ASSEMBLÉE NATIONALE

# 15ème legislature

| | | |
|---|---|---|
| **Question N° : 41975** | De **Mme Maud Petit** ( Mouvement Démocrate (MoDem) et Démocrates apparentés - Val-de-Marne ) | **Question écrite** |
| **Ministère interrogé** > Transition numérique et communications électroniques | **Ministère attributaire** > Premier ministre | |
| **Rubrique** >numérique | **Tête d'analyse** >Stratégie française en matière de défense numérique et de prévention des risques | **Analyse** > Stratégie française en matière de défense numérique et de prévention des risques. |
| Question publiée au JO le : **19/10/2021**<br>Réponse publiée au JO le : **03/05/2022** page : **2945**<br>Date de changement d'attribution : **25/01/2022** | | |

## Texte de la question

Mme Maud Petit appelle l'attention de M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur la stratégie française en matière de défense numérique. En septembre 2021, des élus du territoire de Grand-Orly-Seine-Bièvre ont alerté M. le Président de la République sur les suites données à l'enquête concernant le logiciel espion Pegasus. Cette affaire n'est pas unique : de plus en plus régulièrement, des cyber-attaques de grande ampleur font les gros titres des journaux. Pourtant, ces affaires, au fort retentissement médiatique, ne sont que la face visible des dangers numériques. Le Comcyber (Commandement de la cyberdéfense), créé en 2018 en France, a recensé 831 évènements significatifs. Cela correspond à plus de 2 attaques par jour. La crise sanitaire a accéléré et, parfois même, transformé les usages numériques des particuliers, comme des professionnels : télétravail de masse, recours de plus en plus fréquent au stockage en ligne des données via le *cloud* en sont quelques exemples. Ces évolutions de pratique ont des répercussions en matière de cyber sécurité et les actes malveillants se multiplient allègrement dans le but de récupérer de la data. Elle l'interroge donc sur l'état des lieux de la stratégie de cyberdéfense française et sur les solutions apportées pour prévenir les risques auprès des particuliers et des entreprises.

## Texte de la réponse

Le 9 mars 2022, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié un Panorama de la menace informatique 2021 qui analyse les grandes tendances ayant marqué l'année 2021 et souligne les risques d'évolution à court terme. Dans un contexte de généralisation des usages numériques, le nombre de cyberattaques est en forte hausse. En effet, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37 % entre 2020 et 2021. La menace représentée par les rançongiciels semble s'être stabilisée, néanmoins à un niveau très élevé (203 attaques traitées en 2021 contre 192 en 2020). Les entités touchées en premier lieu par les rançongiciels sont les TPE, PME et ETI qui représentent 34 % des victimes en 2021 (+ 53% par rapport à 2020), suivies par les collectivités (19 %) et les entreprises stratégiques (10 %). Ces attaques aux fins de rançonnage, souvent très médiatisées, ne doivent pas occulter le caractère très préoccupant des campagnes d'espionnage et de sabotage. Les opérations d'espionnage informatique restent en effet la principale finalité des

attaques opérées par les services de renseignements étrangers et leurs sous-traitants. Elles visent tout autant les institutions que des acteurs privés. Cette hausse des cyberattaques s'explique de deux façons. D'une part, les vulnérabilités sont de plus en plus exploitées et les nouveaux usages numériques, moins maitrisés, comme le Cloud sont également exploités par les cyberattaquants ; d'autre part, les capacités d'action des acteurs malveillants, dont les principales intentions demeurent le gain financier, l'espionnage, la déstabilisation et le sabotage, ne cessent de se renforcer. Face à ce renforcement de la cybermenace, le Gouvernement a mis en place de nombreux dispositifs, notamment en déclinaison des mesures du plan France Relance et de la stratégie nationale d'accélération pour la cybersécurité. La plan France Relance poursuit trois grands axes d'effort dans le domaine de la cybersécurité. D'abord, grâce au dispositif des parcours de cybersécurité, 900 collectivités territoriales, établissements publics et établissements de santé seront accompagnés pendant deux ans dans une démarche de renforcement rapide et concrète de leur niveau de cybersécurité. Ensuite, des services automatisés de cybersécurité sont développés pour mieux détecter les cyberattaques, les filtrer au plus tôt et alerter les organisations de leurs vulnérabilités, susceptibles d'être exploitées par des cyberattaquants. Enfin, des centres de réponses à incidents sont créés, en coopération avec les conseils régionaux. Les premiers seront opérationnels dès l'automne 2022 dans toutes les régions volontaires. De même, des secteurs sensibles, comme celui de la santé, le secteur social ou encore ceux du transport aérien et du transport maritime, disposeront de telles structures. La stratégie nationale d'accélération pour la cybersécurité, désormais intégrée dans le plan France 2030, poursuit un double objectif d'accompagnement du développement d'un potentiel économique important et de maitrise des technologies visant à garantir la souveraineté nationale. Ce plan mobilise 1 milliard d'euros, dont 720 millions de financements publics. Son volet économique repose sur cinq axes : le développement de solutions souveraines de cybersécurité ; le renforcement des liens entre les acteurs de la filière ; la sensibilisation de l'ensemble des acteurs à la cybersécurité (individus, entreprises, collectivités, agents et organismes de l'État) ; la formation de la jeunesse et des professionnels à la cybersécurité afin de pallier la pénurie de personnel dans ce secteur ; un soutien en fonds propres. Elle s'articule avec des programmes structurants, notamment les actions du Comité stratégique de filière « Industries de sécurité » et appuie des initiatives comme le Campus cyber ou le Grand défi cyber.