

LA CYBER RÉSILIENCE



© Freepik.com

Même en matière numérique, on peut parler de « territoires »

Les brigades,

pivot de la cyber résilience des territoires

L'espace numérique est (faussement) réputé sans frontière. La déterritorialisation induite par son architecture distribuée et sa remise en cause du cadre espace-temps ont pu laisser croire que la notion même de territoire était obsolète. Au vrai, il n'en est rien. Les exemples de la Silicon Valley ou du Pôle cyberdéfense de la Bretagne soulignent combien les territoires peuvent encore avoir du sens, ne serait-ce que pour catalyser la transformation numérique. Les territoires sont aussi des espaces pertinents pour développer une solidarité face au risque numérique. Le réseau des brigades est un atout pour leur cyber résilience.

Parce qu'il fallait agir en vertu de priorités, la cybersécurité, condition essentielle du développement harmonieux et sûr de l'espace numérique, a été principalement conçue avec une approche « verticale », sectorielle, en privilégiant la protection des systèmes les plus sensibles : opérateurs d'importance vitale (OIV), opérateurs de service essentiel (OSE), fournisseurs de service numériques (FSN) et leurs sous-traitants. De nouvelles mesures ont été décidées par le Président de la République, le 18 février, notamment au profit des collectivités territoriales et des établissements de santé, particulièrement touchés par des cyberattaques depuis la crise de

la Covid-19. C'est une première action en faveur d'organismes qui échappaient jusqu'alors aux « écrans radar ». Mais il faut aller encore plus loin, car la cybersécurité n'a pas encore été prise suffisamment en compte de manière « horizontale », en ayant pour objectif d'unir dans un même destin numérique les acteurs qui contribuent à la dynamique des territoires.

Cette double conception est à l'origine du Forum international de la cybersécurité (FIC) qui a toujours mis au cœur des réflexions l'écosystème numérique dans sa dimension globale, systémique et réticulaire. Les territoires ont parfois développé des initiatives thématiques, comme en témoigne le Pôle cyberdéfense de la Bretagne, très spécialisé comme son nom l'indique, qui se déploie sur un territoire mais pas nécessairement au profit de la cybersécurité de celui-ci. Des initiatives transversales sont également lancées,



MARC WATIN-AUGOUARD

Général d'armée (2s) créateur du Fic (Forum International de la Cybersécurité) et président de l'Institut National pour la Cybersécurité et la Résilience des Territoires

comme le projet très attendu du Campus Cyber, « Beer-Sheva à la française », qui devrait voir le jour, à l'automne, dans le quartier de la Défense. Dans ce dernier cas, le regroupement inédit des compétences n'a pas véritablement d'application territoriale, même s'il suscite l'émergence de campus régionaux.

Il reste donc encore du chemin à parcourir pour développer la cyberrésilience des territoires qui ne sont pas inclus dans une « plaque numérique » et où se côtoient de nombreuses collectivités territoriales, PME, TPE ou ETI, souvent victimes de prédateurs. Celles-ci sont alors bien seules dans leur malheur. Dans ce contexte est né l'Institut National de la Cybersécurité et la Résilience des Territoires (IN.CRT), qui a pris racine à Vannes. Il a pour ambition de compléter les efforts entrepris à l'échelon national en termes de cybersécurité et d'apporter un soutien aux actions menées à l'échelon local. Les relations qu'il doit tisser avec la gendarmerie, notamment avec les brigades, seront de nature à renforcer la « trame de résilience ».

« Tous pour un, un pour tous » pourrait être le mot d'ordre guidant l'action qu'il convient de mettre en œuvre afin de développer une cybersécurité collective et collaborative. Ce n'est pas un hasard s'il s'agit du thème du FIC 2021. Sans confusion des genres, car chacun suit sa propre logique, il est nécessaire

de rapprocher tous les acteurs qui se reconnaissent dans un territoire et créer ainsi une solidarité sans laquelle il n'y aura pas cybersécurité durable. Ce n'est pas une option, c'est une exigence ! Avec son réseau de plus de 3 000 brigades, la gendarmerie a l'opportunité de jouer un rôle essentiel en étant le point d'entrée le plus déconcentré d'organismes centraux (ANSSI, Cybermalveillance, etc.) et d'offrir, grâce au réseau Cybergend une capacité de prévention et d'action qui puise sa force dans le maillage, mais aussi dans la subsidiarité des compétences, au fur et à mesure qu'elles deviennent rares. La proximité, inventée il y a trois siècles lors de la création de brigades, est aujourd'hui une demande pressante de la part des citoyens, des élus locaux. En s'appuyant sur le socle des unités, la gendarmerie doit et peut satisfaire la demande par une offre qui, sans intervenir dans la résolution technique du problème (ce n'est pas son rôle), doit permettre à la victime de ne jamais se sentir abandonnée¹. Il ne s'agit pas d'une question d'opportunité mais de survie. Alors que la cybercriminalité devient la criminalité du XXI^e siècle², la légitimité des acteurs de la sécurité se mesurera demain en fonction de leur capacité à répondre aux sollicitations des personnes physiques et morales. S'ils ne le font pas, ils sont appelés à disparaître. Gageons que les brigades de gendarmerie ont

1 La brigade numérique est une réussite qui ne remplace pas la nécessité d'une réponse locale.

2 Thème du 1^{er} FIC, en 2007.

encore trois siècles devant elles, dès lors que les mesures prises aujourd'hui par la DGGN sont poursuivies et

amplifiées. La gendarmerie, « Cyberforce humaine »³!

IN.CRT

Les fondateurs de cette association sont issus d'horizons différents (élus, universitaires, RSSI, militaires des armées et de la gendarmerie, experts des territoires ou de la cybersécurité). Sa démarche se veut pragmatique en partant des attentes encore non satisfaites pour apporter des réponses pérennes. Les bénéficiaires de son action sont plus particulièrement les collectivités territoriales (régions, départements, communes), leurs établissements publics de coopération (agglomérations, communautés de communes), les groupements publics qui en dépendent (syndicats mixtes, sociétés publiques locales). Les contrats de relance et de transition écologique (CRTE), dans leur composante numérique, offrent une opportunité pour établir un dialogue et un partenariat. Bien évidemment les entreprises privées sont aussi concernées,

car le socle économique est la condition de la prospérité des territoires. Les particuliers ne sont pas non plus oubliés, car leur acculturation est un préalable, toute politique l'ignorant étant vouée à l'échec, parce que l'humain est au cœur de la cybersécurité. Encourager la prise de conscience, développer les bonnes pratiques identifiées par un observatoire des expériences, favoriser la formation constituent quelques facettes du programme. Sans revendiquer un monopole, l'IN.CRT veut être un cristallisateur, un fédérateur au service des territoires.

Son président est le général d'armée (2S) Watin-Augouard, ancien inspecteur général des armées-gendarmerie. Le général d'armée (2S) Lizurey, ancien DGGN et élu local est membre du conseil d'administration.

3 Petit détournement que s'autorise l'auteur, sachant qu'il ne sera pas poursuivi par le créateur du slogan original...