne doivent pas perçues comme uniquement techniques. Le caractère stratégique de cette fonction doit se traduire dans la rémunération proposée ainsi que dans l’organigramme des services (rattachement à la Direction générale par exemple).

AVANT-PROPOS

La cybercriminalité se banalise pour quatre motifs :

1. **La numérisation de l'économie et des services publics,** accélérée avec le confinement lié au développement du télétravail et le déploiement de la fibre ;
2. **La professionnalisation de la cybercriminalité**, facilitée par sa « plateformisation », son industrialisation, et le développement des cryptomonnaies ;
3. **La difficulté de la prévention et de la répression**, lesquelles nécessitent à la fois la prise de conscience de tous et une coopération internationale efficiente ;
4. **L'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique** dont les collectivités territoriales, leurs établissements publics et les établissements de santé, sont soit les cibles soit les victimes collatérales.

Les collectivités territoriales sont responsables de la sécurité des données qu'elles traitent et de leurs services numériques vis-à-vis des autorités et des citoyens. Les normes de cybersécurité et de protection des données instaurent une logique de prévention des risques. Elles impliquent une mise en conformité permanente et dynamique. Les collectivités doivent donc garantir à leurs usagers un niveau optimal de protection.

Le rapport de la délégation sénatoriale aux entreprises établi par Sébastien Meurant et Rémi Cardon[1] a souligné l'ampleur du risque cyber pour les entreprises, en particulier les PME, mais aussi pour toutes les organisations territoriales.

Ce sujet a été à nouveau largement évoqué lors de la 5ème Journée des entreprises organisée au Sénat le 21 octobre 2021 par la délégation aux entreprises, puis lors de la table-ronde conduite avec la délégation aux collectivités territoriales et à la décentralisation, le 28 octobre.

Suite à ces travaux, il est apparu que **les entités publiques**, à savoir les collectivités territoriales, établissements de santé et établissements publics, **sont également concernées par cette menace qui peut paralyser le fonctionnement du service public.** La réponse appropriée pour réduire cette menace nécessite une synergie des actions publiques et privées.

---

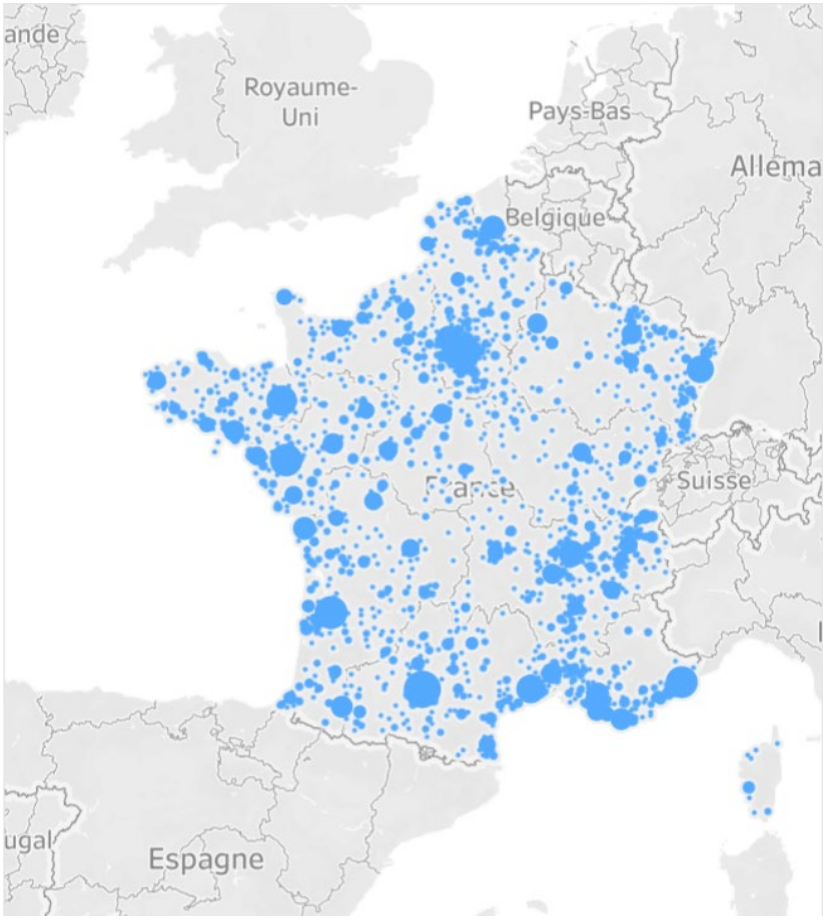
[1] *« La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ? », rapport d'information de MM. Sébastien MEURANT et Rémi CARDON, fait au nom de la délégation aux entreprises n° 678 (2020-2021) - 10 juin 2021.*

I. UNE PRISE DE CONSCIENCE TARDIVE ET INSUFFISANTE DES CYBERMENACES

En 2020, près de 30 % des collectivités territoriales ont été victimes d'une attaque au rançongiciel[1] selon une étude du Clusif[2]. En effet, cette même année a vu le nombre de cyberattaques contre des collectivités territoriales **augmenter de 50 %** par rapport à 2019[3].

Comme l'indique cette carte, les collectivités de toutes tailles et sur tout le territoire sont concernées :

LOCALISATION DES VICTIMES



1 *Un rançongiciel (ou ransomware) est un logiciel malveillant ou virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. Certaines de ces attaques visent parfois simplement à endommager le système de la victime pour lui faire* ***subir des pertes d'exploitation et porter atteinte à son image****.*

2 *https://clusif.fr/newspaper/le-risque-associe-aux-rancongiciels-demeure-sous-evalue-dans-les-collectivites-territoriales-clusif/*
Le Clusif est l'association de référence de la sécurité du numérique en France.

3 *https://www.lesechos.fr/tech-medias/hightech/flambee-dattaques-informatiques-contre-les-mairies-en-france-1284537*

Source : Cybermalveillance.gouv.fr, 2021

En mai 2020, Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'est déclaré « *inquiet* »[1] pour la cybersécurité des collectivités territoriales.

Pourtant, la cybersécurité était, en 2018, loin d'être une préoccupation centrale des collectivités territoriales. Selon un sondage Ifop[2] pour l'Observatoire des Politiques Publiques, en janvier 2020 encore seuls 33 % des fonctionnaires territoriaux interrogés déclaraient que leur organisation avait mis en place un programme de cybersécurité. Le **manque de budget et de personnes qualifiées** justifie en partie les difficultés des collectivités territoriales en matière de cyberprotection de leurs outils et données numériques.

Les élus locaux prennent désormais, et de manière croissante, la pleine mesure de ce risque. Les associations d'élus accompagnent la prise de conscience des collectivités territoriales, qui demeure inégale sur le territoire.

Pour favoriser cette prise de conscience, l'Association des maires de France (AMF) a édité en novembre 2020 un guide intitulé « *Cybersécurité : toutes les communes et les intercommunalités sont concernées* ».

Si ce guide propose une trentaine de recommandations et de bonnes pratiques en matière de sécurité numérique, sa finalité première est avant tout de susciter un questionnement pour les élus. La réflexion ainsi ouverte doit permettre de répondre à cette simple question : **ma commune ou mon intercommunalité est-elle bien préparée face aux risques numériques ?** Quelle que soit la réponse, ce guide a vocation à apporter des conseils pratiques et à proposer les axes prioritaires à renforcer, sinon à développer. S'il n'est pas technique, ce guide propose cependant les briques nécessaires à l'élaboration d'une gouvernance qui devient dès lors garante de l'établissement d'un cadre de confiance numérique. La vocation de ce guide est bien de renforcer la prise de conscience de chacun, élus, mais aussi cadres et agents territoriaux. Elle est aussi de mettre l'accent sur des points d'action très concrets puis d'inviter à partager et construire tous ensemble la sécurité numérique collective que chaque citoyen attend de son territoire.

Source : introduction du guide « Cybersécurité : toutes les communes et les intercommunalités sont concernées ».

---

[1] *Face aux membres de la commission de la défense nationale et des forces armées de l'Assemblée nationale : https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def1920054_compte-rendu.pdf*

[2] *https://2020.forum-fic.com/Data/ElFinder/s23/PDF/20200206-note-cyber-et-territoires.pdf?_t=1581012131*

Faute de temps mais également de compétences et de ressources humaines qualifiées, les petites communes se contentent parfois d'installer ponctuellement un anti-virus, alors que la cybersécurité doit être mise à jour en permanence. Or, la pénurie de compétences est telle que l'ANSSI a lancé un « observatoire des métiers de la cybersécurité » afin d'aider les acteurs concernés dans leur politique de recrutement et de formation. Dans ce contexte, la mutualisation au plus près des collectivités concernées s'avère être un choix judicieux pour mettre en commun les efforts, affronter les pénuries de professionnels qualifiés et ainsi mettre en place **une protection collective**.

II. UN DISPOSITIF DE CYBERPROTECTION PUBLIQUE DÉVELOPPÉ MAIS PEU ACCESSIBLE AUX PETITES COLLECTIVITÉS TERRITORIALES

A. UN BOUCLIER EFFICACE POUR LES CYBERATTAQUES CONCERNANT LES ENTITÉS DE GRANDE TAILLE

Il s'articule autour de **l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** et d'un **réseau de CERT (*Computer Emergency Response Team*)**, organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT sont des centres d'alerte et de réaction aux attaques informatiques, dont les informations sont accessibles à tous.

L'objectif du **volet cybersécurité de France Relance**, lancé en septembre 2020 et dont le pilotage a été confié à l'ANSSI, doit renforcer la sécurité des administrations, des collectivités, des établissements de santé et autres organismes publics, tout en dynamisant l'écosystème industriel français.

Doté d'un fonds de **136 millions d'euros**, il comprend :

- un parcours de cybersécurité ayant pour objectif de renforcer la sécurité des systèmes d'information des bénéficiaires en proposant un pré-diagnostic et un accompagnement par des prestataires compétents, de la maîtrise d'ouvrage jusqu'à la mise en œuvre ;

- des appels à projets, pour certaines collectivités territoriales dont le niveau de cybersécurité est suffisamment mature et le besoin assez clair pour que le projet soit mené hors du cadre des « Parcours de cybersécurité ». Basés sur le cofinancement et destinés à sécuriser des systèmes d'information existants, ces projets peuvent être des prestations d'audit, d'analyse de risque, d'acquisition et de déploiement de produits... ;

- le réseau des CSIRT régionaux (*Computer Security Incident Response Team*), centres de réponse aux incidents cyber au profit des entités implantées sur le territoire régional, devra traiter des demandes d'assistance des acteurs de taille intermédiaire, dont les collectivités territoriales, et les mettre en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

B. LA PRÉVENTION ET L'ASSISTANCE AUX VICTIMES

Depuis 2017, la plateforme Cybermalveillance.gouv.fr, du GIP ACYMA, dispositif national de **sensibilisation, prévention et assistance** aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales, est porté par un **partenariat public-privé**. Outre l'ANSSI et les principaux ministères, cette plateforme rassemble de

nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs de logiciels…

Face à la recrudescence des cyberattaques contre les collectivités territoriales, Cybermalveillance.gouv.fr a créé un groupe de travail dédié à ce public composé de l'ANSSI, l'AVICCA, la Banque des Territoires, le CoTer Numérique et Déclic, et lancé un **programme de sensibilisation** à destination des élus.

Il comporte **trois étapes** :

1. **Étape une : « Menaces et réflexes essentiels pour la sécurité numérique des collectivités »**

Cybermalveillance.gouv.fr répond aux questions de deux maires sur les **principales menaces numériques rencontrées par les collectivités et leurs conséquences,** en apportant des conseils sur les **premiers gestes essentiels à adopter en sécurité numérique**.

La première menace à laquelle les collectivités territoriales et leurs établissements publics sont exposés est **l'hameçonnage**, mail frauduleux destinés à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance, qui représente près d'un quart des demandes d'assistance du dispositif Cybermalveillance.gouv.fr, suivi du **piratage de comptes en ligne** et des **rançongiciels**.

2. **Étape deux : « Vigilance face aux cyberattaques : les collectivités sont toutes concernées ! »**

Le site publie deux **témoignages de communes victimes de différentes formes de cyberattaques**, suivis de **conseils** pour permettre aux collectivités de mieux s'armer et anticiper les risques.

a) Témoignage d'une commune de 20 000 habitants – attaque par rançongiciel

« Durant un week-end en plein été, le réseau informatique de notre commune de 20 000 habitants a été attaqué par un rançongiciel. Les pirates auraient réussi à pénétrer dans notre réseau par nos accès ouverts pour le télétravail. Une grande partie de nos informations était bloquée et les services municipaux se sont retrouvés à l'arrêt. ***Les pirates réclamaient une rançon de plusieurs dizaines de milliers d'euros et menaçaient de publier des informations qu'ils nous auraient volées ce qui peut porter préjudice à nos administrés****. Nous avons refusé de payer et déposé plainte, mais il a fallu plusieurs semaines pour revenir à un fonctionnement à peu près normal. Heureusement toutes nos sauvegardes n'ont*

pas été détruites ce qui nous a permis de récupérer une partie de nos données. Nous ne pensions pas être un jour la cible d'une telle attaque. ***Cela nous a servi de leçon et nous allons maintenant devoir revoir notre niveau de sécurité informatique*** *».*

b) Témoignage d'une commune de 5 000 habitants – attaque par défiguration1 de site Internet

« Un week-end, nous avons été informés par des administrés que le site Internet de notre commune de 5 000 habitants avait été modifié par des pirates et affichait des messages insultants. Nous avons déposé plainte et dû faire intervenir un prestataire spécialisé car ***nous ne trouvions pas la cause de cette attaque qui revenait en permanence****. Ces spécialistes ont découvert que* ***les pirates avaient pris le contrôle complet de notre site et volé tous nos mots de passe****. Ils auraient réussi à s'introduire sur le site par une faille de sécurité dans un de ses modules qui n'avait pas été mis à jour depuis plus de 5 ans. »*

c) Témoignages à l'occasion de la table ronde organisée le 28 octobre 2021

La **table ronde** organisée au Sénat le 28 octobre 2021 met en exergue la **gravité des conséquences** en cas de cyber-attaques ciblant des collectivités territoriales.

Ainsi, M. Cyril Bras, Vice-président de l'Institut pour la cybersécurité et la résilience des territoires, témoigne : *« À Oloron Sainte-Marie, la station d'épuration a été impactée par une cyberattaque ».*

De même, Mme Marie Nedellec, Adjointe au Maire de La Rochelle illustre la situation : *« La cyberattaque ne permettait plus d'utiliser les* ***parkings souterrains*** *de la ville alors que nous étions en pleine période de festivité. En effet, les barrières des parkings sont gérées de manière informatique par le système de la commune de la Rochelle. Le service d'état civil ne fonctionnait plus. Les ressources humaines étaient bloquées.* ***Nous ne pouvions même plus inhumer durant une semaine des personnes dans les cimetières de La Rochelle.****". (…). Cette attaque nous a mis en difficulté en tant que collectivité qui a dû travailler au papier et au crayon durant quatre semaines, et dans la relation aux citoyens en diminuant leur confiance vis-à-vis de l'équipe municipale. (…)* « *Nous avons enregistré des pertes financières étant donné que la piscine, les musées et les parkings n'étaient plus accessibles le temps de restaurer le système ».*

Enfin, M. Alexandre Ouzille, Premier-adjoint au Maire de Villers-Saint-Paul relève : *« Nous n'étions pas protégés contre ce type d'attaque et nous avons perdu l'ensemble des données informatiques, de ressources humaines et financières ».*

---

[1] *La défiguration est le* ***signe visible qu'un site internet a été attaqué*** *et que le cybercriminel en a obtenu les droits lui permettant d'en modifier le contenu. En plus du risque de* ***vol de données*** *personnelles / bancaires,* ***ce type d'attaque peut porter atteinte à l'image de la collectivité*** *auprès des citoyens.*

3. Étape trois : Sensibilisation aux risques numériques : les collectivités se mobilisent

Sensibiliser est à la portée de tous, il existe une multitude d'actions possibles en fonction de ses moyens et de sa maturité sur le sujet. Ces actions sont répertoriées sur le site cybermalveillance.gouv.fr :

- Vidéos de sensibilisation sur les risques numériques
- Campagne de sensibilisation inter-régions sur la cybersécurité
- Supports pour résumer les premiers gestes en cas d'attaque
- I.M.M.U.N.I.T.É.Cyber : questionnaire pour sensibiliser les élus à la cybersécurité. L'évaluation proposée par ce questionnaire repose sur dix questions simples, pour permettre à chaque élu de mesurer lui-même le niveau de cyberprotection mis en place au sein de sa collectivité. Le formulaire d'évaluation a été adressé par l'AMF à ses adhérents début septembre 2021.

Une *newsletter* permet aux élu(e)s de se tenir informé(e)s de l'actualité de la cybermalveillance et des nouvelles menaces.

Plusieurs collectivités ont entrepris des initiatives en matière de sensibilisation, soit qu'elles aient participé à la table ronde au Sénat le 28 octobre dernier, soit qu'elles soient citées sur le site *cybermalveillance.gouv.fr* :

a) Témoignage de la commune de Longueil Sainte Marie (60)

« L'actualité récente a montré qu'une prise de conscience des collectivités locales face aux enjeux de la cybersécurité était nécessaire. Dans ce contexte, la mairie de Longueil Sainte Marie (60) a souhaité engager des actions pour connaître, dans un premier temps, son niveau de sécurité, puis dans un second temps, mettre en place les mesures correctives nécessaires.

Accompagnés par l'Association pour le développement et l'innovation numérique des collectivités (Adico), nous avons préparé un dossier d'homologation au RGS (Référentiel Général de Sécurité). Cette étude a permis de cartographier notre système d'information et de procéder à une analyse de risques sur l'ensemble de son périmètre. En disposant de cette vision globale, nous avons pu définir un plan d'action qui permet de réduire les risques. Concrètement, cela se traduit essentiellement par de la sensibilisation et nous envisageons notamment de réaliser des campagnes de faux mails d'hameçonnage afin d'accroître la vigilance des agents et des élus.

Au terme de cette étude, un arrêté d'homologation a été pris. À l'instar des démarches menées dans le cadre de notre mise en conformité au RGPD, cette décision représente un engagement éthique auprès de nos administrés. À l'entrée de

la mairie, un autocollant est même affiché pour que les usagers puissent facilement comprendre qu'ils entrent dans un environnement de confiance numérique. »

b) Témoignage de la ville de La Rochelle (17)

« L'agglomération de la Rochelle, dans le cadre de ses services mutualisés travaille depuis plusieurs années à l'amélioration continue de sa cybersécurité.

Ainsi, une charte à destination de la communauté d'agglomération et de la ville de La Rochelle est en cours de rédaction à destination de tous les acteurs utilisant les Systèmes d'Information (élus, agents, personnel non permanent…) pour protéger les valeurs de nos collectivités : la disponibilité et la qualité du service public, le respect des obligations légales, la confidentialité et l'intégrité des données sensibles, la protection des investissements, la valorisation de l'image et la préservation de l'environnement.

De plus, nous mènerons des campagnes de sensibilisation pour présenter la charte et ses bonnes pratiques à l'ensemble de nos collaborateurs.

Nous envisageons également de créer un parcours de sensibilisation pour les nouveaux arrivants d'une demi-journée autour de questions très pragmatiques : Où est-ce que je dois stocker mes données pour qu'elles soient sauvegardées ? Pourquoi est-il primordial d'éteindre ses équipements le soir ? Comment je peux déclarer un incident ? Et donner des conseils sur la gestion des mots de passe, les mails malveillants, les usages pro-perso, la protection de la vie privée, etc.

Enfin, il nous semble important de former spécifiquement les acteurs manipulant des données dites « sensibles » sur une journée complète avec des exercices et une évaluation finale. »

c) Témoignage de la ville de Vannes (56)

« Il ne faut pas perdre de vue que 80 % des risques cyber sont liés à l'humain et que 90 % des menaces proviennent d'un mail frauduleux, technique appelée hameçonnage (phishing en anglais). Face à ces constats, nous avons décidé de former en ligne tous nos agents et élus pour leur apprendre à déjouer les pièges des e-mails malveillants. Puis, notre responsable de la sécurité des systèmes d'information (RSSI) a lancé une campagne intensive de faux mails d'hameçonnage sans information préalable. Le résultat : 23 % des agents ont manqué de vigilance et cliqué. Nous avons décidé d'inscrire la campagne dans la durée. Et les résultats sont très encourageants ! Le taux de clics a considérablement baissé, de 23 % à 6 % en un an. C'est une très bonne nouvelle pour la collectivité. »

d) Témoignage de la commune de Tillières-sur-Avre (27)

« Même nos petites communes peuvent être victimes de cybermalveillance, comme le vol de données, le piratage avec demande de rançon, etc. Faire connaître la plateforme de prévention et d'assistance Cybermalveillance.gouv.fr au plus grand nombre est indispensable afin que les agents des collectivités sachent vers qui se tourner en cas de cyberattaque. De plus, la sensibilisation aux bonnes pratiques en

matière de sécurité numérique avec l'affichage de conseils a permis d'initier au sujet en interne et susciter des questionnements. »

e) Témoignage de Toulouse Métropole (31)

« Lors de l'attaque des sites institutionnels de la ville de Toulouse en mai dernier, nous avons dû mettre en place en urgence une cellule de gestion de crise. Fin 2020, la vague d'attaques EMOTET ne nous a pas épargnés, cependant, nous étions davantage préparés. Notre partenaire, Orange CyberDefense (OCD) nous a accompagnés pendant une quinzaine de jours dans l'organisation, les prises de décisions et le management des opérations (techniques, communication, etc.). Ce retour d'expérience nous a permis de consolider notre dispositif et d'identifier les points à améliorer. En parallèle, nous avons poursuivi les actions de remédiation et d'amélioration de nos infrastructures, de nos outils de détection et d'analyse. Nous sommes actuellement en train de réaliser un guide sur la gestion de crise au sein de la collectivité et nous allons organiser prochainement un exercice de gestion de crise cyber pour entraîner nos agents et nous préparer. »

f) Témoignage de Rochefort Habitat Océan (17)

« Suite au renouvellement de la flotte informatique (postes et serveurs) début 2016, l'Office a souhaité réaliser un audit de sécurité afin de renforcer le pilotage du Système d'Information (SI). Avec le soutien de SOLURIS, une analyse de risques a été réalisée pour déterminer la criticité des applications métiers et identifier les vulnérabilités du système d'information pour pouvoir apprécier les risques et les traiter si nécessaire. Dans ce cadre, le Référentiel Général de Sécurité (RGS) a été mis en œuvre afin d'appliquer les bonnes pratiques de gestion de la sécurité pour le Système d'Information.

La sensibilisation du personnel est apparue comme un axe essentiel afin que chaque utilisateur prenne conscience des enjeux en matière de sécurité et de vie privée. Plusieurs actions sont menées en ce sens.

Afin d'accompagner la mise en place d'une charte informatique opposable, un travail impliquant les collaborateurs a été engagé en 2018/2019 sur les pratiques essentielles de sécurité à mettre en œuvre au quotidien. Ce travail a permis d'élaborer une affiche distribuée et expliquée au personnel lors d'un petit déjeuner de travail. Ce document est diffusé à chaque nouvel arrivant lors de sa prise de poste.

Chaque année, des actions de sensibilisation sont menées. Chaque trimestre, une newsletter est diffusée pour rappeler une bonne pratique ou attirer l'attention sur un risque informatique. Par exemple en septembre 2020, la newsletter « Les mots de passe, c'est un peu comme les brosses à dents » a permis de faire un rappel des règles relatives à la gestion des mots de passe.

Annuellement, une réunion de sensibilisation est organisée avec le soutien de SOLURIS. En 2020, les agents de proximité et les responsables d'immeubles qui venaient d'être dotés de téléphones portables ont pu être sensibilisés aux cybermenaces et prendre connaissance des pratiques de sécurité à mettre en œuvre sur les smartphones.

Un groupe de travail « sécurité informatique » composé de 4 collaborateurs et du référent sécurité de l'Office a été créé en 2017. Ce groupe de travail suit les plans d'actions annuels portant sur la sécurité informatique et la protection des données, rédige les newsletters et s'assure de l'acceptabilité et de la mise en œuvre des règles de sécurité auprès du personnel. »

C. L'ENQUÊTE ET LA RÉPRESSION : UNE SPÉCIALISATION CROISSANTE DE LA CYBERGENDARMERIE ET DE L'AUTORITÉ JUDICIAIRE

Le centre de lutte contre les criminalités numériques (C3N) est chargé d'assurer le pilotage et l'appui spécialisé de l'action de la gendarmerie contre la cybercriminalité et les criminalités numériques, de mener ou coordonner les investigations d'ampleur nationale ayant trait à la cybercriminalité, et de réaliser une surveillance permanente de l'Internet, pour y détecter et collecter les preuves des infractions qui peuvent y être commises.

Le réseau d'enquêteurs spécialisés de la Gendarmerie forme une chaîne de 7 000 gendarmes qui seront 10 000 en 2022. Cette montée en puissance s'est traduite par la création le 25 février 2021 du COMCyberGEND, ou Commandement de la gendarmerie dans le cyberespace.

La Cybergendarmerie développe également un rôle de prévention. Les membres des sections opérationnelles de lutte contre les cybermenaces (SOLC) installés au chef-lieu de chaque département, éventuellement accompagnés des référents sûreté, peuvent être sollicités via la brigade de gendarmerie territorialement compétente pour réaliser des opérations de prévention aux cybermenaces et notamment diffuser des conseils de prévention. Un militaire de la brigade territoriale peut utilement être associé à la rencontre. Suite à l'action la SOLC, et le cas échéant des référents sûreté, la commune concernée pourra ensuite s'orienter vers un prestataire de son choix afin de remédier aux difficultés révélées.

Sur le plan judiciaire, le rôle primordial est joué par le tribunal judiciaire de Paris qui bénéficie, depuis la loi du 3 juin 2016, d'une compétence nationale en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et crimes de sabotage informatique.

Il existe depuis 2015 une section du parquet de Paris dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes, aux effectifs toutefois modestes. Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment celle liée à la criminalité organisée.

EXAMEN EN DÉLÉGATIONS

Lors de sa réunion du 4 novembre 2021, la délégation aux entreprises a autorisé la publication du présent rapport.

Lors de sa réunion du 2 décembre 2021, la délégation aux collectivités territoriales a autorisé la publication du présent rapport.

COMPTE RENDU DE LA TABLE RONDE DU 28 OCTOBRE 2021

1. Retour d'expérience des collectivités territoriales – Audition de M. Richard Lizurey, adjoint au maire de Chartres, Mme Marie Nedellec, adjointe au maire de La Rochelle, M. Alexandre Ouzille, premier adjoint au maire de Villers-Saint-Paul

Mme Françoise Gatel, présidente. – Je vous remercie d'avoir répondu à cette invitation conjointe au titre de la délégation des collectivités territoriales. C'est un jumelage avec la délégation aux entreprises, et je salue mon collègue sénateur Serge Babary, qui a eu cette initiative d'engager une réflexion sur la cybersécurité dans les entreprises. Nous avons décidé d'élargir la réflexion sur la cybersécurité pour les collectivités territoriales. Je remercie le président Babary de nous permettre d'utiliser la matière et la réflexion conduite avec sa délégation pour l'adapter à nos collectivités.

Dans toutes les actions conduites en faveur des collectivités territoriales, la réponse qui paraît assez miraculeuse concerne le numérique, avec notamment la télémédecine et la numérisation des services publics aux habitants. Cette dimension est présentée comme un levier d'équité territoriale, avec la possibilité pour les territoires les plus éloignés de bénéficier de cet équilibre territorial auquel le Sénat est très attaché. Ce sujet nous préoccupe tellement que trois collègues de la délégation des collectivités territoriales, Anne-Catherine Loisier, Antoine Lefèvre et Jean-Yves Roux, ont été sollicités pour mener une mission d'information sur ce sujet. La préoccupation de la délégation consiste à recenser des sujets, et surtout valoriser toutes les bonnes pratiques pour aider les collectivités territoriales à trouver des solutions.

Le risque qui paraissait ne concerner que des entreprises est aujourd'hui une réalité pour les collectivités territoriales ou les établissements publics, notamment les hôpitaux ou les communes, y compris les plus petites. Il s'agit de déterminer le degré de conscience des collectivités territoriales vis-à-vis de ce danger qui constitue une réalité. Ensuite, il convient de se demander comment les collectivités territoriales s'emparent du sujet, et s'il y a un écart dans les pratiques des grandes et petites collectivités territoriales. Il ne s'agit pas uniquement d'un sujet technique, mais il faut mettre en place une gouvernance, c'est-à-dire une orientation politique de ce projet.

L'AMF et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ont conçu des guides sur la cybersécurité. Les élections municipales ont été chahutées par la crise sanitaire en 2020. Le sujet

n'est pas suffisamment porté par les collectivités territoriales. Vous avez beaucoup insisté, Monsieur Richard Lizurey, adjoint au Maire de Chartres, sur la question de la cybersécurité. L'objectif de nos deux tables rondes de 9 heures à 11 heures est d'échanger le plus possible sur ces sujets. Les participants à ces tables rondes assisteront à un retour d'expérience des collectivités territoriales.

M. Richard Lizurey, vous êtes vice-président de Chartres métropole spécialisé dans les questions de sécurité au niveau de la métropole. Mme Marie Nedellec, vous êtes adjointe au Maire de La Rochelle, et chargée des systèmes d'information. M. Ouzille, vous êtes premier adjoint de la ville de Villers-Saint-Paul dans l'Oise. M. Cyril Bras est vice-président de l'Institut pour la cybersécurité et la résilience des territoires. La Direction générale de la gendarmerie nationale est représentée par le général de division Marc Boget, que je salue. L'ANSSI est représentée par Mme Gwenaëlle Martinet, cheffe de projet France Relance. M. Jérôme Notin est le directeur général d'ACYMA.

Je transmets la parole à Monsieur Serge Babary en le remerciant des initiatives prises par sa délégation. Je salue également les représentants de l'AMF, de l'AMRF et de l'ADF qui assistent à la réunion par visioconférence.

M. Serge Babary, président. – Je vous remercie, Madame la présidente. J'ai rencontré certains d'entre vous lors de la réunion de la délégation sénatoriale aux entreprises de la semaine dernière. Je vous remercie d'être présents. La délégation aux entreprises a travaillé dès 2020 sur le sujet de la cybersécurité, au début de la crise. Les entreprises numérisées avaient un avantage sur les autres et il était urgent que la révolution numérique pénètre dans le monde des PME.

Nous nous sommes inquiétés de la flambée des cyberattaques qui nécessite de pouvoir conjuguer digitalisation et cybersécurité. Nous avons proposé à deux de nos collègues, Sébastien Meurant en visioconférence et Rémi Cardon qui est présent parmi nous, de réaliser un rapport sur la cybersécurité dans les TPE et PME qui a été adopté en juin 2021.

Après les milliers d'entreprises attaquées, des dizaines de cliniques et de collectivités territoriales ont été des proies très faciles, trop faciles, des cybercriminels. Une carte non exhaustive d'attaques sur des villes, hôpitaux, institutions, centres de secours, régions ou départements victimes de cyberattaques, a été communiquée aux participants à la table ronde.

Ce phénomène va non seulement durer, mais il va s'amplifier. La délégation aux entreprises a inscrit d'ailleurs ce sujet à l'agenda de sa cinquième journée consacrée aux entreprises, le 21 octobre dernier. Jérôme Notin, directeur du site cybermalveillance.gouv.fr, est intervenu devant près de 150 chefs d'entreprise et une trentaine de sénateurs. Je l'ai salué tout à l'heure.

Fédérer les énergies publiques et privées de la cybersécurité sera le défi du futur Campus Cyber qui devrait fonctionner au début de l'année 2022. J'ai prévu de visiter, avec mes collègues de la délégation, ce forum dès son ouverture.

Le Sénat représente les collectivités territoriales. Pour cette raison, j'ai proposé à Mme Gatel d'organiser conjointement cette table ronde destinée à sensibiliser nos collègues et les collectivités afin de prendre les mesures appropriées pour renforcer la cybersécurité. Un plan pour la cybersécurité a été annoncé le 18 février 2021 par le Président de la République. Les démonstrateurs territoriaux sont en train d'expérimenter de nouvelles chronologies pour les diffuser à tous les territoires. Cette démarche vertueuse est-elle suffisante ? Nous avons hâte de connaître l'amélioration de sa répartition. Notre collègue Vincent Segouin, secrétaire à la délégation aux entreprises, est très affuté sur ces questions.

Mme Françoise Gatel, présidente. **–** Nous commençons par le retour d'expérience des collectivités territoriales. Nous disposons de 50 minutes pour cette première table ronde, puis la parole sera donnée aux collègues qui le souhaitent et représentants d'associations d'élus, l'AMF, l'ADF et l'Association des maires ruraux de France. J'invite M. Richard Lizurey à livrer son témoignage.

M. Richard Lizurey, adjoint au maire de Chartres. **–** Tout d'abord, merci d'organiser cette matinée autour d'un sujet important dont il convient de s'occuper, et pour lequel il faut sensibiliser la totalité des structures locales. Le premier axe de mon intervention porte sur la difficulté de sensibiliser les élus et agents du service public. Cette situation n'est pas liée à un manque de volonté, mais de connaissance et de temps, parfois de budget, mais c'est extrêmement rare. La question des compétences et du temps est beaucoup plus importante.

Je souhaite prendre l'exemple de Chartres dont la métropole regroupe 66 communes et 140 000 habitants, à la diversité très importante. Je me suis attaché à faire le tour des communes dès mon élection. Celles que j'ai vues présentent les caractéristiques de petites communes dans lesquelles le maire exerce une profession. Le secrétaire de mairie travaille souvent à mi-temps quand il ou elle est présent, et n'a souvent pas de compétence en cybersécurité.

Le « mur administratif » est problématique étant donné que le maire est chargé de nombreuses tâches et responsabilités. Lorsque j'invite un maire de notre métropole à s'occuper de cybersécurité et lui demande ce qu'il prévoit de faire dans ce domaine, la première remarque est une surprise. La seconde remarque consiste à dire qu'un cousin a installé un antivirus sur les ordinateurs de la mairie. La cybersécurité va bien au-delà de l'installation d'un antivirus, mais cette dimension se heurte à la compétence des communes en termes de ressources humaines. Chartres Métropole n'a pas de

responsable des systèmes d'information, alors que ce sujet est important. La numérisation a progressé alors que la sécurité est restée en arrière. Un gouffre est constaté pour essayer de mettre la sécurité au niveau nécessaire du numérique.

Des zones blanches demeurent dans certaines communes. Il n'y a pas de réseau de 5G partout ou même de connexion Internet sur l'ensemble de notre territoire, alors que nous sommes à 80 kilomètres de Paris. Nous ne pouvons pas nous adresser à ces personnes de la même manière entre les petites communes et la ville-centre. Le département d'Eure-et-Loir a été cyber-attaqué deux fois au cours des dernières années.

Le premier constat est celui de la diversité, le second concerne le besoin d'accompagnement. Les élus sont conscients des difficultés, mais ils se demandent ce qu'ils peuvent faire. Chacun tente de faire du mieux possible. L'État a lancé un plan de cybersécurité, mais le ruissellement n'a pas lieu au niveau des territoires. Les initiatives partent du centre par la mise en place de politiques nécessaires, mais nous n'atteignons pas les petites communes. Il est intéressant de réfléchir à la mise en place de plateformes du type ENT (espace numérique du travail) pour les petites communes qui n'ont pas les moyens de rémunérer un responsable de la sécurité des systèmes d'information (RSSI) , tout en étant soucieux de la protection des administrés. Ces éléments n'ont pas vocation à rejoindre l'escarcelle de sociétés européennes ou étrangères. En effet, la souveraineté suppose de confier les données en France, étant donné que les élus sont responsables des données hébergées par les opérateurs.

Le constat est celui d'une diversité, d'une volonté de bien faire des élus, mais d'un manque de capacité. Deux postes de responsable de la sécurité des systèmes d'information ont été ouverts et ils n'attirent pas suffisamment de candidats. Les collectivités territoriales éprouvent des difficultés à recruter, étant donné que les collectivités territoriales ne proposent pas le même niveau de salaire que celui des grandes entreprises, salaires qui sont beaucoup plus élevés que ceux des collectivités territoriales. Il faut poursuivre les efforts pour amplifier le ruissellement.

Les grandes métropoles sont désormais équipées de matériel informatique et de systèmes de cybersécurité. Les petites communes sont en train d'être oubliées. La mise en place d'un système de cybersécurité national suppose de s'occuper également des petites communes. Je souhaite partager avec vous une volonté des élus, mais je déplore un manque d'accompagnement quotidien lié à un défaut de ressources humaines dans ce domaine.

Mme Françoise Gatel, **présidente**. **–** Je vous remercie pour cette présentation qui laisse penser que le plus petit peut constituer le maillon faible pour le plus gros. J'invite Mme Marie Nedellec, adjointe au maire de La Rochelle, à nous apporter son témoignage.

Mme Marie Nedellec, adjointe au maire de La Rochelle. – Je vous remercie, Madame la présidente, Monsieur le président, Mesdames et Messieurs les sénateurs. Nous avons été victimes d'une cyberattaque le 26 décembre 2020. La Rochelle compte 70 000 habitants, l'agglomération 170 000 habitants. Nous avons le même maire et président d'agglomération. La direction des services informatiques (DSI) est mutualisée. Je suis en charge de la DSI pour la ville et la communauté, et responsable de la transformation numérique étant donné que notre collectivité accompagne les acteurs vers une transformation responsable du numérique. Le service est composé de 40 personnes avec un délégué à la protection des données (DPO) et un RSSI pour les diriger.

Nous avons été victimes d'une cyberattaque entre 5 heures et 7 heures du matin le 26 décembre. L'attaque a mobilisé des équipes en interne et à l'extérieur étant donné que nous n'avions pas la possibilité d'intervenir aussi rapidement à cette date. La première anomalie a été découverte durant l'après-midi. Le service DSI ne détecte pas d'intrusion jusqu'à ce que la directrice générale des services ait constaté que des fichiers étaient inaccessibles. Nous nous sommes alors rendu compte de l'intrusion sur le serveur. Nous avons alors fait le choix de couper la liaison Internet et d'éteindre tous les serveurs de la ville et de l'agglomération.

Nous avons mis en place une cellule de crise composée de la directrice générale des services, du directeur général adjoint responsable DSI, et le dimanche le directeur de la DSI a été victime d'un problème cardiaque, qui l'a rendu indisponible. Nous allons faire preuve de malchance dans cette affaire. Je suis l'élue présente. Le maire président me délègue l'ensemble de cette mission. Nous intervenons à plusieurs sur cette cyberattaque. Le directeur des affaires juridiques, le responsable d'équipe infrastructure et réseau, le RSSI et le DPO sont également présents.

Les premières actions ont consisté à contacter l'ANSSI qui sera injoignable au départ. Nous portons plainte auprès de la gendarmerie qui nous accompagne et faisons une première déclaration auprès de la CNIL, conformément aux procédures légales. Nous vérifions l'état de nos systèmes d'information coupés d'Internet. Les serveurs de la communauté d'agglomération ne sont pas touchés, mais nous faisons le choix de ne pas les allumer durant trois jours, le temps de régler les premières failles du système.

Une bonne nouvelle est que la sauvegarde n'est pas touchée, ce qui nous rassure, même s'il faudra quatre semaines pour rétablir le service. La sauvegarde nous permet de rétablir progressivement une grande partie des services. Nous sommes rapidement conscients que nous n'y arriverons pas seuls. Sur les conseils de la gendarmerie, nous identifions un prestataire privé, étant donné que notre prestataire considère qu'il n'est pas capable d'intervenir suite à cette panne.

Nous allons être accompagnés par une société de cyberdéfense pour mettre en place des mesures de sécurité complémentaires et rétablir le système. Le groupe Orange nous accompagne. La première phase consiste à découvrir d'où vient l'attaque. Un fichier déposé dans nos serveurs indique qu'une rançon permettrait de recouvrer le site. Nous avons fait le choix d'œuvrer différemment. Nous sommes victimes d'une faille sur notre pare-feu qui a permis à l'attaquant de récupérer des identifiants, ce qui ouvre l'accès aux serveurs de la ville avec les identifiants. Nous avons cumulé une négligence sur le pare-feu, le VPN, le réseau privé virtuel, n'est pas assez sécurisé, mais les équipes de DSI avaient été mises à rude épreuve durant la crise sanitaire. Les services ont dû mobiliser toutes les équipes pour mettre en place du télétravail. Certaines négligences ont été identifiées, mais il n'a pu y être remédié, faute de moyens humains. En outre, les serveurs de Microsoft n'ont pas été mis à jour en temps voulu.

53 serveurs sur 150 et 42 postes de travail sur 1 000 ont été infectés par cette attaque. Concernant les données, sujet particulièrement sensible, les attaquants revendiquent leur attaque et font apparaître un certificat de mariage pour nous faire croire qu'ils ont piraté toutes nos données. Nous avons eu peur, en tant qu'élus, étant donné que ce certificat était une donnée personnelle. Cependant, Orange retrace le chemin de l'attaque et affirme que les attaquants n'ont pas prélevé de données personnelles dans les serveurs. Ils sont restés dans des postes d'agents, d'où ils ont récupéré le certificat de mariage qu'ils ont utilisé pour nous menacer. Cette situation nous a amenés à effectuer une nouvelle déclaration à la CNIL.

Ensuite, la restauration du système d'information a été progressive, ce qui a imposé de prioriser les services. La cyberattaque ne permettait plus d'utiliser les parkings souterrains de la ville alors que nous étions en pleine période de festivités. En effet, les barrières des parkings sont gérées de manière informatique par le système de la commune de la Rochelle. Le service d'état civil ne fonctionnait plus. Les ressources humaines étaient bloquées. Nous ne pouvions même plus inhumer durant une semaine des personnes dans les cimetières de La Rochelle.

La troisième phase d'action a porté sur la sécurisation d'urgence en vue de régler les failles de sécurité. La phase de sécurisation permettra d'être mieux armé face à ces cyberattaques. Ces sécurisations soulèvent des enjeux de sensibilisation. Cette attaque nous a mis en difficulté en tant que collectivité qui a dû travailler au papier et au crayon durant quatre semaines, et dans la relation aux citoyens en diminuant leur confiance vis-à-vis de l'équipe municipale.

Nous avons enregistré des pertes financières étant donné que la piscine, les musées et les parkings n'étaient plus accessibles le temps de restaurer le système. Un impact important a été constaté par les citoyens, notamment en raison du blocage des bornes automatiques qui permettent de sécuriser la ville. Enfin, des retards ont été constatés dans les démarches

administratives. La direction des systèmes d'information a été fortement mobilisée et des agents sont rentrés de congé afin de sauvegarder la collectivité. Enfin, cette attaque a provoqué un fort stress pour ces agents.

Je suis aussi élue à la communication à la ville et l'agglomération. Nous avons fait le choix de communiquer pour rassurer les concitoyens. Nous avons choisi d'expliquer ce qui s'était passé. Il était important d'employer les bons mots au bon moment. Par exemple, nous ne pouvions pas dire que notre sauvegarde était intacte dans un premier temps. La ville-centre a été attaquée, une commune de 70 000 habitants. Cette attaque a révélé l'impact de ce type d'événement sur les communes de l'agglomération. Nous avons fait le choix de créer deux postes d'accompagnement à la cybersécurité des communes de l'agglomération à la suite de cette attaque.

Mme Françoise Gatel, **présidente. –** Merci pour ce témoignage extrêmement intéressant qui soulève la question du risque de la mutualisation entre collectivités. Nous y reviendrons. M. Alexandre Ouzille, premier-adjoint au Maire de Villers-Saint-Paul, nous sommes ravis de vous accueillir. Vous nous ferez part de votre témoignage.

M. Alexandre Ouzille, premier adjoint au maire de Villers-Saint-Paul. – Notre commune est une ville moyenne de 6 500 habitants de l'Oise. Les services informatiques sont gérés par une personne chargée de la bibliothèque, qui n'est pas spécialiste de ces sujets. Un prestataire externe intervient sur la sécurité et l'appui aux utilisateurs. Le 1er juin 2020 à 2 heures du matin, nous avons été victimes d'un cryptovirus : l'ensemble des données bureautiques de Villers a été amputé. Il y a dans notre commune un accès déporté des services municipaux au centre social par un VPN. Les attaquants ont accédé aux identifiants et testé un certain nombre de codes pour accéder aux serveurs. Nous n'étions pas protégés contre ce type d'attaque et nous avons perdu l'ensemble des données informatiques, de ressources humaines et financières.

Nous avons établi ce constat le 2 juin. Nous sommes immédiatement revenus au travail manuel. Tous les quinze jours, une sauvegarde manuelle est désormais réalisée par un agent pour sauvegarder toutes les données de la ville. La réinstallation et la reconfiguration des serveurs a coûté 58 000 euros, dont 13 000 euros pris en charge par l'assureur, et entraîné la mobilisation de 2 ETP durant un trimestre à plein temps, respectivement aux finances et aux ressources humaines, pour ressaisir des données sensibles. Cette situation a fortement impacté leurs horaires et leur travail quotidien.

Sur les paies, nous ne pouvions que reproduire la dernière paie dans le système d'information. Nous avons mimé les paies durant six mois, le temps de réinstaller le système en procédant à des ajustements à l'issue de cette période. Nous n'avons pas renouvelé le contrat avec notre prestataire sur la sécurité. La défaillance à l'origine de la cyberattaque semblait évitable.

Elle a été repérée plusieurs mois auparavant sans qu'une action n'ait été mise en œuvre par le prestataire. Cette situation aurait pu être évitée.

Nous nous sommes appuyés sur l'intercommunalité de Creil-sur-Oise. Un service mutualisé est en cours de mise en place au niveau de l'agglomération, qui regroupe des personnes très compétentes. Le fait intercommunal peut être un relais sur les questions de cybersécurité. Un frein vient néanmoins de la sensibilité des données des communes. Il faut avoir confiance envers les autres communes de l'agglomération pour transférer des données. Les serveurs peuvent rester dans des villes, mais je pense que la dimension intercommunale est fondamentale sur les questions de cybersécurité.

Mme Françoise Gatel, **présidente. –** Je vous remercie et propose aux représentants de l'AMF, de l'ADF et de l'association des maires ruraux d'intervenir.

Mme Vincent, Association des maires ruraux. – Merci pour ces témoignages. Il est très important de sensibiliser les élus et les secrétaires de mairie à ces nouvelles pratiques de cybersécurité. Il y a un manque de connaissance, de compétence et de budget dans les petites communes. L'État met en place des moyens. Chaque territoire est différent en termes de moyens et d'accès. Il faut agir à une échelle plus réduite et non au niveau étatique.

Mme Françoise Gatel, **présidente. –** J'invite Mme Marie-Laure Pezant, chargé de mission à l'Association des maires de France, à intervenir.

Mme Marie-Laure Pezant, chargé de mission à l'Association des maires de France. – La cybersécurité est un sujet qui occupe l'AMF depuis un an, étant donné qu'avec nos partenaires présents nous avons mené un certain nombre d'actions. Nous souhaitons accompagner les communes urbaines ou rurales. Il est important de les sensibiliser davantage. La vulnérabilité croît notamment par le développement du télétravail. Il est nécessaire d'intégrer le risque de cybersécurité au sein des plans de prévention. Il faut mettre en place un certain nombre de processus au niveau du plan de continuité d'activité pour anticiper le risque. Il faut mener des exercices en les intégrant à des missions de sécurité plus classiques, comme les exercices de lutte contre le terrorisme. Enfin, il faut tenir compte de l'impact psychologique fort de ces attaques sur les agents. Nous assistons à un certain nombre de difficultés.

Mme Françoise Gatel, **présidente. –** Je vous remercie pour la brièveté de votre intervention et l'importance de la dimension humaine auprès des personnes victimes de la cyberattaque et que vous évoquez auprès de nos concitoyens. Je transmets la parole à la représentante de l'Assemblée des départements de France.

Mme Virginie Langlet, représentante de l'ADF. – L'Assemblée des départements de France a créé plusieurs groupes de travail dans le domaine

de la cybersécurité afin de partager les bonnes pratiques et les avis sur les prestataires. Je rejoins le point de vue des témoins de cyberattaques. Nous en avons connu dans les départements. Nous constatons un manque de formation des agents en matière de cybersécurité. Les élus sont intéressés par le sujet, mais il est difficile pour un RSSI en place dans les départements de former les élus et de les sensibiliser au sujet.

Deux départements ont présenté à l'ADF un retour d'expérience sur des campagnes de *phishing* fictives organisées par des prestataires spécialisés, pour étudier le taux de personnes qui se feraient manipuler. Ces taux atteignent de 40 à 70 % des personnes, malgré les formations diffusées sur ces sujets. Il est fondamental de continuer de former et d'apprendre à gérer une crise. La communication avec les médias est très importante. Il faut restaurer la confiance avec les usagers, ce qui requiert un important travail de communication.

Mme Françoise Gatel, **présidente. –** Je vous remercie pour cette intervention. J'invite le Sénateur Rémy Cardon, secrétaire de la délégation aux entreprises, co-rapporteur de la mission sur la cybersécurité, et la Sénatrice Michelle Gréaume à intervenir.

M. Rémi Cardon. – Je vous remercie. J'ai remis, avec Sébastien Meurant, un rapport bâti après six mois de travaux et 47 auditions du public des PME et TPE sur la cybersécurité. Nous avons souhaité organiser une table ronde avec les collectivités territoriales aujourd'hui, étant donné que nous avons constaté qu'elles sont très touchées. La cybersécurité est un sujet d'actualité. La troisième économie mondiale serait le cyber risque si cette activité était un pays et ces attaques génèrent plus de 6 000 milliards d'euros de coûts dans le monde.

Les familles de mafias s'organisent très bien dans cette industrie. La France commence à s'emparer du sujet. Le Cybercampus sera ouvert en janvier ou en février 2022. Nous manquons de formations suffisantes et de personnel qualifié. La cybersécurité éprouve des difficultés à percer dans nos domaines. Je comprends les difficultés des communes qui ont subi une cyberattaque. Un travail important doit être mené avec les intercommunalités qui doivent sensibiliser les petites et les moyennes communes à ce sujet.

Il n'est pas très difficile d'expliquer qu'il faut stocker correctement les données et effectuer des sauvegardes régulières. Certaines habitudes des secrétaires de mairie sont plus ou moins bonnes. Les départements ont un rôle à jouer. Ils ont un devoir de fournir des solutions adéquates à des prix raisonnables. La sécurité totale n'existe pas. Les communes doivent sauvegarder régulièrement les données. Cela constitue un enjeu de continuité du service public. Une TPE, une PME, une collectivité ou un grand groupe peuvent être victimes de ces attaques. La délégation aux

entreprises et la délégation aux collectivités territoriales sont légitimes pour travailler ensemble sur ce sujet.

Mme Françoise Gatel, **présidente**. **–** Je transmets la parole au sénateur Franck Montaugé.

M. Franck Montaugé. **–** Je souhaite remercier tous les intervenants pour la qualité et l'intérêt de leurs propos. Au Sénat, une commission d'enquête s'est penchée sur la question de la souveraineté numérique et a tenté de l'appréhender dans ses différentes dimensions. Parmi les recommandations figurait celle de couvrir le territoire national en *data centers* pour des raisons de développement industriel, de couverture de la 5G dans les territoires ruraux, et de mettre en place des stratégies concertées à l'échelle des départements, avec des garanties de management et de sécurité des systèmes d'information.

L'équipement du territoire en fibre optique est souvent pris en charge par des syndicats pilotés par les départements avec la participation des collectivités territoriales, dont les communautés de communes qui sont en charge du sujet. Il faut assurer un lien de continuité entre l'équipement du territoire en fibre et cette question de la cybersécurité du point de vue des collectivités territoriales. Nous pourrions envisager la possibilité que ce syndicat puisse, dans le prolongement de ce qu'il fait en matière d'infrastructure, prendre en charge tout ou partie de cette question de la sécurité des données des collectivités territoriales.

Cette suggestion pratique doit être étudiée. Ce serait un moyen de progresser. J'ai entendu que cette question puisse être appréhendée à l'échelle des intercommunalités, ce qui est seulement envisageable pour les territoires qui en ont les moyens. Ainsi, dans le Gers où je suis élu, les intercommunalités ne peuvent financer les ressources et les compétences associées à la question de la cybersécurité. L'échelle départementale paraît appropriée dans notre territoire pour traiter ce sujet.

Mme Michelle Gréaume. **–** L'informatique a rapidement évolué. Tout le monde n'a pas une bonne réception Internet, ce qui est peut-être une chance, en offrant du temps pour se protéger davantage. Les données volées en entreprise et les collectivités territoriales sont très sensibles, notamment pour la sécurité, l'état civil, le bancaire ou le médical. La crainte se pose sur la revente des fichiers qui pourrait en résulter.

Au vu de votre expérience, qu'avez-vous mis en place pour renforcer la confiance des usagers à utiliser le numérique ? Y a-t-il eu des modifications sur la sécurité des logiciels par les prestataires et la mise en place d'une certification ou d'une homologation de sécurité sur les logiciels en place ? Y a-t-il eu un suivi d'indemnisation, notamment pour les citoyens victimes de falsification d'état-civil ou de vol d'identité, qui constitue aussi une atteinte à la réputation de la ville ?

Mme Françoise Gatel, **présidente**. – J'invite Anne-Catherine Loisier à intervenir.

Mme Anne-Catherine Loisier. **–** Bonjour à tous et merci pour ces témoignages. Vous nous avez confié, à moi et mes collègues, une mission sur la numérisation des collectivités territoriales. L'État s'est engagé à numériser pour 2022 les principaux services et sensibiliser davantage les collègues aux potentielles attaques numériques pour la protection des populations. Il convient de sensibiliser sur la vulnérabilité numérique. Le déploiement de la 5G renforcera cette vulnérabilité. Il est ressorti de nos auditions qu'en parallèle de cette sensibilisation, il faut attirer leur attention sur les failles de l'outil, et créer une veille permanente, étant donné qu'une collectivité territoriale qui n'a pas encore été attaquée pourra l'être, et une collectivité territoriale attaquée une fois pourra l'être de nouveau deux ou trois fois. Le numérique est un objet risqué. Il faut utiliser cet outil en étant conscient de ses failles.

Il est nécessaire d'assurer cette veille. L'échelon du département en coopération avec la gendarmerie et les délégations territoriales me paraît être le mieux adapté pour assurer cette veille et informer les collectivités territoriales. Un maillage de *data centers* est en place dans les territoires. En Côte d'Or, les collectivités territoriales ne souhaitent pas intégrer ces dispositifs qui donnent le sentiment que l'externalisation des données crée un risque supplémentaire. Pouvez-vous nous éclairer sur ce point ?

Mme Françoise Gatel, **présidente**. – La seconde table ronde sera animée par M. Vincent Séguin, Secrétaire à la délégation aux entreprises. J'invite les trois grands témoins à se faire écho de l'audition et répondre aux questions à la suite de ces interventions. Pouvez-vous faire écho à ces témoignages ?

Mme Marie Nedellec, adjointe au maire de La Rochelle. **–** Comment rétablir la confiance avec les citoyens ? Il y a l'action lors du rétablissement des données. Nous avons fait le choix de communiquer par tous les moyens, dont la presse, étant donné que les outils informatiques n'étaient pas disponibles. Nous avons un rôle de sensibilisation sur la donnée. Nous avons mis en place un nouveau portail dédié aux familles et il a fallu faire preuve de grande pédagogie à destination des citoyens et agents sur le terrain. Enfin, la sensibilisation des élus est très importante étant donné que les élus locaux ne maîtrisent pas le sujet. Nous avons créé des postes au sein de l'agglomération pour accompagner les communes.

J'aimerais attirer l'attention sur les syndicats départementaux informatiques, qui ne peuvent être prescripteurs et éditeurs de logiciel, c'est-à-dire le DPO et le RSSI. Ces postes doivent être scindés, le DPO devant être rattaché à la Direction générale des services et non à la DSI, afin de ne pas fragiliser la gouvernance dans les petites communes qui ne maîtrisent pas ces sujets. La ville de La Rochelle n'avait pas d'assurance en matière de

cybersécurité. Nous avons fait le choix d'en souscrire une désormais, avec une potentielle indemnisation pour la collectivité et les citoyens.

M. Alexandre Ouzille, premier adjoint au maire de Villers-Saint-Paul. – À la suite de la mise en place des évolutions informatiques que nous avons apportées, nous avons effectué un audit externe sur lequel nous avons communiqué dans le magazine municipal suivant. Le département est assez lointain. Selon moi, l'intercommunalité est le bon outil pour traiter des sujets de cybersécurité.

M. Richard Lizurey, adjoint au maire de Chartres. – Il est important d'insister sur la diversité des témoignages et de mettre en place une gouvernance extrêmement précise. La cybersécurité est traitée au niveau national, départemental, régional, des intercommunalités, etc. Il est extrêmement difficile de s'y retrouver. Un élu non spécialiste de l'informatique ne peut identifier la pertinence des offres des prestataires. Nous avons besoin que les services de l'État décryptent la qualité de l'offre des prestataires.

Mme Françoise Gatel, **présidente. –** Je vous remercie pour ces explications. Vos témoignages sont extrêmement intéressants en termes de sensibilisation. J'évoquerai quelques points en conclusion, d'une part la prise de conscience de la gravité extrême de ce risque, d'autre part une prise de conscience du personnel et de nos concitoyens. Le second axe concerne la prévention. J'ai compris que vous préconisez la séparation de la gouvernance et du volet technique qui soulève des difficultés. Le Sénat n'a pas de religion dans ce domaine. Il n'est pas possible de définir a priori une échelle de pertinence. L'intercommunalité peut être extrêmement pertinente alors que dans d'autres cas le sujet est porté par les départements. Il est surtout important que le sujet soit traité au niveau du territoire le plus pertinent, en confiant le sujet à des collègues compétents sur les sujets de cybersécurité.

2. Audition de Mme Gwenaëlle Martinet, cheffe de projet France Relance, M. Marc Boget, commandant de la gendarmerie dans le cyberespace, M. Jérôme Notin, directeur général ACYMA et M. Cyril Bras, vice-président de l'Institut pour la cybersécurité et la résilience des territoire

M. Vincent Segouin, secrétaire à la délégation aux entreprises. – Madame la Présidente a bien résumé la situation. Les témoignages précédents prouvent que les systèmes de sécurité sont parfois faillibles. Les petites communes ne s'intéressent pas assez au sujet. La semaine dernière, nous avons organisé la Journée des entreprises au Sénat, qui a abouti au même constat. Les petites entreprises considèrent qu'elles sont trop petites pour être attaquées. Elles ne savent pas quel budget allouer à la cybersécurité. Plusieurs intervenants de l'État présents autour de la table pourront évoquer les bonnes pratiques à adopter en la matière. J'invite

M. Cyril Bras, vice-président de l'Institut pour la cybersécurité et la résilience des territoires, à intervenir en premier lieu.

M. Cyril Bras, vice-président de l'Institut pour la cybersécurité et la résilience des territoires. – Je vous remercie de me donner la parole sur ce sujet important qu'est la cybersécurité. Plutôt que de répondre directement à votre question, je souhaite livrer un témoignage du travail sur le terrain. Avant d'occuper cette fonction, j'ai travaillé dans les services de sécurité informatique en collectivité, et j'ai initié un réseau de 140 RSSI. Les attaques cyber sont permanentes. L'adhérence au numérique est forte. Nous accumulons une dette colossale avec des systèmes d'information obsolètes. Certains fournisseurs de solutions logicielles font n'importe quoi. Des systèmes industriels sont oubliés. À Oloron Sainte-Marie, par exemple, la station d'épuration a été impactée par une cyberattaque.

Les collectivités territoriales souffrent d'un manque de compétence en matière de SSI, service qui est souvent dilué dans la DSI. Il n'y a pas souvent de RSSI dans les communes. Certains collègues RSSI ont l'interdiction de s'adresser aux élus ou au Directeur général des services (DGS). Il n'y a pas de protection du type DPO ou de cadre juridique pour alerte en cas de problème. Le CNFPT génère les fiches de poste de la fonction publique. La vision du RSSI date d'il y a dix ans. Il est temps que cette fiche soit actualisée. Le RSSI doit devenir un directeur de la sécurité numérique.

Notre fonction de RSSI est perçue comme uniquement technique. Il est important de comprendre la nécessité d'un changement. Les salaires offerts par les collectivités territoriales pour les RSSI sont par ailleurs très insuffisants.

Le dernier volet d'action est réglementaire. Les prestataires ne veulent pas se mettre en conformité et les collectivités territoriales n'ont pas de levier pour les faire changer. Le RGPD aide beaucoup. Les solutions sont a priori conformes au RGPD. De nombreux points doivent être améliorés.

La sensibilisation est ultra-efficace au niveau des agents, que j'ai transformés en acteurs de la cybersécurité. C'est l'affaire de tout le monde. Tout le monde doit agir étant donné que les attaques se déroulent sur la touche physique et sémantique. La sensibilisation des petites communes à ce sujet est essentielle. Le problème consiste à faire prendre conscience des enjeux énormes associés à la cybersécurité. Les cyber-attaques sont importantes. Il est fondamental de se saisir du sujet en amont.

M. Vincent Séguin. – J'invite le Général Marc Boget à intervenir, la gendarmerie apportant un secours très précieux aux collectivités territoriales.

M. Marc Boget, commandant de la gendarmerie dans le cyberespace. – Je vous remercie. La situation est très clairement sérieuse ainsi que l'illustre le niveau de menace. La cyberdélinquance représentant un coût de 1 000 milliards de dollars par an, 10 milliards de dollars par an, avec

un retour sur investissement pour un cyberdélinquant de 200 à 500 %. Nos adversaires s'organisent vite. Le numérique est partout. La 5G et les objets connectés font exploser le problème. J'ai décompté 3 Wifi accessibles dans cette salle, dont un téléphone qui partage sa connexion avec d'autres utilisateurs et une montre connectée…

Cette dimension s'accentuera de façon exponentielle. Le nombre de plaintes liées au risque cyber a augmenté de 20 % de 2019 à 2020, et de 28 % au premier semestre 2021 par rapport à 2020. Le premier retour confidentiel des équipes chargées de la sécurité informatique des Jeux Olympiques de Tokyo évoque une multiplication par neuf du nombre de cyberattaques de Londres à Tokyo, et le même coefficient est attendu pour Paris. 70 000 attaques avérées à Tokyo donnent 630 000 attaques attendues à Paris en 2024.

La sécurité commence par le maillon le plus faible. Il y a quelques jours, un Président directeur général d'une multinationale suisse voulait échanger avec moi pour me demander ce qui était arrivé dans une entreprise achetée par ses soins à Dax, attaquée et qui a perdu l'ensemble de ses documents informatiques, alors que son chiffre d'affaires annuel s'élève à 140 millions d'euros. Ils étaient en cours d'acquisition de cette société qui détient des archives papier pour une grande partie de ses données. Cette société a été attaquée par le biais de sa filiale américaine, de taille très modeste et mal protégée. Les attaquants ont commencé à détruire des données avant de chiffrer tous les disques durs de la société.

Nous sommes confrontés à trois types de délinquants. Le très haut du spectre concerne des attaquants qui trouvent des vulnérabilités non connues des systèmes de protection. Ils trouvent des portes d'entrée non détectées, et il faut avoir des experts de très haut niveau pour s'en protéger. Nous avons la chance d'avoir des compétences dans ce domaine en France. Des délinquants du bas du spectre réalisent du *phishing* et des escroqueries d'un montant de 500 ou 600 dollars. Ils passent sous les radars de l'autorité judiciaire. Au milieu du spectre se trouvent des délinquants ordinaires qui sont organisés en offrant des catalogues de services, en associant une vulnérabilité, de la puissance de calcul, de scan, de blanchiment d'argent, avant de lancer une attaque.

Nous avons beaucoup entendu le besoin d'accompagnement des collectivités avec un focus particulier en complément du travail de l'ANSSI sur les moyens et les petits délinquants. Les situations sont très diverses. Je souhaite relayer le message de Cyril Bras sur l'importance pour les collectivités territoriales de donner au RSSI l'accès aux élus de sa collectivité. Il est important de favoriser une prise de conscience des élus locaux. J'ai récemment demandé à un élu local s'il était bien protégé contre la cybersécurité. Il m'a répondu qu'il était trop petit pour s'en occuper. Après un rapide calcul, nous avons constaté qu'il maniait 450 millions d'euros de budget.

La gendarmerie nationale a créé le commandement du cyberespace, regroupement de 7 000 cyber-enquêteurs couvrant l'intégralité du champ de la prévention à l'investigation, avec une vraie accélération donnée par le Directeur général de la gendarmerie, Christian Rodrigues, convaincu que la prochaine crise sera cyber. Nous serons 10 000 cyberenquêteurs en 2022 partout sur le territoire, en métropole comme en outremer. 40 % des officiers ont un profil scientifique.

La gendarmerie ne pourra pas tout faire seule. Nous travaillons avec de nombreux partenaires. Ce travail collectif nous permettra de marquer des points, la police nationale, l'ANSSI comme grand maître de cybersécurité et les associations d'élus. Nous avons lancé avec l'AMF un dispositif « Immunité cyber » qui consiste à poser 9 questions aux élus pour identifier ce qu'ils ne font pas ou ne savent pas faire. En cas de réponse « rouge », nous les invitons à contacter les gendarmes pour leur apporter des solutions. Il faut leur faire prendre conscience de l'importance de ce sujet.

La cybersécurité comporte deux phases, en amont et en aval. Lorsqu'une commune est attaquée, la réaction doit être de prévenir immédiatement la gendarmerie ou la police. Dès la phase de rançon, il est possible de vous accompagner. Les enquêteurs interviennent avec des négociateurs du GIGN au sujet de la demande de rançon. Il faut geler les menus numériques et prendre un certain nombre de traces. Lorsque des élus portent plainte trois semaines plus tard, cela est trop tardif.

Une opération internationale vient de concerner l'Ukraine pour interpeller des cyberdélinquants qui ont notamment attaqué en France, conclusion d'une enquête démarrée dès la demande de rançons, ce qui a permis de recueillir des éléments en vue de les identifier. Le dépôt de plaintes est encore très faible par rapport à la situation réelle des cyberattaques en France.

M. Vincent Segouin. – Je vous remercie, Général Boget. Nos collègues vous adresseront vraisemblablement un grand nombre de questions. J'invite Mme Gwenaëlle Martinet, cheffe de projet France Relance, membre de l'ANSSI, à intervenir.

Mme Gwenaëlle Martinet, cheffe de projet France Relance. – Je vous remercie de nous donner la parole. Je ne reviendrai pas sur la menace représentée par la cybersécurité. Je souhaite vous parler de ce qui est mis en place dans le cadre de France Relance. Une enveloppe de 136 millions d'euros a été déployée pour augmenter la cybersécurité dans les collectivités territoriales, en incluant les hôpitaux et les établissements publics, sous le pilotage de l'ANSSI.

Nous avons décidé de mettre en place des mécanismes gagnants-gagnants. L'objectif de cette démarche consiste à augmenter la cybersécurité en irrigant l'écosystème industriel de la cybersécurité. L'objectif n'est pas de donner de l'argent aux entreprises. Nous avons mis en place plusieurs

mécanismes. Le premier concerne les parcours de cybersécurité, qui permettent à l'ANSSI d'envoyer un prestataire qui accompagne tout au long du parcours afin de l'éclairer sur ce qu'il y a à réaliser et ce qui est le plus urgent.

Nous apportons à la fois des ressources humaines, des prestataires, des compétences, une méthodologie et de l'argent, car nous finançons les actions mises en place pour augmenter la cybersécurité, via une subvention et un cofinancement pour impliquer chaque acteur. Ce qui est gratuit n'a pas de valeur. Un financement à 100 % donnerait un pic de cybersécurité qui ne durerait pas longtemps. Il faut accompagner chaque bénéficiaire afin que ce projet perdure. Il faut expliquer comment passer les contrats, avec qui, et le coût de ces contrats. Il a été décidé de pérenniser les actions, aider à monter cette première marche et faire durer la cybersécurité.

Au niveau territorial, l'ANSSI doit aider 500 collectivités territoriales dans le cadre de France Relance. 370 collectivités territoriales sont volontaires pour évoluer en matière de cybersécurité. Cette démarche suppose de nommer un interlocuteur. Les petites collectivités territoriales qui n'ont pas d'interlocuteur ne peuvent bénéficier de ce parcours. Nous travaillons avec la gendarmerie afin de mettre en place des mécanismes les concernant. Nous insistons sur l'accès de cet interlocuteur auprès des élus et faire en sorte qu'ils soient écoutés, entendus et valorisés.

Un autre mécanisme concerne les centres de réponse à incident cyber mis en place dans chaque région. Il faut mettre à disposition des acteurs de taille intermédiaire des interlocuteurs vers qui se retourner en cas d'attaque cyber, une réponse humaine et un numéro de téléphone. Nous étudions quels prestataires disponibles peuvent rapidement intervenir, avec un parcours d'incubation pour les aider à se développer. Ces centres verront le jour en 2022. Toutes les régions ont répondu présent.

M. Vincent Segouin. – Nous aurons beaucoup de questions à poser étant donné que 500 collectivités territoriales sur 36 000 représentent un nombre peu élevé. Je transmets la parole à M. Jérôme Notin, directeur général ACYMA, intervenu la semaine dernière, lors de la 5ème Journée des entreprises, au sujet de la cybersécurité des entreprises.

M. Jérôme Notin, directeur général ACYMA. – Je ne reviendrai pas sur l'état de la menace et la compréhension du besoin de sensibilisation, qui n'existait pas il y a quelques années. La première étape consiste à avoir conscience du problème. Nous sommes associés à la gendarmerie nationale pour que ce phénomène soit pris en compte. Nous avons parlé de ce qui a été mis en place.

L'ACYMA a été créé en 2017 à la suite du constat que les cyberattaques augmentaient sur l'ensemble du spectre des particuliers aux opérateurs d'importance vitale. Le dispositif national d'assistance aux victimes d'attaque de cyber malveillance a été mis en place en 2017. Le

ministère de l'Intérieur s'est profondément investi pour la création d'ACYMA à destination des administrations et particuliers. L'ACYMA offre une mission d'assistance. La sensibilisation des particuliers et des petites collectivités territoriales à la cybersécurité est nécessaire. Il est important de maîtriser les aspects techniques pour se protéger. Les collaborateurs doivent intervenir pour augmenter le niveau de sécurité. Un guide de sensibilisation a été créé dès la première année. Une mallette destinée aux élus a été adressée aux nouveaux élus en 2020 pour les doter des outils de sécurité.

Le guide « Que faire en cas d'attaque ? » est destiné aux petites collectivités territoriales victimes le plus souvent de rançongiciels. Un dispositif d'alerte cyber a été lancé durant l'été 2020 pour alerter 3 à 4 millions d'entreprise à travers la CPME et le Medef. Une vidéo a été réalisée avec la Caisse des Dépôts pour présenter des mises en situation de maires face à la cybersécurité.

L'observation de la menace permet d'adapter le contenu des sensibilisations et d'adresser des alertes. Lors du lancement du dispositif en 2017, nous avons constaté que les prestataires de sécurité intervenaient beaucoup sur la fraude à la réparation informatique, alors que nous pensions que ce serait plutôt sur le rançongiciel. Le service d'enquête de la gendarmerie nationale s'est saisi de ce sujet. Ce service est le leader de la *taskforce* d'Europol sur les sujets de la fraude à la réparation informatique. L'ACYMA adresse des alertes publiques afin de remplir nos missions à bas coût de sensibilisation et d'accompagnement des victimes.

Le Général Boget évoquait le besoin des élus d'identifier les prestataires qualifiés en cybersécurité. L'ANSSI valide des produits de cybersécurité. Nous avons créé un label « Expert Cyber », le 18 février 2021, pour identifier les prestataires compétents en remédiation et en accompagnement à la sécurisation. 135 prestataires sont labellisés aujourd'hui par l'AFNOR, alors qu'ils étaient 50 à avoir cette habilitation le 18 février. Ces prestataires sont identifiés comme compétents pour mettre à l'état de l'art les systèmes d'information des collectivités territoriales et des PME qui en feront la demande.

M. Vincent Segouin. – Je vous remercie pour vos interventions. Vers qui puis-je me diriger si je suis à la tête d'une collectivité ?

M. Jérôme Notin, directeur général ACYMA. – J'ai besoin de sensibiliser les agents et d'avoir des éléments techniques. La gendarmerie accomplit un travail extraordinaire sur ces aspects. Je suis en lien sur les contenus produits par nos soins, diffusés dans l'ensemble des unités. Pour les aspects techniques, en 2021, nous savons identifier deux, trois ou cinq entreprises par département. Ils ont de 5 à 20 collaborateurs compétents en termes d'intégration de solutions, qui doivent être les plus françaises possible, les plus qualifiées par l'ANSSI. La sensibilisation des acteurs des collectivités territoriales doit se poursuivre.

M. Cyril Bras, vice-président de l'Institut pour la cybersécurité et la résilience des territoires. – L'INCRT a mis en place des formations locales pour faire monter en compétence des personnes qui le souhaitent et devenir RSSI de petites collectivités. Des expérimentations sont effectuées auprès de petites collectivités en réunissant des partenaires locaux.

M. Marc Boget, commandant de la gendarmerie dans le cyberespace. – La gendarmerie apporte sa pierre à l'édifice, notamment pour permettre aux élus de mettre le pied à l'étrier. Le maire dont je parlais qui gère un budget de 450 millions d'euros m'a avoué qu'il ne connaissait rien à l'informatique. Il apparaît un vrai besoin de traduction et d'accompagnement des élus pour qu'ils comprennent que la cybersécurité n'est pas insurmontable. Nous pouvons nous inscrire dans cette démarche vertueuse en matière de cybersécurité. La gendarmerie assure le lien dans le cadre d'un travail collectif.

M. Vincent Segouin. – J'invite M. Antoine Lefèvre et Mme Anne-Catherine Loisier, co-rapporteurs de la mission numérique des collectivités, à s'exprimer.

M. Antoine Lefèvre. – Avec mes collègues, nous conduisons une mission sur les initiatives digitales exemplaires menées par les élus locaux. Nous apprécions particulièrement vos interventions. Notre attention est portée sur la protection des populations. Nous voulons étudier les projets numériques et ce qui permet de renforcer l'ordre public : drones, caméras piétons, vidéoprotection, etc., ainsi que ce qui touche à la sécurité civile et la prévention des risques (incendie, climatique, sanitaire, etc.). L'actualité en livre chaque jour des exemples éloquents.

Nous voulons renforcer l'efficacité de l'action publique locale. Les usages numériques se développent. Notre devoir de vigilance et de protection doit s'intensifier. Nous devons marcher sur nos deux jambes pour éviter de créer dans les territoires des colosses numériques aux pieds d'argile. Au vu de votre expérience, à quels risques les collectivités peuvent-elles s'exposer ? Les attaques dont elles sont l'objet peuvent-elles avoir un impact sur les projets numériques dans le domaine de la protection des populations ? Pourriez-vous présenter des précédents pour illustrer vos propos ?

Mme Anne-Catherine Loisier. – Le Sénat a adopté il y a environ 18 mois, à l'initiative de mon collègue sénateur Laurent Lafon, une proposition de loi en partenariat avec l'ANSSI en vue de mettre en place un cyberscore sur l'ensemble des dispositifs proposés aux collectivités territoriales. Que pensez-vous de cette initiative ? Je vous remercie.

Mme Gwenaëlle Martinet, cheffe de projet France Relance. – L'initiative du cyberscore est intéressante, mais elle doit être manipulée avec précaution, car c'est une photo à l'instant T, qui varie très rapidement. Il faut garder une attention constante en matière de cybersécurité étant donné

qu'un cyberscore satisfaisant à un moment ne durera que si l'on continue d'investir dans la cybersécurité. Les *smart cities* représentent un point d'attention très important étant donné que ce système devient une source d'entrée et de nouvelles attaques qui permettraient par exemple d'arrêter les feux de circulation, et de bien d'autres risques mettant à mal le service public.

M. Cyril Bras, vice-président de l'Institut pour la cybersécurité et la résilience des territoires. – L'accès aux parkings ne fonctionne plus après une attaque, et cela diminue les rentrées d'argent pour la collectivité comme nous l'avons vu dans l'exemple de La Rochelle. La collectivité peut être poursuivie sur le plan juridique. Enfin, des employés de mairie étaient au chômage technique, ce qui représente un coût énorme pour les collectivités territoriales.

Mme Sylvie Robert. – Ce sujet n'est pas suffisamment pris en compte dans les collectivités territoriales. Les attaques ont souvent lieu le week-end et durant les vacances. J'ai noté le développement exponentiel des notifications en 2021. Je souhaite revenir sur la carte projetée depuis ce matin concernant les cyberattaques identifiées dans les collectivités territoriales. Les attaques concernent beaucoup de communes transfrontalières. Le confirmez-vous ? La carte vous permet-elle d'anticiper ? La dimension du sujet dépasse l'hexagone et nécessite l'amélioration de la coopération transfrontalière. Des éléments permettent-ils d'anticiper sur d'autres cyberattaques ?

M. Richard Lizurey, adjoint au maire de Chartres. – D'après la carte communiquée par le Sénat, la « diagonale du vide » de la France semble préservée des cyberattaques.

M. Marc Boget, commandant de la gendarmerie dans le cyberespace. – Je ne retrouve pas dans votre carte un certain nombre d'attaques contre des communes. J'ai été informé d'une nouvelle attaque survenue dans une commune ce matin. Il serait surprenant que l'origine transfrontalière soit un critère, étant donné que les frontières n'existent pas dans le cyber. Un *hacker* n'a pas intérêt à viser une commune située près de la frontière. Les attaques menées depuis un pays étranger sont aussi rapides à Paris ou à Sydney. La hiérarchisation des adresses IP fait que des créneaux de plages IP attribués à certains secteurs sont peut-être davantage ciblés.

M. Jérôme Notin, directeur général ACYMA. – Nous utilisons une cartographie de la position géographique des victimes. Il y en a sur l'ensemble de la France, et non seulement en zone frontalière. La presse quotidienne régionale (PQR) parle beaucoup de cybersécurité dans l'Est de la France, en raison de l'appétence des journalistes sur ces sujets.

M. Vincent Segouin. – La carte que nous présentons n'est pas exhaustive, mais illustrative de la diffusion de la cybermenace à tout le territoire.

Mme Françoise Gatel, présidente. – Il y a selon moi un fléchage naturel vers les collectivités territoriales les plus peuplées et les plus riches. La diagonale du vide est moins attaquée du fait qu'il y a moins de richesses.

M. Cyril Bras, vice-président de l'Institut pour la cybersécurité et la résilience des territoires. – Annecy a été piraté lorsque la Rochelle a été attaquée. Saint-Affrique a été récemment attaquée. Les attaques concernent aussi de petites communes.

M. Rémy Pointereau. – Nous parlons des attaques. Appréhendons-nous des *hackers* ? Sont-ils identifiés ? Leurs méthodes changent. Avons-nous des mesures répressives suffisantes contre eux ?

M. Marc Boget, commandant de la gendarmerie dans le cyberespace. – Il arrive que nous arrêtions des cyberattaquants. Nous en avons récemment arrêté en Ukraine, qui sont traduits devant la justice. La gendarmerie peut-elle arrêter tous les cyberdélinquants ? Non. Ce serait présomptueux de le penser. Il faut augmenter le niveau de résilience. Les délinquants sont des fainéants dans le monde physique et cyber. Ils vont où c'est le plus simple. Une maison avec une alarme et des chiens est mieux sécurisée qu'une maison au fond des bois, sans alarme.

Nous poussons à la prévention et à l'augmentation du niveau de résilience, afin de monter le niveau de cybersécurité, ce qui éloignera les cyberdélinquants. Nous avons tous un rôle à jouer, gendarmerie, police, services de renseignement, etc. 47 pays ont livré un bilan évoquant 4 000 enquêtes pour lutter contre la cybersécurité. Nous sommes très bien connectés au niveau international. Les pays collaborent bien entre eux. Tout le monde joue le jeu. Sur le plan technique, nous avons des partenariats poussés sur le plan international.

Mme Michelle Gréaume. – Pouvez-vous, Général, transmettre le questionnaire dont vous avez parlé ? Des recherches sont-elles en cours pour protéger certains logiciels nationaux des attaques venant de satellites, et pour protéger les collectivités territoriales en France ?

M. Marc Boget, commandant de la gendarmerie dans le cyberespace. – L'enquête dont je parlais a été envoyée aux 30 000 adhérents de l'AMF. Elle sera de nouveau envoyée par les gendarmeries départementales afin d'irriguer tous les élus. Je rejoins le point de vue de Gwenaëlle Martinet, cheffe de projet France Relance à l'ANSSI, sur le fait que les outils magiques ne seront pas suffisants sur la durée. Il faut se prémunir de l'idée qu'un produit miracle permettrait de se prémunir contre toutes les cyberattaques.

Mme Gwenaëlle Martinet, cheffe de projet France Relance. – Il se pose la question de la sécurité des logiciels et de la sécurité des satellites, qui sont deux sujets distincts, qui ne sont pas liés entre eux. La liaison satellitaire est très bien sécurisée.

M. Vincent Segouin. – Je vous remercie tous pour votre présence et votre témoignage. La sensibilisation est le meilleur moyen d'avancer sur le dossier. Nous avons identifié ce souci. Le chantier ouvert devant nous est immense. Il faut privilégier les actions coordonnées. Il est important que toutes les collectivités territoriales prennent conscience du sujet et identifient quels investissements doivent être consacrés à la cyberdéfense pour demain. Le meilleur moyen de protection consiste à sensibiliser les petites collectivités et les petites entreprises.

Mme Françoise Gatel, **présidente**. **–** Je souhaite remercier mes collègues Sénateurs Serge Babary et Vincent Segouin, président et secrétaire de la délégation aux entreprises, pour l'excellent travail accompli et notre coopération. La valeur de la sécurité de la chaîne dépend du maillon faible. Nous devons tous nous acculturer à ce danger. Je souhaite vous remercier pour ces témoignages très intéressants sur le fait que le risque est partout. Je remercie les associations d'élus qui accompagnent les personnes sur le terrain. Nous voyons comment l'État nous accompagne dans le domaine de la cybersécurité. Je suis heureuse de féliciter les collègues qui portent cette mission au titre de la délégation des collectivités, qui peut contribuer à valoriser tout ce que nous faisons. Je vous remercie très sincèrement.

M. Serge Babary, président. – Je me félicite de la coopération entre les délégations sur ce sujet. Il était important d'étendre à la délégation des collectivités territoriales les contacts que nous avons pris au sein de la délégation aux entreprises. Nous avons vu la répartition des attaques sur tout le territoire et dans tous les domaines : communes, hôpitaux, services de sécurité, etc. Nous pouvons nous réjouir de la fédération des énergies, entre le public et le privé, entre les services de police et de gendarmerie. La création du Cybercampus en février 2022 rassemblera toutes les forces publiques, privées et technologiques afin que la France soit bien armée dans ce combat. Une première promotion de cybergendarmes est prévue pour former de jeunes gradés qui diffuseront la culture de la cybersécurité dans les territoires.

Nous continuons le travail sur la cybersécurité au sein de notre délégation. Il est important d'évoquer le problème assurantiel lié aux sommes demandées par les rançongiciels, ce qui impose d'adopter une réponse unique et précise. Certains chefs d'entreprise ont la tentation de payer les rançons demandées pour redémarrer l'activité. Des assurances couvrent ce risque. Il y a des réserves en France pour couvrir ce risque, qui est pris en charge aux États-Unis. Le service public ne paie jamais. Nous devrons débattre de ce sujet afin d'obtenir une position claire de l'administration sur le caractère assurable, ou pas, des cyber rançons. Merci pour vos différents témoignages qui sont précieux. Je vous souhaite une bonne journée.

INFOGRAPHIES : QUE FAIRE EN CAS DE CYBERATTAQUE ?

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique