



# TRIP DE PRINTEMPS 2024

28 et 29 mai

Table ronde 3  
Cybersécurité : dispositifs nationaux et européens pour  
agir dans les territoires

---

## CYBERSECURITE : DISPOSITIFS NATIONAUX ET EUROPEENS POUR AGIR DANS LES TERRITOIRES

Animateur :

■ Luc DERRIANO  
Chargé de mission - Avicca

Intervenants :

- Mathieu HAZOUARD  
Président Campus Cyber - Nouvelle Aquitaine,
- Jean-Michel MORER  
Vice-président - APVF - Petites Villes de France
- Amandine DEL AMO  
Chargée de mission – Partenariats GIP ACYMA -  
[Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)
- Célia NOWAK  
Déléguée à la sécurité numérique - ANSSI PACA

Nous allons démarrer sur le thème de la cybersécurité.

Combien d'attaques ou de fuites de données dans nos collectivités ?

Quelles sont les solutions mises en place sur le territoire national et puis sur le territoire européen pour mieux y faire face ?

Finalement, qu'est-ce que les collectivités attendent de l'État ? Et réciproquement, qu'est-ce que l'État peut demander aux territoires pour mieux coordonner notre défense collective, pour que nous jouions un peu plus collectif encore sur ce sujet ?

Pas une semaine sans qu'une cyberattaque ne fasse la Une de l'actualité. Malheureusement, les collectivités ne sont pas épargnées. Elles se placent au deuxième rang des victimes les plus ciblées, avec 10 incidents par mois en moyenne. C'est l'information tirée de la dernière synthèse de la menace qui avait été publiée fin octobre 2023 par l'ANSSI. Justement, il y a pas mal d'enquêtes sur le sujet : Panorama de la cybermenace de l'ANSSI, Panocrim du Clusif ou encore le rapport d'activité de cybermalveillance.gouv.fr qui constatent tous qu'il y a un nombre et une sophistication croissants des incidents affectant nos collectivités publiques, chaque année. L'ANSSI notamment précise que 24 % des victimes d'attaques par rançongiciel en 2023 étaient des collectivités. Le secteur est donc jugé encore trop vulnérable.

Et les conséquences sont très lourdes pour les services publics. Ce sont des interruptions d'activité dans 40 % des cas, des destructions de données dans 20 % des cas, des pertes financières dans 20 % des cas : ces chiffres sont mentionnés dans le rapport du Clusif. Les attaques perturbent notamment des services qui sont bien visibles comme le service de paie des agents, le versement des prestations sociales ou encore la gestion de l'État civil. Certains services essentiels tels que les SDIS ou bien la distribution de l'eau ne sont pas épargnés. Mais jusqu'à présent, il n'y a pas eu d'interruption d'activité sur ces domaines. Ce qui est sûr c'est que la reprise d'une activité normale peut être très longue et que c'est souvent très coûteux.

C'est un panorama un peu noir. Mais pour autant des solutions se sont mises en place et c'est ce que nous allons présenter lors de cette table ronde. Pour que la défense soit un peu plus collective et mieux organisée, il y a des sensibilisations des communes, des outils de diagnostic, des labels Expert Cyber, des exercices de simulation. Des CSIRT se mettent en place, des campus cyber sont créés un peu partout sur le territoire. Et puis il y a la directive européenne NIS V2 qui devrait être transposée très prochainement, normalement en octobre. Ce sont donc tous ces dispositifs, certains qui sont anciens, enfin qui ont quelques mois ou quelques années, d'autres qui sont tout nouveaux, que nous allons vous présenter par les acteurs, par ceux qui les mettent en place.

Nous allons donc entrer dans le vif du sujet. Mathieu HAZOUARD, vous êtes conseiller régional Nouvelle-Aquitaine, délégué aux enjeux numériques, président du Campus Cyber en Nouvelle-Aquitaine. Vous êtes aussi membre du bureau de l'Avicca. Avant de présenter dans le détail le Campus cyber et son CSIRT, est-ce que vous avez vécu une attaque ou est-ce que vous avez entendu parler d'attaques cyber dans votre région ?

### Mathieu HAZOUARD

---

Évidemment, nous avons entendu parler d'attaques. C'est quand même le cœur de l'action du Campus cyber de Nouvelle-Aquitaine. Mais les cas que nous pouvons mettre sur la place publique ou médiatiser sont très peu nombreux parce que souvent, et nous y reviendrons, quand nous sommes attaqués, nous avons peur de le faire savoir. Je peux cependant partager deux exemples concrets en Nouvelle-Aquitaine.

Par exemple, la société GUYAMIER qui est un gros transporteur de l'agglomération bordelaise et l'hébergeur COAXIS qui héberge les données de nombreux experts comptables. Le patron de COAXIS est venu témoigner. Il a évoqué le rançongiciel dont il a été victime par le fameux groupe LockBit. Les conséquences techniques sont lourdes, mais pas seulement. Il y a la question de son image vis-à-vis de ses clients et donc de sa réputation.

Du côté des collectivités, l'agglomération de Poitiers en particulier a subi des attaques du même ordre. Souvent, nous sommes sur du rançongiciel ou alors simplement du cryptage de données. Mais nous voyons comment, derrière, cela grippe les machines et là, c'est un service public qui peut être impacté de la paie de ses agents jusqu'à la mise en difficulté pour porter ses politiques publiques.

## Luc DERRIANO

---

Je pose la même question à Célia NOWAK. Vous êtes déléguée régionale Provence-Alpes-Côte d'Azur pour l'ANSSI, l'autorité nationale en matière de cybersécurité. Avant de parler aussi de l'ANSSI et des moyens qui sont mis en œuvre pour lutter contre les cyberattaques, est-ce que vous avez aussi un exemple de cyberattaque dans le secteur public en PACA ?

## Célia NOWAK

---

En tant qu'agence en charge des enjeux de cyberdéfense, l'ANSSI enregistre et suit de nombreux incidents. Ce que l'on constate dernièrement, c'est que de nombreuses collectivités font parties des victimes de rançongiciels recensées par l'ANSSI, alors qu'elles ne sont historiquement pas nos bénéficiaires prioritaires. Il y a en effet une augmentation dans ce secteur.

Le premier exemple que je souhaitais vous donner concerne une grande métropole de la région PACA, qui, en mars 2020, est victime d'une cyberattaque. Vous vous rappelez, c'est la première période de COVID, des personnes qui sont malades décèdent. Or, la cyberattaque a rendu indisponible l'accès aux plans des cimetières. On voit ici que les conséquences de l'attaque ne sont pas seulement techniques ...

Le deuxième exemple concerne une collectivité de 8 000 habitants. Là, je vais utiliser comme illustration, les chiffres du coût que cela a représenté pour la collectivité. Un premier chiffre : 250.000 euros de coût de remédiation, les experts qui sont venus, le

coût de reprise d'activité, de remontage des systèmes d'information, le rachat de nouveaux serveurs, leur mise en place, etc. Et je réitère ce chiffre de 250.000 euros pour les salaires. Au total cela fait donc 500.000 euros.

Ces attaques peuvent être « fatales » : du côté des TPE, PME, nous voyons que parfois des entreprises mettent la clé sous la porte. Côté collectivité, il y a parfois un soutien, mais cela pose vraiment des problématiques au niveau du budget et de la continuité d'activité.

## Luc DERRIANO

Amandine DEL-AMO, vous représentez cybermalveillance.gouv.fr. A l'Avicca, nous connaissons cybermalveillance.gouv.fr puisque nous participons au groupe de travail dédié aux collectivités depuis l'origine. Et vous avez mentionné dans votre dernier rapport d'activité que 17 % des demandes d'assistance que vous aviez eues en 2023 émanaient de la part de collectivités qui représentaient précisément 4.122 demandes d'assistance.

Est-ce que vous pouvez nous donner quelques exemples de ces demandes d'assistance ?

## Amandine DEL-AMO

Hier encore, une toute petite collectivité Dammartin-en-Goële comprenant, 9.300 habitants, a été attaquée, une autre dans le nord, à Gravelines, le 26 avril, Albi courant avril, Saint-Nazaire et toutes les communes alentours, comptant au total 70 000 habitants.

Les attaques ciblent vraiment tout type de collectivités, des plus petites aux plus grandes. Il faut vraiment s'y préparer. Dans notre rapport, nous notons que les collectivités représentent 2 % des demandes d'assistance sur notre plateforme. Cela peut sembler anodin. Mais quand on rapporte ces chiffres au volume respectif des

catégories de l'INSEE, donc 68 millions de particuliers, 6 millions d'entreprises et 35.000 collectivités, cela veut dire que pour un particulier aidé, nous aidons une entreprise et 35 collectivités.

Notre dispositif accompagne et aide des collectivités tous les jours. Je ne peux pas en citer d'autres, les données étant anonymisées. Mais ce que je peux vous dire c'est que les types d'attaques qui les touchent, comme monsieur HAZOUARD l'a dit, sont des rançongiciels et de l'hameçonnage qui touche tous les publics.

La troisième menace, c'est le piratage de comptes. Ce sont trois menaces à avoir en tête et auxquelles il faut absolument se préparer.

## Luc DERRIANO

---

A Cybermalveillance.gouv.fr, vous vous occupez plutôt des petites communes, en dessous de 30.000 habitants ?

## Amandine DEL-AMO

---

Tout à fait. Nous sommes là pour accompagner les plus petites collectivités. Que ce soit en matière d'assistance, via notre plateforme où les collectivités vont pouvoir trouver des conseils personnalisés et des prestataires pour les accompagner dans leur remédiation, mais aussi en matière de sécurisation en amont des attaques, pour les collectivités qui ont conscience des enjeux. Elles peuvent trouver sur notre plateforme un parcours spécifique pour être mises en relation avec des prestataires de confiance, labellisés ExpertCyber pour les aider à se sécuriser. Sur la partie prévention, sensibilisation nous avons de nombreux contenus et outils que nous présenterons tout à l'heure.

## Luc DERRIANO

---

Je me tourne maintenant vers Jean-Michel MORER. Vous êtes vice-président de l'APVF, association des petites villes de France, maire de Trilport, une commune

seine-et-marnaise d'environ 6.000 habitants. Avez-vous également été confronté à ce type d'attaque ou bien est-ce que vous avez entendu parmi vos voisins, communes ou services publics, parler des attaques et de leurs conséquences ?

## Jean-Michel MORER

---

Je pense qu'effectivement, c'est une problématique générale qui s'adresse à toutes les entités, qui si elles ne sont pas importantes en nombre d'habitants, sont à contrario essentielles à celles et ceux qui les animent. C'est vraiment ce qu'il faut préciser.

J'ai deux exemples en tête. Un qui a défrayé la chronique et impacté directement, qui est l'attaque subie par le Conseil départemental de Seine-et-Marne ; elle a mis à plat absolument toutes les fonctions de cette collectivité, y compris téléphoniques. Aucun commentaire à faire sur l'organisation interne, je pense cependant qu'il y a de sérieux enseignements à en tirer. Et puis une qui m'a touchée directement, qui nous a valu d'avoir un crash test en temps réel, au niveau de ma commune, et perturbé les services à peu près une demi-journée. Elle prouve que même si nous avons déployé des moyens de sécurisation pertinents, il s'agissait tout de même d'une véritable alerte.

Au niveau de l'APVF, nous pensions qu'effectivement il y a le dommage financier et l'estimation du coût en milliers d'euros qui en découle et les budgets à équilibrer, mais il faut également intégrer tous les dommages directement collatéraux : sur l'ambiance des services, le climat et les conditions de travail, le doute, l'inquiétude, la peur parfois des agents au lieu de la confiance qui doit prévaloir dans nos collectivités comme dans nos entreprises. Des dommages difficilement quantifiables mais qualifiables

Cela souligne également que le devoir de vigilance que nous devons tous avoir, s'affranchit des seuils de population. Nous reviendrons tout à l'heure sur NIS2, qui

est, en termes d'organisation administrative, une organisation administrative quelque peu caricaturale à déployer.

Oui, la cybersécurité doit faire absolument partie de notre ADN et nous devons l'adresser sans la sataniser, en se disant que nous rentrons dans une nouvelle ère et que nous devons acquérir une véritable culture du risque, sans la craindre mais en apprenant les bons réflexes. Les vérités absolues doivent place au doute et à la prévention.

## Luc DERRIANO

---

Nous avons fait un tableau qui montre tout type d'attaques, tout type de collectivités publiques ou d'entreprises qui peuvent être concernées. L'idée ce n'est pas de stigmatiser les uns ou les autres. Nous voyons bien que cela atteint aussi bien des collectivités qui se sont préparées que d'autres qui se sont laissé surprendre. L'idée maintenant, c'est plutôt de montrer qu'il y a des solutions, qu'il y a une organisation qui s'est mise en place depuis déjà plusieurs années.

Nous allons commencer avec Mathieu HAZOUARD, président du campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine. En quoi consiste ce campus, quels en sont les fondateurs, qu'est-ce que nous pouvons y trouver ? Et puis vous insisterez peut-être plus particulièrement sur le CSIRT régional, ce centre régional de réponse à incidents qui est hébergé au sein de ce campus.

## Mathieu HAZOUARD

---

Pour décrire brièvement le Campus Cyber de Nouvelle-Aquitaine, il est issu d'une réflexion qui remonte à 2016. Je me rappelle de premières réunions autour du président du Conseil régional, Alain ROUSSET. Nous avons déjà des acteurs qui étaient venus nous voir en disant qu'il y avait une réalité et vraisemblablement un besoin de positionnement, d'intervention d'une collectivité régionale pour répondre aux enjeux. Le fait que ce campus ait été créé il y a deux ans déjà relève de cette histoire. Et puis je dirais qu'aujourd'hui, il trouve sa réalité face à ce que vous avez

décrit dans votre propos introductif. On voit bien que ces chiffres-là et les exemples qui ont été énoncés juste à présent montrent la nécessité d'intervenir fortement.

Le campus a aujourd'hui trois principales missions, la première étant d'être un centre de réponses à incidents et en parallèle il y a deux autres missions que je ne veux pas décorrélées des autres, elles sont toutes aussi importantes.

La deuxième, et vous l'avez rappelé, je suis conseiller régional, donc nous intervenons en regard d'une compétence développement économique de la collectivité régionale. Notre objectif est de montrer qu'en Nouvelle-Aquitaine, nous avons un savoir-faire et des entreprises qui sont en capacité de répondre à l'enjeu, qui sont des offreurs de solutions, qui sont pour certaines ce qu'on appelle des pure players, qui bossent dans l'économie numérique, d'autres qui accompagnent les démarches. C'est aussi faire en sorte que cet écosystème ne soit pas dissocié d'une réalité et des gens qui sont attaqués. C'est autant les accompagner financièrement dans le cadre de projets d'innovation : par exemple les emmener sous une même bannière au forum international de la cybersécurité qui s'appelle maintenant InCyber à Lille. Donc nous étions sous une même bannière, la bannière régionale et avec le campus, et il y avait douze boîtes qui ont pu montrer leur savoir-faire. Cet élément est important : nous voyons que cela a permis de monter en puissance et de faire en sorte que les entreprises travaillent ensemble. Elles ne se connaissaient pas auparavant. A l'AG du campus, il y a 15 jours, deux boîtes, sont venues nous présenter une solution à faire ensemble et nous allons élargir un peu le spectre.

Le troisième objectif du Campus, et nous le voyons aussi à l'aune de ce qui a été dit avant, c'est la dimension formation, sensibilisation, acculturation. Nous pourrions revenir sur l'enjeu formation. Nous le disons souvent, nous n'avons pas assez de gens formés d'une manière générale sur les métiers du numérique. Et aujourd'hui nous n'avons pas assez de gens formés qui maîtrisent l'enjeu cybersécurité, pas assez de data scientists, pas assez de techniciens informatiques. Nos cohortes de nouveaux diplômés chaque année ne suffisent plus à répondre à l'enjeu. Nous avons aussi

l'ensemble des organismes de formation ou écoles, universités qui font partie du Campus pour cette dimension de sensibilisation.

Aujourd'hui, nous avons un champ assez incroyable. Je l'illustre parce que souvent, nous avons l'impression que nos grands groupes sont ceux qui sont les plus armés. Nous avons fait au début de l'histoire du cyber des diagnostics cybersécurité ou maturité cyber sur ce que nous appelons les ETI, les entreprises de taille intermédiaire donc les plus grosses entreprises en dessous des grands groupes en Nouvelle-Aquitaine. Nous leur avons dit, nous venons vous payer deux jours de diagnostic, simplement il faut que votre DSI soit là et que nous interagissions. Et sans jugement de valeur, cela a été catastrophique. C'était Orange Cyber qui nous accompagnait et le chargé de mission nous a raconté un jour que quand il a commencé le diagnostic et qu'il a pris la main en 30 secondes sur le système d'information de l'ETI, le DSI a failli s'évanouir. Donc vous voyez la réalité, ce n'est pas parce qu'on est une petite commune, quand je dis petite encore une fois juste par le nombre d'habitants, jusqu'à un grand groupe, qu'il y en a qui sont mieux armés que les autres. Ce n'est pas cela du tout. Et donc nous avons une dimension de sensibilisation qui est fondamentale.

Derrière, il faut mettre les moyens. Évidemment, prendre une solution et être bien protégé coûte cher. Mais, quand on subit une attaque, le coût est encore plus élevé.

Vous m'avez interrogé sur quels sont les membres fondateurs et pourquoi cette dynamique ? Je faisais référence au travail partenarial de longue date, donc parmi les membres fondateurs du campus, il y a la région Nouvelle-Aquitaine, notre agence de développement d'innovation, ADI, le GIP ACYMA et cybermalveillance.gouv.fr qui est avec nous, et le CLUSIR, qui est la déclinaison du CLUSIF à l'échelle régionale. Nous voyons qu'avoir réussi à réunir tout le monde dans les membres fondateurs, fait qu'aujourd'hui nous commençons à avoir une certaine envergure, en tout cas la capacité à être légitime et reconnu par ce que nous faisons.

Sur le CSIRT alors, quel moyen, comment ça marche ?

Notre centre de réponses à incidents est le cœur du réacteur. Ce campus a été créé pour les entreprises et les collectivités, quelle que soit leur taille, quelle que soit leur nature. Ce centre de réponses à incidents a été créé le 1er avril de l'année dernière. Cela fait 16 mois. Nous avons traité 310 cas depuis cette date d'ouverture et 150 depuis le 1er janvier 2024. Nous avons déjà décrit les différents types d'attaques. Je rajouterai ce que nous appelons le défacement de sites. Cela consiste à prendre la main sur votre site Internet et à y mettre autre chose, une image. Sur les 310 cas à traiter, c'est 70 % du privé et 30 % du public collectivité. Mais nous avons eu aussi à faire face à des attaques sur des établissements hospitaliers, par exemple.

Évidemment, nous sommes là pour y répondre. Il faut quand même parler de chiffres, car cela coûte. Nous avons bénéficié d'un soutien financier de l'État qui a accompagné le début des fameux CSIRT en France. Alors comme je n'aime pas le nom, je préfère parler de Centre de Réponses à Incidents. Le budget : un million d'euros sur trois ans, dont 300.000 euros de l'État. Le conseil régional met 600.000 euros de subventions de fonctionnement par an. C'est un élément important, mais cela nous oblige à penser le modèle économique de ces campus pour les prochaines années, parce que nous le voyons bien, la puissance publique ne va pas pouvoir faire cela toute seule.

## Luc DERRIANO

L'ANSSI a accompagné et financé la naissance de ces centres de réponse en région. L'ANSSI, c'est combien de personnes aujourd'hui ? C'est combien de moyens ? Qu'est-ce que vous mettez en œuvre pour nos territoires ? Et puis vous reviendrez plus spécifiquement sur un exemple, le kit de simulation d'exercice. Mais dans un premier temps, donc l'ANSSI, comment ça marche ?

## Célia NOWAK

Vous l'avez déjà mentionné, l'ANSSI, c'est l'autorité nationale en matière de cybersécurité et cyberdéfense. Aujourd'hui, nous sommes environ 600 agents. La

plupart sont à Paris, puisque nous sommes une agence qui appartient aux services du Premier ministre. Et nous sommes rattachés au SGDSN, qui est le Secrétaire général pour la Défense et la Sécurité nationale. Nos agents réalisent quatre grandes missions. Une mission de défense. C'est d'ailleurs pour cela qu'on nous appelle parfois les cyberpompiers de l'État. Et comme je le disais, nous avons historiquement des bénéficiaires qui sont des OIV, des opérateurs d'importance vitaux, et également les services de l'État. Maintenant, nous traitons aussi d'autres victimes, des collectivités qui nous appellent, des entreprises qui ne sont pas forcément régulées.

Notre première mission est donc de venir appuyer les victimes de cyberattaques. La seconde mission, est de connaître la menace cyber grâce aux éléments qui nous sont remontés nous comprenons effectivement quelle menace on doit faire face et comment y réagir. Il y a aussi une mission de partage de la menace qui se concrétise par des panoramas que nous publions chaque année via des guides, etc. Et pour finir, il y a aussi une mission d'accompagnement des territoires à augmenter leur niveau de cybersécurité, les entreprises, etc.

Nous sommes plutôt une agence centralisée. Mais, depuis 2017, il y existe également des délégations régionales., représentés par un ou deux délégués. Pour ma part, je représente le binôme pour la PACA. Nous avons un rôle de représentation de l'ANSSI en région ainsi qu'un rôle de facilitateur d'initiatives qui se créent sur les territoires. Vous parliez du campus en Nouvelle-Aquitaine. Ce sont des dispositifs avec lesquels nous allons travailler.. Nous allons pouvoir mettre en lien les acteurs des territoires avec ces dispositifs qui existent déjà. Nous avons aussi cette mission de démultiplier l'action de l'agence. En résumé, les missions de l'ANSSI.

Pourquoi les collectivités sont-elles attaquées ? Nous constatons qu'il y a deux types de grandes menaces, la menace d'espionnage, ce sont plutôt des attaques qui sont ciblées pour récupérer de la donnée stratégique, et la fameuse cybercriminalité qui répond à des logiques lucratives. Ici, on va avoir des attaques qui sont plutôt opportunistes. Pour que ce soit un peu plus illustratif, prenez l'image de la pêche au chalut. Quelqu'un va lancer son filet et puis il va le remonter. Il va voir ce qui a mordu

à l'hameçon. Finalement, ici, vous pouvez être dans ce filet parce que vous n'aviez pas fermé la porte ou la fenêtre de votre mairie et l'attaquant a réussi à s'infiltrer. Et ce qu'il faut retenir de cela, c'est que nous avons une tendance à avoir des menaces qui sont diffuses : vous n'étiez pas forcément la cible initiale, mais effectivement vous allez devenir la victime. Donc retenez bien cela. La bonne nouvelle face à cette mauvaise nouvelle, c'est que justement en mettant en place de l'hygiène informatique, nous allons fermer ces fameuses portes et fenêtres en mettant des antivirus, en mettant en place des pare-feux. C'est le côté technique. Mais aussi en mettant en place de la sensibilisation aux agents pour qu'ils évitent de cliquer sur des mails de phishing. Il faut mettre en place une organisation, une gouvernance cyber, que ce soit pour la préparation, la prévention, mais aussi la réaction à la gestion de crise. Concernant l'hygiène informatique, il existe beaucoup de ressources. Cybermalveillance est une mine d'or pour récupérer des kits, des fiches réflexes, etc.

L'ANSSI met aussi à disposition de nombreux guides. Je peux vous en proposer deux. Le premier se nomme « la cybersécurité en 13 questions pour les TPE-PME ». C'est un guide qui est notamment à destination d'un public n'ayant pas de notion technique. Lire ce guide vous permet de vous situer, d'évaluer votre niveau de maturité cyber vis-à-vis des grands volets qui vous sont proposés.

Il y a également un guide sur l'hygiène informatique en 42 points qui peut être utilisé par vos équipes techniques ou vos prestataires. Nous avons également un MOOCs si vous voulez aller plus loin.

Concernant l'hygiène informatique, les questions sous-jacentes sont « comment la mettre en place ? Comment puis-je évaluer mon niveau de maturité cyber ?

Côté ANSSI, nous sommes en train de lancer un dispositif pour répondre à ces enjeux : MonAideCyber. MonAideCyber est un outil d'évaluation que nous mettons à disposition, donc un diagnostic cyber. Pendant 1h30, avec un aidant qui a été formé par l'ANSSI, vous allez pouvoir faire le tour de votre niveau de préparation : où vous

en êtes ? Qu'est-ce que vous avez mis en place ? Vous pourrez ainsi disposer d'une vision globale de votre niveau de cybersécurité.

Ce qui est intéressant surtout, c'est que six mesures prioritaires à mettre en place dans les six prochains mois vous sont proposées. Et c'est ce qui manquait finalement aujourd'hui. On savait parfois qu'on était mauvais, il n'y avait pas besoin de faire un diagnostic pour ça, mais on ne savait pas comment aller plus loin. Et donc là, ce sont des mesures qui sont d'ailleurs issues des guides que je vous ai cités, des bonnes pratiques à mettre en place.

Vous pouvez vous rapprocher de l'équipe Mon Aide cyber ou alors des délégués régionaux. Il y a une carte des délégués qui est disponible sur le site de l'ANSSI.

J'ai beaucoup parlé de prévention, de préparation et effectivement parlons aussi de réaction à la gestion de crise cyber. Le risque zéro n'existant malheureusement pas, il s'agit alors d'éviter qu'un petit incident devienne une crise ingérable. Or, il y a plusieurs façons pour bien réagir.

Il convient déjà de préparer un dispositif de réaction. Je vois sur le terrain, notamment en PACA, de plus en plus de collectivités souhaitant bénéficier de conseils pour intégrer le risque cyber au sein de leur PCS (Plan communal de sauvegarde). Des travaux sont ainsi menés, avec comme première réflexion, se demander « que faire en cas d'attaque » pour constituer une fiche réflexe.

Qui je dois appeler ? Cela peut être un CSIRT régional ou mon prestataire de réponses à incidents. Cela dépend de votre contexte.

Que dois-je faire pour assurer ma continuité d'activité ?

Il faut par ailleurs souligner que pour être prêt, il faut aussi s'entraîner de crise. Nous le faisons pour les risques naturels, les incendies, pourquoi pas pour la cyber ?

Et en ce sens côté l'ANSSI, nous avons également mis en place plusieurs outils d'accompagnement. Il y a un guide qui existe déjà depuis quelques années sur la création d'exercice. Puis depuis un an, nous avons publié un kit d'exercice qui comprend un scénario de gestion de crise adapté aux spécificités des collectivités.

Un panel de documents accompagne cela, avec l'objectif de vous aider à accélérer votre organisation d'exercice. Nous savons en effet que cela est consommateur en temps, c'est d'ailleurs aussi pour cela qu'il faut parfois faire appel à un prestataire.

L'idée du kit est de permettre à une personne qui n'est pas forcément du monde de la cyber d'organiser l'exercice. Donc il y a un panel d'outils, de documents qui expliquent quelles sont les grandes étapes. Il y a également des fiches pour les joueurs, des fiches pour les observateurs qui leur donnent le rôle à tenir.

Mais si vous ne voulez pas vous lancer de suite dans un exercice grandeur nature, il y a également des outils qui vous permettent d'avoir au moins un exercice de réflexion : vous pourrez ainsi être guidés et vous questionner, en petit groupe, sur les actions à mener en cas d'attaque.

C'est une autre approche de l'exercice dit « de simulation » dont vous pouvez saisir. En tout cas, En tout cas, tout cela est bénéfique, déjà pour éviter le stress Et ainsi éviter de créer une crise dans la crise. Nous voyons en effet que subir une attaque reste une expérience très traumatisante. C'est quelque chose qui épuise les équipes, qui créé des tensions. La préparation peut aussi permettre de répondre à cette problématique.

## Luc DERRIANO

---

Lire les guides, c'est bien, mais s'entraîner, expérimenter, faire de la mise en pratique, c'est mieux ! Et là en plus vous le faites sans risque puisque vous êtes dans une simulation, un exercice. Alors il y a d'autres éléments, d'autres dispositifs d'accompagnement des territoires et là je me tourne à nouveau vers vous Amandine DEL AMO. Sur [cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), il y a la sensibilisation, des outils de diagnostic, des labels Expert Cyber, des études pour les petites communes. Est-ce que vous pouvez nous présenter vos principaux dispositifs utiles à connaître quand on est une commune ?

## Amandine DEL-AMO

---

Pour compléter les exercices de crise, il est important de sensibiliser vos équipes pour qu'elles soient préparées, et qu'elles aient conscience des risques pour la collectivité. En cliquant sur un lien malencontreux, il peut y avoir des incidences. Donc pour acculturer, nous avons lancé une e-sensibilisation gratuite il y a quelques mois à destination des collectivités qui est disponible via le CNFPT. Et puis également pour les collectivités qui souhaiteraient pouvoir l'héberger en propre au sein de leurs systèmes d'information. Elles peuvent nous demander les fichiers SCORM ou HTML5 si elles le souhaitent.

Cette e-sensibilisation est vraiment faite pour comprendre les risques et s'approprier les bonnes pratiques. C'est une première étape qui convient à tout agent. Même un agent qui n'est pas forcément devant son écran peut être intéressé par ce type d'e-sensibilisation qui pourrait être obligatoire dans un parcours d'un nouvel arrivant, par exemple.

Nous mettons à disposition ces outils gratuits qui ne coûtent rien à votre collectivité mais qui sont indispensables aujourd'hui pour sensibiliser.

Nous avons ensuite, pour ceux qui le souhaitent, des nouvelles mallettes cyber pour créer des ateliers de sensibilisation avec un jeu de cartes. C'est un outil supplémentaire qui est à votre disposition.

Nous avons aussi des outils en termes de communication. Faire une sensibilisation à un instant T c'est bien, mais il faut absolument parler du sujet dans la durée. Nous avons pour cela une méthode de sensibilisation que nous avons créée avec le groupe de travail, il y a quelque temps maintenant mais qui est toujours d'actualité et que vous pouvez réutiliser. C'est un plan d'action, un plan de communication pour parler de la cyber avec des outils. Donc n'hésitez pas là encore à vous en emparer pour le donner à votre service communication et qu'il puisse parler du sujet régulièrement.

Cela complète les actions du cyber mois que nous pilotons pour la deuxième année. Si votre entité souhaite s'engager sur le cyber mois et parler de cybersécurité à cette occasion, durant cet événement européen, en octobre, n'hésitez pas nous ouvrons cette année le collectif au plus grand nombre. L'idée est que toute entité qui souhaite s'engager puisse avoir les informations en amont. Nous avons une première réunion le 6 juin pour présenter les grandes lignes de cette campagne du cyber mois 2024. Rapprochez-vous de Luc pour pouvoir vous y associer si vous le souhaitez et utilisez tous ces supports qui vont vous être fournis pour pouvoir parler de la cybersécurité tout au long de l'année.

## Luc DERRIANO

Revenons sur le Label Exper Cyber. La demande des collectivités était d'avoir des prestataires dans lesquels nous pouvons avoir un peu plus confiance.

## Amandine DEL AMO

C'est très important en effet. Nous nous rendons compte que naturellement, les collectivités vont vers leur prestataire historique qui les accompagne, qui a mis en place le système informatique de la mairie. Mais malheureusement, ce prestataire

n'est pas forcément au meilleur niveau en matière de cybersécurité. Et il est important de vérifier que ce qu'il a mis en place tient la route.

Nous nous rendons compte également que les sauvegardes ne sont pas faites, que les mises à jour ne fonctionnent pas, etc. Il est donc très important de vous assurer que votre prestataire local ait les compétences pour assurer la sécurité de votre collectivité et des données que vous hébergez. Pour cela, vous pouvez vérifier s'il est labellisé Expert Cyber ou s'il est certifié ANSSI.

Ensuite, vous pouvez aussi faire des tests, vérifier que votre sauvegarde fonctionne, vérifier que vos mises à jour sont bien faites pour patcher toutes les failles, puisqu'il y a des failles dans les systèmes. Il faut aussi s'assurer que ce soit fait parce que les sauvegardes vont être le seul moyen pour vous de revenir à la normale si vous êtes attaqué, et vous avez compris, allez être attaqué...

## Luc DERRIANO

Gouverner c'est prévoir. Nous avons vu tout à l'heure avec l'exemple de la Nouvelle Aquitaine que les acteurs locaux se préparent à mettre en place un Cyber Campus, à mettre en place toute cette chaîne humaine depuis 2016. L'Europe se prépare aussi. Jean-Michel, vous avez accepté de nous parler de la transposition de la directive NIS V2, pour Network & Information Security.

## Jean-Michel MORER

Pour information, une directive européenne met à peu près quatre ans à être élaborée, puis il faut compter deux à trois ans pour la transposer en droit français et ensuite se mettre en mouvement. Malgré de tels délais qui peuvent paraître inappropriés au regard des urgences immédiates dont il faut se prémunir, il est important effectivement que l'Europe se préoccupe de cette priorité absolue.

Ceci étant, une fois ce constat posé, lorsque nous voyons le développement de l'IA, nous constatons que les risques comme leur prévision sur quatre à cinq ans, vont croître et aller parfois bien au-delà de nos estimations.

Il apparaît que clairement, NIS2 est une injonction, en qualité de représentant des collectivités à la parole libérée et libre, je dirais qu'il est important de donner à nos communes les moyens de répondre à de telles injonctions, c'est bien là où le bas blesse.

Je me rappelle avoir négocié au nom des collectivités avec d'autres associations et même obtenu gain de cause avec Amélie de MONTCHALIN, ministre de la Transformation et de la Fonction publiques dans le cadre du Plan de relance des moyens pour mieux armer la cybersécurité, alors oubliée. Nous avons même positionné l'ANSSI en tête de pont ; force est de constater que nous avons été quelque peu déçus sur le terrain des actions concrètes qui ont suivi, notamment sur les problématiques de seuil pour qu'une collectivité puisse initier un parcours de sécurisation.

La directive européenne, comme toute directive est assez technocratique, or dans le panel des différentes collectivités, surtout en France, il y a plus que des nuances. Nous pourrions faire une exégèse juridique intéressante, mais uniquement si nous avons du temps à perdre me semble-t'il.

NIS2 existe, c'est un fait, j'espère tout d'abord qu'une de ses conséquences directes sera de donner à l'ANSSI des effectifs supplémentaires, tant en ce domaine la question des moyens est cruciale, également d'ailleurs pour toutes nos collectivités.

Je tiens à saluer le rôle de l'ANSSI concernant la protection des opérateurs de télécommunication qui a été de première importance au moment du Covid, parce qu'il y a eu beaucoup d'attaques, et la période actuelle n'est pas plus reposante, compte tenu du contexte pré olympique et de la situation géo politique

internationale plus que compliquée. Il est urgent de se mettre en mouvement en cohérence, c'est là qu'il convient de préciser que la sécurité, c'est un peu comme la santé, il y a toute une chaîne d'acteurs à mettre en mouvement, chaque maillon est important et essentiel, aussi mieux vaut complémentarité que concurrence.

C'est un peu l'inquiétude que nous avons aujourd'hui sur la mise en place des différentes instances et maillons. Je suis un élu de Seine-et-Marne, la région Île-de-France a fait un choix différent des autres régions par rapport au CSIRT. C'est la seule qui a délégué son CSIRT à une entreprise privée. Je tiens à le signaler, sans commenter cette décision. Constat cependant, nous ne sommes pas plus en avance que les autres régions, loin s'en faut !

Je pense cependant qu'il faut privilégier cohérence dans l'action collective et montée en compétence et puissance des différentes collectivités, des ETI, des personnels, en fait de tout l'écosystème, y compris au niveau local. En région parisienne, nous partons du principe, que quand nous habitons la grande couronne, il n'y a pas de savoir-faire, et que nous devons absolument passer par le parapluie de quelques grandes entreprises spécialisées dans la sécurité, qui en théorie sont très bonnes, mais en pratique pas toujours, et qui propose des coûts d'intervention parfois démesurés.

Or il y a dans nos territoires, de véritables savoir-faire et des entreprises compétentes qu'il faut challenger et valoriser. Pour faire effectivement résilience, nous avons besoin de tout le monde et il est important non d'avoir un livre de recettes mais d'acquérir une culture du risque qui doit être collaborative, intégrant le fait que le risque de demain n'est pas celui d'hier, d'autant qu'avec l'IA tout va évoluer.

Il faut donc mettre en résonance tous les acteurs et les inciter à aller dans le même sens et à travailler ensemble. Et c'est aussi pour cela qu'en tant qu'association d'élus l'APVF a trouvé plus pertinent de soutenir et d'accompagner cybermalveillance.fr dans l'action remarquable de vulgarisation, d'acculturation, qu'ils mènent que de mettre notre grain de sel.

Nous ne voulons pas refaire quinze fois les mêmes outils, surtout et notamment lorsqu'ils sont excellents. Par contre, au niveau des élus, nous avons une vraie connaissance de nos territoires, de leurs contraintes et potentialités.

Aussi, les régions, ont un rôle important de mise en réseau, d'animation, de moyens à déployer mais soulignons-le, parfois certaines petites structures sont bien mieux protégées que des grandes. C'est cette mise en mouvement, cette cohérence, qui ont amené des associations d'élus qui se rencontraient pour négocier avec l'État, notamment sur l'inclusion numérique à vouloir se regrouper et travailler ensemble.

Pour ma part, je suis venu à discuter cybersécurité par l'inclusion numérique ayant beaucoup travaillé avec les équipes de Cédric O notamment sur le déploiement des conseillers numériques France Service ... Ce souci de travailler en équipe, d'avoir ainsi une vue enrichie de nos différences expériences et strates nous permet d'avoir une vision assez claire de la réalité du terrain et des enjeux à relever.

C'est ainsi qu'est né la Belle Alliance, plus formellement d'ailleurs au moment de la dernière élection présidentielle, afin d'établir de manière collaborative une plateforme de propositions communes s'adressant à la politique numérique territoriale à déployer pour le pays.

A un moment donné, nous nous sommes rendu compte dans le cadre de la transformation numérique des territoires que l'État nous disait globalement ce qu'il allait faire et n'écoutait ni nos attentes, ni nos problèmes et surtout que l'État ne proposait pas d'action globale mais partait en ordre séparé, ministère par ministère et quelquefois sur des standards et solutions déjà dépassés et non inter opérables, parfois même quelque peu hors sol. L'association Déclica dressé le panorama de toutes les injonctions de l'État et leur échéancier auxquelles nos collectivités devaient répondre en matière numérique. Avec la Belle Alliance, ensemble, nous avons eu une parole commune et sommes devenus une véritable force de propositions concrètes. C'est ce qui a mené l'État à nous considérer différemment, à

constater que nous étions capables d'idées et de dynamiques. C'est toute la richesse de ce collectif très informel, collaboratif qui s'appelle la Belle Alliance.

Lors de la dernière présidentielle, nous avons ainsi élaboré un manifeste reposant sur le socle de nos compromis, et les idées et valeurs que nous partagions. Nous avons retenu pour chaque thématique ou proposition le plus petit commun dénominateur, il est important de faire se rencontrer et travailler ensemble des acteurs qui ne se rencontrent pas habituellement pour produire du commun et du partagé

C'est pourquoi il me semble important de travailler avec des prestataires essentiels de l'éco système tel Stormshield ou d'autres, ils ont un vrai savoir-faire en sécurité. Or partant de là ils estiment qu'il n'y a aucun intérêt à être labellisés, c'est dommage et dommageable. Il est essentiel que la sécurité informatique et ses professionnels soient présents dans tous les territoires ... Ce qui nécessite à la fois des acteurs privés mais également au niveau de nos collectivités de nous regrouper, l'échelon le plus adéquat dépend tout simplement des nuances de nos territoires : région, département, intercommunalité, syndicat ... peu importe. L'important est globalement de travailler en équipe et d'aller vers l'avant, d'être en cohérence et de faire monter les compétences globales.

Il faut faire que nous soyons en capacité de déployer toute une chaîne de défense ; nous attendons de l'État qu'il s'inscrive en chef d'orchestre, parce que la dorsale, la doctrine, doivent être apportées par les compétences de l'État, nous avons besoin de l'ANSSI et de moyens logistiques et humains qu'elle peut réunir et qu'elle peut déployer.

Je crois que l'important aujourd'hui est de dire que les collectivités sont matures et qu'elles n'ont pas besoin d'injonctions, de directives qui nécessitent une inertie importante avant d'être efficaces. La labellisation est une piste intéressante mais ne constitue pas le parapluie et le bouclier absolu. Et c'est pour cela que devons

acquérir culture du risque et travail collaboratif ... Il est essentiel de disposer de personnes d'univers différents qui dialoguent, échangent sur la cybersécurité.

La responsabilité des régions par rapport à cette mission d'animation éminente essentielle est importante. Il faut mettre en dialogue et en tension toutes les énergies et les potentialités des territoires. Une fois que nous en serons arrivés là, une grande partie du chemin aura été accompli.

## Luc DERRIANO

---

L'Avicca a également signé ce courrier commun des associations d'élus demandant notamment une étude d'impact sur la mise en œuvre de NIS 2 en réclamant des moyens humains et matériels pour pouvoir répondre à la mise en place de la directive. Cette demande a été entendue puisque cette étude d'impact est inscrite dans le projet de transposition actuel.

Nous arrivons maintenant à la fin de cette table ronde et je vais demander à chacun un mot de conclusion. Je vais d'abord me tourner vers les organismes qui représentent l'État et leur demander ce qu'ils attendent des territoires pour renforcer cette défense commune.

## Célia NOWAK

---

En définitif, nous pouvons prendre la question dans les deux sens. Que faire, et qu'attendez-vous de nous ? Qu'est-ce que vous pouvez aussi attendre de nous ?

Je crois, d'abord qu'il y a un besoin de coordination important, parce que chacun porte la cyber de son côté. Il n'y a pas que l'ANSSI qui la porte, il y a aussi Cybermalveillance, la gendarmerie, la police, bien entendu le privé et cela fait effectivement plusieurs années que nous travaillons avec eux. Vous l'avez compris, il y a beaucoup d'acteurs. Aussi, nous pouvons attendre de l'État qu'il soit un coordinateur. Et justement, sur les territoires, c'est parfois le rôle des délégués

régionaux de l'ANSSI. Pour vous donner une illustration en PACA, nous avons créé des instances de coordination inter-services. Et puis, nous travaillons également de concert avec les acteurs du territoire, les collectivités, les syndicats. Ils ont des bonnes idées et nous avons envie de les aider à les faire émerger. C'était d'ailleurs l'une des volontés avec un dispositif local de l'ANSSI.

De notre côté, que pouvons-nous attendre de vous ? Ce sont vos idées et aussi une logique de mutualisation. Nous le voyons aujourd'hui, notamment pour répondre aux besoins des plus petites communes qui n'ont pas les moyens, des initiatives se mettent en place soit par des syndicats, notamment les OPSN soit par de plus grandes collectivités.

Pour vous donner un exemple, dans la région PACA, dans les Hautes-Alpes (05), qui est un territoire rural où il y a un tissu économique moins important que sur la côte méditerranéenne, le Département a décidé de mettre à disposition des plus petits des services. Ils font du diagnostic MonAideCyber, des audits et ils vont effectivement assister les communes. Ce sont des initiatives que nous pouvons accompagner pour les structurer et pour qu'ensemble nous soyons plus forts et mieux préparés.

## Luc DERRIANO

---

Concernant les délégués régionaux de l'ANSSI, nous sommes très contents qu'il y ait un nom en face de chaque case, ce qui n'a pas toujours été le cas. Félicitation pour cela. Ce n'est pas simple de recruter, nous l'avons bien compris. Je pose la même question à [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr).

## Amandine DEL-AMO

---

Nous essayons, via notre groupe de travail, de prendre vos besoins, de les identifier pour travailler ensemble dessus. Donc n'hésitez pas à remonter à Luc ce qui vous serait nécessaire au quotidien pour que nous puissions vous l'apporter. C'est une première chose.

Deuxièmement, il faut que vous vous sécurisiez d'une manière ou d'une autre. Il y a beaucoup d'initiatives étatiques qui sont mises en œuvre dans les territoires. Donc, rapprochez-vous des CSIRT, des OPSN. Il y a des offres qui sont en train de se mettre en place, d'autres sont en cours d'élaboration pour mutualiser davantage et apporter des outils avec des prix adaptés aux collectivités.

Troisièmement, restez en veille sur le sujet : des solutions existent dont vous n'êtes pas forcément au courant. Nous sommes à votre écoute si vous avez des besoins.

## Luc DERRIANO

---

Maintenant, je vais me tourner vers les représentants des territoires. Réciproquement, qu'est-ce que les territoires peuvent demander aux organismes de l'État ?

## Mathieu HAZOUARD

---

D'abord, je voudrais réparer un oubli, je n'ai pas cité l'ANSSI dans les membres fondateurs du Campus cyber. Simplement en plus dire que le directeur et le directeur adjoint du campus cyber Nouvelle-Aquitaine sont les deux derniers délégués de l'ANSSI en région Nouvelle-Aquitaine ce qui montre une certaine porosité. Mais en revanche j'aimerais bien que l'ANSSI se dote, en tout cas qu'on lui donne plus de moyens.

Le premier point qui me semble important et aussi à l'aune de ce que nous avons entendu, c'est qu'il y a une nécessité de cohérence d'action et de visibilité. Vous avez vu déjà tout ce que nous avons mis en avant. Nous allons vous annoncer dans quelques semaines la mise en place du « 17 cyber ». Ce n'est pas encore tout à fait prêt et nous espérons pouvoir en parler ce matin. Mais pourquoi je dis ça ? C'est qu'après, il faut simplement mieux saisir le qui fait quoi ? C'est déjà plutôt pas mal avec cette porte d'entrée que nous hiérarchisons entre un campus régional, et

même des acteurs un peu plus locaux. Par exemple, en Nouvelle-Aquitaine, nous avons mis en place des centres de réponses locaux. Voilà une réalité territoriale plus fine. Il faut simplement qu'un maire ou un chef d'entreprise sache à qui s'adresser, soit pour une problématique post-attaque, soit très en amont pour simplement se protéger. Cette dimension de cohérence me semble essentielle.

Le dernier point, alors peut-être que je vais être un peu orthogonal par rapport à votre position, Monsieur MORER, sur NIS2. J'entends les vraies difficultés des collectivités et de tous les acteurs qui vont être concernés par le fait de pouvoir se mettre à niveau. Comment cela va-t-il se passer en termes organisationnels et financiers ? Mais je pense que c'est fondamental et pourquoi ? Nous sommes d'abord dans un temps où nous parlons d'Europe, d'élections européennes. Et je trouve que c'est une réalité concrète de ce que peut faire un acteur, l'Union européenne, en imposant aussi à l'ensemble des acteurs sur le territoire de se protéger. Je dis que c'est fondamental, parce que nous sommes en retard, c'est qu'à chaque fois nous reculons. Et si nous n'avons pas le cadre, nous allons encore procrastiner et nous dire que ce n'est pas si grave. C'est ma crainte.

Donc, je pense que poser le cadre est important. Et qu'il faut qu'ensemble, nous réfléchissions aux moyens que nous y mettons. En Nouvelle-Aquitaine, nous venons de décider depuis six mois de mettre en place des écosocioconditionnalités. Beaucoup de structures le font. Donc, nous regardons l'impact sociétal et environnemental des aides, des structures à qui nous apportons nos aides. Mais au regard de cela, nous avons aussi mis en place la cyberconditionnalité. Quand la Région est sollicitée pour une aide financière, nous demandons à la structure où elle en est-elle par rapport à la protection de ses données, de ses savoirs faire ?

On nous a dit, c'est coercitif, c'est impossible, il ne faut pas. Nous avons dit, nous venons vous accompagner car vous n'êtes pas protégés, mais nous n'allons pas vous donner l'aide maintenant. Vous allez voir le Campus cyber qui va vous dire vers quel acteur vous tourner et qui va être un ambassadeur pour vous accompagner. Je

pense que ce cadre-là est fondamental. C'est aussi un cadre de confiance que nous apporterons à tout le monde.

Je termine par la question des moyens que nous y mettons collectivement pour faire en sorte que les modèles que nous avons créés soient pérennes. Il faut vraiment que l'ANSSI, Cybermalveillance.gouv.fr, les régions se mettent tous autour de la table. La Belle Alliance est un cadre. Il faut qu'ensemble, chacun mette cette contribution financière parce que ce sont des éléments importants. Et là, nous aurons réussi l'exercice.

## Luc DERRIANO

Il faut quand même dire que dans la plateforme commune de la Belle Alliance nous avons notamment ciblé les CSIRT en disant que l'occasion serait ratée si nous ne profitons pas de la directive NIS V2 pour prolonger les moyens mis à disposition sur ces CSIRT pour 2 à 3 ans seulement.

## Jean-Michel MORER

Effectivement j'ai peut-être été quelque peu caricatural mais ma conviction est qu'il ne faut pas attendre la directive NIS 2 pour agir, la sécurité informatique n'est certainement pas un cadre encadrant une photo, la problématique de la cybersécurité et qu'elle est tout le temps en mouvement, c'est plus de la vidéo qu'un cliché.

Si l'on n'intègre pas cette réalité NIS 2 risque de devenir un arrêt sur image. Nous ne devons pas attendre que la directive nous rattrape, mais nous situer dans l'anticipation et ne jamais oublier qu'une directive doit être régulièrement mise à jour pour être utile et efficace.

Notre feuille de route en ce domaine doit être claire, graduelle et n'oublier aucun maillon de la chaîne. Une des problématiques est le qui fait quoi ? Les maillons les plus compliqués à mettre en place, sont les maillons intermédiaires.

Au niveau de la Seine-et-Marne, nous avons initié des ateliers avec nos OPSN en faisant travailler ensemble des binômes, maire / DGS. Nous avons eu comme participants la plus grande commune de Seine-et-Marne, plus de 55 000 habitants et une des plus petites comprenant 148 habitants, dans le même atelier. C'était hyper intéressant. Pour beaucoup de participants à ces ateliers, plus de 25 collectivités, la question essentielle était : à qui je vais m'adresser ?

Il faut que nous soulevions le capot et que, techniquement, nous ne parlons plus de conduite à avoir, mais déployons des solutions opérationnelles qui tiennent compte du budget de la commune. L'état doit accompagner ce mouvement et mettre en place les conditions d'un dialogue territorial constructif afin que chacun travaille en synergie.

NIS 2 est utile, c'est un cadre. Mais attention ne l'attendons pas pour nous mettre en mouvement, chacun à sa place car tous les maillons de la chaîne sont importants et c'est la chaîne qui fait sens.

Luc DERRIANO

---

Vous l'avez compris, le sujet n'est pas épuisé. Merci à toutes et à tous pour votre participation et votre écoute attentive.