Madame la Députée du Rhône,

Monsieur le Président du conseil départemental,

Madame la Vice-présidente de la Région, en charge du numérique,

Monsieur le gouverneur militaire de Lyon, cher Philippe,

Madame la Présidente du Cybercercle,

Mesdames et messieurs,

***

Tout d'abord, je tiens à remercier M.Christophe GUILLOTEAU de nous accueillir à l'occasion de cette 5ème étape du tour de France de la Cybersécurité 2019, qui s'inscrit pleinement dans l'esprit du mois européen de la cybersécurité.

J'adresse également mes vifs remerciements à Mme Bénédicte PILLIET pour son invitation et c'est avec plaisir que je prends la parole ce matin pour échanger avec vous sur la cybersécurité et ses enjeux sous le prisme de la gendarmerie et plus particulièrement de la région Auvergne – Rhône-Alpes.

***

Véritable rupture stratégique, 4ème révolution industrielle, les transformations induites par le digital ont profondément bouleversé notre société et gommé les frontières entre les sphères physique et numérique. Partant, les dépenses liées à la cybersécurité s'envolent dans le monde pour atteindre selon IDC 106 milliards de dollars en 2019, soit 10 % de plus qu'en 2018 et les experts tablent sur 150 milliards de dollars atteints en 2023.

***

Dans ce nouveau contexte, le **territoire numérique** devient pour la gendarmerie un territoire d'action à part entière, à l'instar du classique **territoire physique** et du **territoire des mobilités** également en pleine expansion.

A cet égard, en investissant le cyberespace, la gendarmerie a aussi intégré dans ses actions la dimension numérique des mobilités qui génèrent d'importants échanges de données, et ce, afin d'assurer **un continuum dans sa mission de sécurité.**

Dans ce cadre, notre action au profit d'un **numérique de confiance** est capitale, non seulement, pour assurer dans cet écosystème virtuel la sécurité des infrastructures reposant sur le numérique mais aussi, pour garantir la sûreté de l'utilisateur.

En effet, **le biotope criminel se métamorphose** au rythme des évolutions numériques et la cybercriminalité prend peu à peu le pas sur la délinquance de droit commun « classique ». Ainsi, le rapport « risque d'être interpellé / profits » est, dans la majeure partie des cas, favorable aux cybercriminels, et chaque avancée technologique leur offre de nouveaux outils et de nouvelles opportunités pour développer leurs entreprises criminelles.

La menace est plus que jamais d'actualité et elle vise indifféremment les entreprises, les collectivités ou les particuliers. Elle évolue, se perfectionne et je dirais même, se professionnalise. Ainsi, en 2019, plusieurs phénomènes ont poursuivi leur croissance, voire ont élargi leur spectre :

- les attaques par rançongiciels (ou ransomwares) sont toujours aussi nombreuses, mais elles ont évolué et **visent désormais directement** les **serveurs des entreprises**, paralysant totalement leur activité.

- le phénomène de « sextorsion », portant sur un chantage à la webcam prétendument piratée, s'est manifesté par une diffusion massive de mails visant à rançonner aussi bien les professionnels que les particuliers. Les cybercriminels jouent là sur le ressort psychologique le plus efficace, la peur.

Dans ce contexte, je souhaite souligner un récent succès obtenu par les enquêteurs Gendarmerie. Un serveur informatique pirate, basé en France, avait inoculé un virus à plus de 850 000 ordinateurs dans le monde. Les cybergendarmes du C3N, Centre de Lutte Contre les Criminalités Numériques, ont pu neutraliser le *botnet Retadup* et mettre en place une désinfection à distance des machines. Il s'agit d'un réel tour de force et en l'occurrence, d'une première mondiale.

***

Si le numérique est devenu un outil incontournable, mal maîtrisé, il peut devenir source de vulnérabilités face à des cybercriminels déterminés et très pro-actifs (vol de données, intrusion et / ou blocage des systèmes avec ou sans demande de rançon, espionnage, etc ,..).

Pour y faire face, la gendarmerie a, elle-aussi, conduit sa propre politique de **transformation numérique**.

S'appuyant sur les travaux du Conseil Scientifique de la Gendarmerie Nationale, notre communauté s'ouvre toujours davantage au monde universitaire. A cet égard, la convention récemment signée avec le CNRS est novatrice. L'idée est de travailler sur des thématiques à fort intérêt opérationnel :

des outils connectés pour être plus mobiles et efficaces (Néogend), le *Big Data* afin d'optimiser notre manœuvre opérationnelle (analyse prédictive), l'Intelligence Artificielle ou encore des outils de cyber-veille.

Le volet **formation** est aussi un impératif. Dés la formation initiale en école (ESOG et EOGN), des cours sont dispensés aux élèves pour les sensibiliser aux différentes formes de criminalité liées aux technologies numériques.

En matière de **prévention**, depuis bientôt une douzaine d'années, au travers de ses différentes actions, la gendarmerie nationale et plus particulièrement la région de gendarmerie Auvergne-Rhône-Alpes s'est pleinement engagée dans la politique de sécurité économique territoriale, dont la lutte contre la cybercriminalité est la composante essentielle.

Le nombre d'actions régionales conduites est à la hauteur des enjeux : ce sont plus de 3000 TPE-PME qui chaque année bénéficient du dispositif tranquillité-entreprises, plus de 2500 chefs d'entreprises, qui assistent aux conférences de sensibilisation aux risques cyber.

Pour ce qui concerne le volet **investigations**, c'est toute une chaîne criminalistique intégrée qui se met en place : en central, le C3N, Centre de Lutte Contre les Criminalités Numériques au niveau du Pôle Judiciaire de la Gendarmerie Nationale à Cergy-Pontoise, puis des enquêteurs spécialisés Nouvelles Technologies (N'TECH) dans les unités de recherches ; titulaires d'un DU ou d'un master II, ils s'appuient sur un réseau de proximité et des correspondants N'TECH. Pour la RGARA, ce sont pas moins de 27 experts N'TECH et 458 Correspondants N'TECH répartis dans 248 unités territoriales.

Les gendarmes arment également, avec nos collègues policiers, la plate-forme PHAROS, de signalement des contenus illicites, hébergée à la DCPJ.

La gendarmerie nationale a également développé la plate-forme PERCEVAL, qui vise à recueillir, analyser et lutter contre le contentieux massif des usages frauduleux de carte bancaire par internet et qui traite plus de 4000 signalements par semaine.

Dans un avenir proche (2020), THESEE, en cours de développement par la police, par le Service des Technologies et des Systèmes d'information de la Sécurité Intérieure aura pour but d'harmoniser le traitement des plaintes relatives aux escroqueries sur Internet.

***

7

Ce que vous devez retenir, c’est que tout utilisateur d'un smartphone, d'une tablette, d'un ordinateur fixe ou d'un portable est une victime potentielle. Il faut cesser de croire que ça n’arrive qu’aux autres ; les entreprises ne sont pas les seules concernées par ce phénomène : hôpitaux, mairies, universités, sont régulièrement les cibles de cyber-escrocs.

Le plus important n’est pas de savoir SI vous allez être victime mais surtout QUAND vous le serez.

Protéger vos avoirs immatériels et vos systèmes d’informations doit donc être VOTRE PRIORITÉ. Et pour y parvenir, vous pouvez utilement vous appuyer sur le pôle « sécurité économique » de la région de gendarmerie Auvergne - Rhône-Alpes. (Éric POZZI présent / B to B).

Cet engagement fort est partagé avec nos partenaires, au premier rang desquels la CPME, le MEDEF, les CCI régionales et locales, la CRMA[1] et le CESER, avec lesquels nous agissons en parfaite symbiose et synergie.

1 Chambre régionale de métiers et de l’artisanat

8

Nous allons poursuivre ces actions de sensibilisation et ces interventions communes à travers la Région, car **notre engagement premier est la sécurité de tous, au cœur même de nos territoires dont nous avons la responsabilité.**

Clairement, je ne souhaite pas que nos PME, que nos collectivités territoriales, souvent les plus vulnérables, soient en quelque sorte les « oubliées de la cybersécurité ».

Un tel engagement ne vaut que s’il s’inscrit dans une démarche de partenariat et d’échanges. Cette journée en est une parfaite illustration.

***

Merci de votre attention.