ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

– Audition commune, à huis clos, de M. Stanislas Martin, directeur des risques d'EDF et de M. Patrick Guyonneau, directeur de la sécurité du groupe Orange, sur le rôle des opérateurs d'importance vitale (OIV) pour la défense globale.

Mercredi
10 avril 2024
Séance de 11 heures

Compte rendu n° 57

SESSION ORDINAIRE DE **2023-2024**

Présidence de M. Thomas Gassilloud, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures sept.

M. le président Thomas Gassilloud. La présente audition, à huis clos, vise à poursuivre l'étude du rôle stratégique de certains acteurs économiques en matière de défense globale, en l'espèce ceux des réseaux de télécommunication et de l'énergie. Nous auditionnons M. Stanislas Martin, directeur des risques d'EDF, et M. Patrick Guyonneau, directeur de la sécurité du groupe Orange, qui auront l'occasion de préciser le périmètre de leurs responsabilités respectives, s'agissant notamment d'EDF, qui distingue sécurité nucléaire et sûreté nucléaire.

Le retour d'expérience (Retex) de la guerre en Ukraine démontre chaque jour que les infrastructures civiles indispensables à la vie d'une nation constituent des cibles stratégiques en cas de guerre. La veille de notre arrivée en Ukraine, où j'accompagnais la présidente de l'Assemblée nationale, six gigawatts de capacités avaient été ciblés par les Russes. Lorsque nous étions à Odessa, nous avons observé la présence de nombreux groupes électrogènes.

Cela en dit long sur le rôle de l'énergie en cas de crise majeure ou de guerre. La résilience de la nation est conditionnée à la robustesse des activités d'importance vitale, qu'il s'agisse d'usines, de centres de données ou de réseaux divers et variés.

Messieurs, votre audition doit nous aider à comprendre comment des entreprises d'importance telles que les vôtres s'organisent pour anticiper les risques d'ampleur et protéger leurs activités si le pire arrivait. Nous souhaitons savoir de quelle façon vous identifiez les risques, comment vous formez et sensibilisez vos agents, notamment à la cybersécurité – on dit souvent que le risque, en matière de cyber, est entre le clavier et la chaise.

Vous pourrez également nous éclairer sur ce que la crise covid et surtout la guerre en Ukraine vous ont fait redécouvrir ou réapprendre. Quel Retex en tirez-vous pour l'avenir ? Quelles sont les forces à mettre en exergue et les faiblesses à combler ?

Le statut des opérateurs d'importance vitale (OIV) est fixé par le code de la défense, qui les définit comme suit : « Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ». La liste des OIV étant classifiée, nous ignorons si Orange et EDF en font partie. Nous pouvons toutefois supposer que, compte tenu du caractère sensible de leurs activités, il est probable que ces entreprises fassent partie des quelque 300 OIV, qui gèrent 1 500 points d'importance vitale (PIV) et sont soumis à certaines obligations.

M. Stanislas Martin, directeur des risques d'EDF. Je suis heureux de m'adresser à votre commission sur le sujet ô combien important de la robustesse du système électrique en France.

Le groupe EDF tient compte des risques pesant sur la nation dans ses activités opérationnelles selon trois axes. Le premier est relatif au nombre de crises réelles que le groupe a dû gérer récemment, en conformité avec ses obligations réglementaires et en coopération avec les services de l'État, et au Retex qu'il en a retiré. Le second est relatif au dispositif d'analyse des risques et d'élaboration des plans d'action associés. Le troisième est dédié à son organisation de crise et de continuité d'activité.

Si EDF a historiquement mis en œuvre des organisations pour gérer les crises et accroître la résilience du système électrique, le groupe n'a cessé de s'adapter dans sa structure

et de tirer les enseignements des crises. À titre d'exemple, les événements météorologiques extrêmes tels que les tempêtes de 1999, la canicule de 2003 et, plus récemment, les tempêtes Ciaran et Domingos ont suscité et suscitent toujours des analyses d'adaptation au changement climatique.

L'accident de Fukushima survenu en 2011 a donné naissance, au sein d'EDF, à la force d'action rapide du nucléaire (Farn) en 2014. La crise de la corrosion sous contrainte et des marchés de l'énergie de l'hiver 2022-2023, qui a induit des risques de délestage, a provoqué une sensibilisation inédite de nos compatriotes à la sobriété, une réforme des marchés de l'électricité à l'échelon européen et une prise de conscience de l'impératif de souveraineté énergétique. Ces divers événements démontrent qu'il est nécessaire de créer des organisations résilientes à tout type de crise, pour les rendre efficaces, coordonnées et agiles, afin d'élaborer des solutions proportionnées et adaptées au besoin de continuité de nos activités stratégiques.

Si le caractère et la nature des crises ont sensiblement évolué, au cours des dernières années, en fréquence, en complexité et en coût, leur caractère systémique accentue l'imbrication de la gestion des risques et de la gestion de crise. Ce caractère systémique exige une bonne cohérence des actions entre les opérateurs et les pouvoirs publics, comme nous le constatons dans le cadre de la préparation des Jeux olympiques et paralympiques (JOP) de 2024.

EDF est soumis à des obligations réglementaires, en tant que premier producteur électrique du pays et en tant qu'entreprise stratégique. Ses activités sont indispensables au fonctionnement de l'économie et de la société, ainsi qu'à la défense, à la sécurité et à la survie de la nation. Comme telle, elle relève de l'article R. 1332-10 du code de la défense. EDF interagit fortement avec les pouvoirs publics dans les phases d'anticipation, de préparation, d'alerte, de gestion de crise et de Retex, à trois niveaux.

Le premier est celui des services du Premier ministre, dont le Secrétariat de la défense et de la sécurité nationale (SGDSN). Nous collaborons avec eux sur plusieurs plans : l'analyse des risques face à la menace ; la préparation des plans nationaux tels que le plan national de réponse à un accident nucléaire ou radiologique majeur (PNR-ANRM) ; la conduite d'exercices de crise conjoints ; la gestion effective des crises. Nous nous conformons aux exigences formulées par l'Agence nationale de la sécurité des systèmes d'information (Anssi) dans le cadre de la stratégie de la France en matière de défense et de sécurité des systèmes d'information.

Le deuxième niveau est celui de nos ministères de tutelle : le ministère de la transition écologique, par le biais de la direction générale et de l'énergie et du climat (DGEC), et le ministère de l'économie et des finances. Dans ce cadre, nous travaillons notamment à la transposition des directives européennes, que j'évoquerai lorsque je détaillerai les risques analysés dans le plan de préparation aux risques dans le secteur électrique.

Le troisième niveau est le ministère de l'intérieur, avec lequel nous collaborons dans le cadre de la direction générale de la sécurité civile et de la gestion de crise (DGSCGC), des zones de défense et des préfectures de départements.

Le groupe se met continuellement en conformité avec les évolutions réglementaires du code de la défense, en intégrant notamment les modifications induites par les lois de programmation militaire (LPM) et par les projets de loi de transposition en droit français de la directive sur la résilience des entités critiques, dite directive REC, de la

directive sur la sécurité des réseaux et de l'information, dite directive NIS, et du règlement sur la résilience opérationnelle, dit règlement DORA, s'agissant des dispositions financières.

J'en viens à l'organisation visant à renforcer la résilience du groupe aux risques majeurs, en regroupant les fonctions de gestion de risques, de contrôle interne et de gestion de crise au sein d'une même direction – la direction des risques – et d'une même filière – la filière « Risques, contrôle interne et crises » –, où travaillent environ 400 personnes.

Outre les aspects réglementaires de sa mission, la direction des risques réalise une actualisation annuelle de la cartographie des risques du groupe, validée en comité exécutif (Comex) et présentée aux organes de gouvernance. Chaque risque majeur est affecté à un membre du Comex, qui porte la responsabilité de son instruction et du déploiement du plan d'action associé.

Cette analyse traite des grands risques pesant sur la continuité d'activité du groupe et correspondant, pour certains, à ceux décrits dans le plan de préparation aux risques dans le secteur électrique. Les risques majeurs affectant le groupe EDF et pesant sur la nation sont les risques climatiques, les dépendances aux matières critiques, le risque de *black-out*, les attaques cyber et sécuritaires, les risques d'accident nucléaire et hydraulique, l'accès aux compétences et la continuité d'activité lors de grands événements tels que les JOP.

S'agissant des risques liés aux événements climatiques extrêmes, dont la fréquence et l'intensité augmentent, et de la nécessaire adaptation de notre parc, de nos ressources et de nos processus, nous évaluons l'impact du changement climatique sur nos installations et déployons depuis plusieurs années un plan d'action global sur nos actifs de production. Cette action est renforcée par une approche plus systémique à l'échelle territoriale.

La continuité d'activité nous amène à prendre en considération les risques de dépendance géopolitique et industrielle pour nos approvisionnements et accès aux matières critiques. En la matière, EDF a instauré des plans de diversification des approvisionnements et des stockages stratégiques. Ces plans sont régulièrement actualisés, notamment en fonction des sanctions internationales.

S'agissant du risque d'équilibre entre l'offre et la demande sur les réseaux, la contribution d'EDF à la maîtrise du risque de *black-out* figure dans ses obligations réglementaires, conformément à son contrat de service public et à sa responsabilité de gestionnaire d'équilibre. S'agissant du délestage, le travail effectué avec les pouvoirs publics en préparation de l'hiver 2022-2023 a permis d'améliorer les processus de gestion de telles crises.

S'agissant du risque d'attaque cyber, le groupe applique la stratégie de la France en matière de défense et de sécurité des systèmes d'information, édictée par l'Anssi. Il organise des exercices de crise cyber et améliore en continu la résilience des systèmes de surveillance et d'information. Il a notamment créé un centre opérationnel de sécurité cyber et une équipe experte dédiée, dans une approche transversale.

En ce qui concerne le risque d'accident industriel, la maîtrise de la sûreté est une priorité absolue pour tout exploitant. La direction des risques est garante de la coordination des politiques du groupe et joue un rôle prescriptif auprès des métiers, qui ont eux-mêmes développé leur propre référentiel de sûreté et de sécurité. Les équipes d'EDF exercent cette responsabilité dans une logique d'amélioration continue.

La prévention du risque d'accident industriel grave repose principalement sur trois axes : la conformité des installations au référentiel de conception et à ses évolutions dans le temps ; la conformité de l'exploitation aux textes réglementaires ; la maîtrise des situations à risque en exploitation normale ou dégradée. Ce risque est stable et fait l'objet d'un bon niveau de contrôle grâce aux dispositifs de maîtrise et de sécurisation mis en œuvre.

S'agissant de l'activité nucléaire, ses résultats sont corroborés par les contrôles effectués par l'Inspection nucléaire, qui est une entité interne au groupe EDF, et par les entités externes qu'est l'Autorité de sûreté nucléaire (ASN), l'Agence internationale de l'énergie atomique (AIEA) et l'Association mondiale des exploitants nucléaires (WANO). L'existence d'une organisation de crise nucléaire solide au sein du groupe, la Farn, le GIE d'intervention robotique sur accidents (GIE Intra) et l'application des modifications de sûreté conduites dans le cadre des visites décennales post-Fukushima favorisent une limitation de l'impact du risque.

S'agissant du risque sécuritaire, la protection des installations nucléaires et hydrauliques contre la malveillance relève de l'exigence interne de protection du patrimoine d'EDF d'une part et, d'autre part, des exigences réglementaires liées à la responsabilité de l'exploitant fixées par les arrêtés relatifs à la protection et au contrôle des matières nucléaires, de leurs installations et de leur transport, dits arrêtés PCMNIT, et aux secteurs d'activité d'importance vitale (SAIV), ainsi que des dispositions introduites par la loi du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, dite LPM 2014 – 2019. Tous les sites sont conformes aux obligations émises par le Service du haut fonctionnaire de défense et de sécurité (SHFDS).

Face au risque de tensions sur les compétences des filières de la transition énergétique correspondant à la mise en œuvre des orientations présentées par le Président de la République à Belfort le 10 février 2022, telles que la prolongation du parc existant, le programme EPR 2, le développement des énergies renouvelables (EnR), notamment en mer, et l'adaptation des systèmes énergétiques à l'augmentation du volume de raccordement, le projet Compétences porté aux niveaux Comex et stratégique vise à sécuriser les compétences du groupe.

De façon plus immédiate, l'entreprise est exposée, en tant que sponsor et fournisseur des JOP, à un risque de rupture de continuité d'activité. Un projet interne piloté par la direction des risques s'assure de la prise en compte des contraintes liées à la proximité de nos sites avec certains sites olympiques. Ce travail est mené en étroite collaboration avec la Préfecture de police de Paris, le Comité d'organisation des Jeux olympiques et paralympiques (Cojop), la préfecture de Paris et d'Île-de-France, la préfecture de Seine-Saint-Denis et le ministère de la transition écologique.

S'agissant de la robustesse de notre dispositif de gestion de crise et des plans d'action destinés à garantir la résilience de nos organisations, elle est un devoir à l'égard de nos partenaires. Depuis 2005, l'entreprise s'est dotée d'une politique de gestion de crise, mise à jour en 2017, pour intégrer les exigences de continuité d'activité et de Retex applicables à tout type de crise pouvant survenir au sein d'EDF, à la suite d'événements d'origine interne ou externe susceptibles de menacer nos intérêts. L'efficacité de sa mise en œuvre au niveau du siège est conditionnée par une organisation de crise préparée, réactive, adaptable et entraînée, ce qui suppose l'élaboration de doctrines de crise, des actions de formation et d'entraînement ainsi que le maintien opérationnel des dispositifs d'alerte et de mobilisation.

Les exercices de préparation, réglementaires ou en réponse à un risque avéré de la cartographie des risques du groupe, mobilisent les permanents à tous ses niveaux, des opérationnels au Comex, sur des scénarios travaillés avec chaque métier, afin d'identifier les points d'amélioration à tester. Les exercices SECNUC, Blackout, Golfech et Bugey, ont été respectivement réalisés en 2021, 2022, 2023 et 2024, en coopération avec les services de l'État et en impliquant le plus haut niveau de l'entreprise qu'est le Comex.

Au titre de l'alerte, un dispositif de permanence 24/7 mobilisant environ soixante-dix permanents représentant tous les métiers du groupe garantit une remontée d'information immédiate à un correspondant unique, en lien avec la présidence et la cellule ministérielle de veille opérationnelle et d'alerte (CMVOA) du ministère de la transition écologique. Sur décision du directeur de permanence et après analyse de la situation, comme ce fut le cas lors du démarrage de la crise en Ukraine, ou selon les critères prédéfinis en cas d'incident nucléaire, une équipe de crise est mobilisée immédiatement dans le centre de crise du groupe. Le directeur de crise engage alors les actions immédiates et peut décider d'activer les plans de continuité d'activité à tout moment. Il veille à appliquer les procédures et à les ajuster si les circonstances l'exigent.

Pendant la phase de gestion de crise, le directeur de crise intègre, depuis 2005, une cellule d'aide à la réflexion stratégique et à l'anticipation, appelée force de réflexion rapide, dont la capacité de questionnement, d'analyse critique et d'inventivité, en appui au directeur de crise, a fait ses preuves lors des dernières grandes crises qu'a connues le groupe. Dès la première réunion de l'équipe d'examen de la sûreté d'exploitation (OSART) d'EDF, l'AIEA a mis en avant, au titre des meilleures pratiques, l'organisation de crise du groupe, complétant et confortant ainsi l'organisation de la direction du parc nucléaire.

Outre les moyens mobilisés en sortie de crise, un Retex est systématiquement réalisé à chaud et à froid. Il est intégré au guide méthodologique d'élaboration des plans de continuité d'activité et au plan de mitigation de la cartographie des risques du groupe.

M. le président Thomas Gassilloud. Par anticipation sur les questions à venir, j'appelle l'attention sur le caractère vital de l'électricité. Sans électricité, tout est coupé – pour le pétrole, il reste un peu d'essence dans les réservoirs et nous avons trois mois d'autonomie stratégique –, notamment la circulation, les réseaux bancaires, les approvisionnements en énergie et la capacité de fonctionnement des institutions.

Par ailleurs, il existe des risques industriels liés à l'activité d'EDF, illustrés par la guerre en Ukraine, qui a touché la retenue d'eau du barrage de Kakhovka et de la centrale nucléaire de Zaporijia. J'ai eu l'occasion de rencontrer les personnels de la Force d'action rapide nucléaire (Farn), qui est très bien dotée, notamment en comparaison des unités du génie de l'armée de terre, dont certains matériels sont vieillissants. Elle dispose de bûcherons, de bateaux, de capacités de pompage et de capacités nucléaires. Beaucoup de ses 400 personnels sont des réservistes d'EDF, occupant une autre fonction dans le groupe.

Monsieur Guyonneau, votre parcours illustre la défense globale. Vous avez commencé votre carrière en commandant une section d'infanterie chez les marsouins. Vous l'avez poursuivie à la Direction générale de l'armement (DGA), au sein des programmes aéroterrestres. Vous avez ensuite rejoint le ministère de l'intérieur, notamment à la Direction générale de la police nationale (DGPN) et au Service des technologies et des systèmes d'information de la sécurité intérieure (STSISI). À présent, vous servez au sein d'une entreprise qui est sans doute un OIV. Vous êtes l'incarnation d'un parcours au service de la défense globale.

M. Patrick Guyonneau, directeur de la sécurité du groupe Orange. Le rôle des opérateurs critiques que sont les OIV et les opérateurs de services essentiels (OSE) connaît de nos jours un infléchissement.

Ils sont le fruit d'une vision gaullienne, inspirée par Michel Debré, tirant les leçons de la drôle de guerre, de l'étrange défaite et de l'effondrement de 1940. En 1958, la vision globale de la défense allie défense militaire, défense civile – qui ne se réduit pas à la sécurité civile – et défense économique. Il s'agissait de disposer de toutes les ressources possibles pour pouvoir les mobiliser – je n'y inclus pas les ressources morales, l'existence d'un ennemi désigné suffisant alors à maintenir le moral de la nation.

Si les forces de la nation demeurent mobilisées, les secteurs d'activité d'importance vitale (SAIV), tels qu'ils sont définis par le décret du 23 février 2006 relatif à la sécurité des activités d'importance vitale, relèvent d'une vision et d'une organisation au sein desquelles ils sont juxtaposés. Chacun a un ministère responsable et une vision propre, en partant du principe selon lequel chacun sait délivrer sa production dans la durée. Sur la base de cet invariant, les missions de protection ont concentré l'attention, d'abord contre les actes malveillants, notamment le sabotage et le terrorisme, qui sont essentiellement des menaces internes, puis contre les risques naturels et technologiques et, depuis 2013, contre les menaces cyber, conformément à l'article 22 de la LPM 2014 – 2019.

Ce modèle a plusieurs limites : l'émergence de menaces sécuritaires de basse intensité, le terrorisme ayant pris une ampleur inattendue ; la dissociation assez forte, dans les textes et dans les mesures, entre le cyber et le physique, qui sont parfois difficiles à concilier ; l'évolution de l'économie d'une logique de production et de stocks à une logique de services et de flux ; la fin des monopoles d'État, qui induit la multiplicité des interlocuteurs, même si chaque secteur a souvent un opérateur prépondérant ; l'intrication des services entre opérateurs, qui induit leur interdépendance.

À cet égard, la vision du Livre blanc sur la défense et la sécurité nationale 2008 est intéressante, à trois titres. D'abord, elle inclut les notions de volonté et de capacité, rappelant que l'intention précède les moyens. Ensuite, elle rappelle la nécessité de résister à des agressions et à des catastrophes majeures, rehaussant la vision de la sécurité à la défense. Enfin, elle mentionne le besoin de rétablir une capacité à fonctionner normalement ou en mode dégradé socialement acceptable.

La résilience est une question de priorisation, qui doit associer la société par le biais des notions de juste nécessité et d'acceptabilité sociale. Il s'agit de définir ce qui est socialement acceptable en temps de paix, de crise et de guerre, s'agissant par exemple de l'usage d'internet.

La vision globale de la défense ne peut qu'être saluée. La perspective de disposer, dans un avenir proche, d'une loi relative à la résilience couvrant toutes les obligations afférentes, nous semble intéressante pour assurer le continuum public-privé et garantir une cohérence d'ensemble entre les sujets physiques et cyber. Au sein d'Orange, la sécurité s'inscrit dans le cadre d'une vision globale. Je suis chargé de l'anticipation des risques, de la sûreté, qui est pour l'essentiel la sécurité physique des installations, de la cybersécurité et de la gestion de crise. Si j'échoue sur les deux premiers aspects, il m'incombe d'assurer la suite et la remise en état des installations avec mon équipe.

Pour faire vivre cette cohérence d'ensemble et le continuum public-privé, nous devons créer des conditions de confiance : celle des citoyens ; celle des acteurs publics et privés, car nous devons inclure la coopération dans la régulation ; celle des autres opérateurs.

Dans ce dispositif global, l'État établit les priorités tout en assurant l'égalité de traitement en matière d'exigences et la transparence assurant le partage des informations relatives au niveau de menace.

Il s'agit de faire en sorte que tous les opérateurs soient à armes égales. Dans le monde ouvert qui est le nôtre, dans l'Union européenne et au-delà, il ne faut pas que les principaux OIV soient soumis à des exigences plus fortes que celles imposées aux petits opérateurs et aux autres opérateurs européens.

Les conditions à réunir pour bâtir cette confiance peuvent sembler difficiles à faire vivre : il faut notamment associer la transparence et le niveau de secret nécessaire pour préserver nos priorités, qui sont stratégiques et régaliennes, et masquer nos faiblesses. À cet égard, nous plaçons beaucoup d'espoir dans la future loi relative à la résilience, qui concernera Orange à trois titres : la transposition du règlement DORA, car nous assurons un service financier à l'échelle mondiale grâce à l'application Orange Money ; la transposition de la directive NIS ; la transposition de la directive REC. Une loi unique offrira une forte visibilité et permettra d'éviter l'empilement des dispositifs, lequel oblige parfois à cheminer parmi les doubles négations pour comprendre exactement l'exigence qui s'applique.

Orange est présent dans 200 territoires, aux régimes juridiques distincts – tel est le cas des outre-mer en France –, essentiellement pour des activités de services aux entreprises (B2B), dont certaines sont des multinationales et des OIV. Nous avons environ 140 000 salariés, dont la plupart travaillent dans vingt-six pays d'Europe, Russie comprise, du Moyen-Orient, d'Afrique du nord, centrale et de l'ouest, jusqu'à Madagascar. Tout cela forme une énorme palette de risques quotidiens. Nous avons conservé la propriété de nos grandes infrastructures de communication, que nous gérons ou cogérons dans le cadre de syndics, soit environ 450 000 kilomètres de câbles sous-marins.

Les risques que nous traitons sont de quatre ordres : l'intégrité de nos salariés ; la protection des données de nos clients, dont plusieurs sont des États et des ministères des affaires étrangères ; la continuité de nos réseaux face au risque cyber et au risque de sabotage ; le risque d'espionnage pesant sur le patrimoine, d'entreprise ou d'État, de nos clients. Le rapport de l'Anssi intitulé *Panorama de la cybermenace 2023* indique que les opérateurs de télécommunication sont ceux qui font le plus souvent appel à elle.

En matière de résilience, nous agissons selon quatre axes. L'anticipation est assurée par une équipe de prospective et de veille à court terme, et par la mise à jour régulière de notre analyse des risques et des menaces. La prévention est assurée par la mise en œuvre d'une politique de prévention incluant des contrôles, des exercices, des mesures techniques telles que la redondance et la supersécurisation de certains systèmes, des mesures humaines, notamment la formation des salariés, et des mesures d'organisation et de planification.

La gestion de crise repose sur des plans de continuité d'activité (PCA) et sur des plans de reprise d'activité (PRA). Toutefois, chaque crise nous fait aller de surprise stratégique en surprise stratégique. Les plans sont utiles et nécessaires, mais malheureusement pas suffisants. Le Retex permet de boucler la boucle, en exploitant les exercices et les crises pour faire évoluer notre système de veille, notre système d'analyse et nos politiques de prévention et de sécurisation.

J'en viens aux difficultés majeures que nous rencontrons, qu'il importe de signaler dans le cadre d'une audition consacrée à la défense globale et dans la perspective de la future loi relative à la résilience.

La première est de définir ce qui est socialement acceptable. Internet est indispensable au télétravail, qui s'est développé depuis la crise du covid, mais est-il indispensable d'avoir accès à des plateformes de vidéos telles que YouTube ? A-t-on le droit de supprimer ce service si l'énergie vient à manquer ?

Les opérateurs ne peuvent en décider seuls. Une fois un réseau déployé, il fonde une architecture pour une soixantaine d'années, voire pour quatre-vingts ans. Le réseau cuivre, qui est ancien, sera fermé au grand public d'ici 2030. Nous n'avons pas l'agilité pour faire évoluer rapidement nos architectures. Nous modifions les réseaux mobiles tous les dix ans, pas les grandes infrastructures dont le déploiement coûte plusieurs milliards à l'échelle de la France.

La deuxième difficulté est l'interdépendance entre secteurs et entre opérateurs, qui doivent se connaître. En cas de délestage, Réseau de transport d'électricité (RTE) a besoin des opérateurs de télécommunication pour actionner les postes à haute tension (HTA). La fin du monopole oblige à développer le travail entre secteurs et entre opérateurs. Il faut se connaître, tenir compte du besoin d'en connaître – je ne peux pas partager les documents classifiés transmis par l'État, d'autant que je ne sais pas quels opérateurs sont des OIV – et s'exercer ensemble.

La troisième difficulté réside dans les enquêtes administratives préalables à la délivrance d'une habilitation de sécurité, qui soulèvent de nombreux problèmes en matière de ressources humaines, dans la mesure où tous nos salariés ne sont pas français, qu'ils travaillent ou non en France. Que faire si l'enquête n'autorise pas la délivrance d'une habilitation ? Un salarié intervenant le matin sur un site du ministère des armées et l'après-midi sur un site de TotalEnergies fait l'objet de deux enquêtes distinctes, dont la conclusion n'est pas nécessairement identique.

La quatrième difficulté réside dans la chaîne d'approvisionnement. Nos sous-traitants et nos fournisseurs, notamment les équipementiers en matériels et en logiciels, ne sont pas tous soumis aux directives qui nous sont applicables. Beaucoup sont asiatiques ou américains ; les textes français et européens, tels que la législation européenne sur la cyberrésilience (CRA), ne font pas partie de leurs préoccupations.

La cinquième difficulté découle du fait que nous sommes dans un monde en crise multiforme et permanente. Depuis deux semaines, j'ai traité cinq crises : la rupture de câbles sous-marins au large de l'Afrique ; une crise au Sahel ; une faille de sécurité dans le réseau privé virtuel (VPN) de l'éditeur américain Ivanti ; les conséquences des événements du Moyen-Orient en Égypte et en Jordanie ; les conséquences de la guerre sur l'Ukraine et la Russie. Si l'on ajoute à tout cela la préparation des JOP, on prend la mesure de la tension à laquelle sont soumises nos organisations et de la fatigue qui en résulte pour nos salariés, ce qui les expose au risque de ne pas avoir le bon réflexe, de ne pas se conformer aux plans, de ne pas prendre la bonne décision et de commettre des erreurs.

M. le président Thomas Gassilloud. Les services critiques de l'État eux-mêmes utilisent de plus en plus les réseaux civils de télécommunications en lieu et place des réseaux étatiques historiques.

Au sein de la gendarmerie, le réseau Rubis, soumis aux astreintes inhérentes au statut militaire, intègre progressivement le réseau radio du futur (RRF), dont un lot important a été attribué à Orange. Cela signifie que, demain, nos gendarmes utiliseront des radios mobiles civiles dans leur activité quotidienne. De même, le système FR-Alert, qui permet d'informer la population d'une zone donnée par l'envoi massif d'un SMS, est un dispositif

important en matière de défense globale et de résilience reposant sur les relais de télécommunication civils.

Nous en venons aux interventions des orateurs des groupes.

M. Mounir Belhamiti (RE). Les JOP sont une cible importante pour les cyberattaques. Nous devons nous assurer que nous sommes prêts à faire face aux menaces. Les OIV jouent un rôle crucial dans la sécurité de ces événements. Leur vigilance et leur expertise sont essentielles pour anticiper, détecter et neutraliser les cybermenaces.

Leur mission est d'autant plus importante lors d'événements d'envergure internationale, qui portent les enjeux de sécurité à leur paroxysme. Le Cojop ne s'y est pas trompé : il a positionné Orange et EDF au rang d'opérateurs P1 dans le classement des cercles d'importance. Du point de vue factuel, la chaîne énergétique dans son ensemble, incluant RTE et Enedis, doit être considérée comme stratégique.

Comment préparez-vous les JOP en matière de cybersécurité, s'agissant notamment de la prévention des actes de sabotage ? Quelle est votre logique de préparation et de réponse aux menaces potentielles ?

La directive NIS 2, qui vise à atteindre un haut niveau commun de cybersécurité au sein de l'Union européenne, offre une opportunité unique pour améliorer notre cybersécurité. Son périmètre d'application, plus large que celui de la directive NIS, offrira davantage de protection en imposant des obligations plus strictes en matière de gestion des risques et de signalement des incidents. Êtes-vous prêts à l'appliquer ? La considérez-vous comme un atout pour renforcer notre sécurité ? Certains aspects devraient-ils bénéficier d'ajustements ou d'améliorations ?

Par ailleurs, je m'interroge sur la pertinence, au sein de la logique de défense globale et de résilience de la nation, de la fermeture du réseau cuivre. Son intérêt économique et opérationnel est évident mais, dans une logique de gestion des risques, notamment cyber, une attaque massive et coordonnée sur les nœuds de raccordement optique endommagerait la fibre optique physique et les antennes-relais, ce qui entraverait le fonctionnement du dispositif FR-Alert. Comment tenez-vous compte d'un tel scénario ?

M. Stanislas Martin. Le projet JO, continuité d'activité, risques et interfaces (Jocari) est piloté par la direction des risques d'EDF. Il vise à s'assurer que les organisations permettant de garantir la continuité d'activité pendant les JOP sont prêtes et que nous serons en capacité de traiter des événements exceptionnels tels que des intrusions et des actes de malveillance. Par ailleurs, EDF, comme RTE et Enedis, est sponsor et fournisseur officiel des JOP.

Notre première préoccupation est la proximité de certains de nos sites stratégiques et du village olympique. Les plans de sécurisation des sites olympiques sont organisés en trois cercles concentriques. Le premier est sous la responsabilité directe du Cojop, les deux autres sont sous la responsabilité des préfectures ; tous incluent des contraintes d'accès.

Certaines de nos activités vitales se trouvent à la limite du premier cercle et du deuxième. Nous avons prévu de les déplacer à l'extérieur des trois cercles. Il s'agit notamment de la gestion de l'équilibre entre l'offre et la demande, d'EDF Trading et de certaines activités d'astreinte pour les crises nucléaires.

S'agissant de la cybersécurité, les systèmes industriels de nos sites sont déconnectés et indépendants des systèmes de gestion. Ils ne sont pas connectés à des systèmes

externes. Leur mise à jour exige une intervention sur place et fait l'objet de procédures très strictes. Nos moyens de production sont à l'abri des menaces cyber.

Nous prévoyons de subir des attaques sérieuses sur nos systèmes d'information en tant qu'opérateur sans doute d'importance vitale. Leur nombre a d'ores et déjà augmenté à l'approche des JOP. Nous en subissons plusieurs milliers chaque année. Nous les avons toujours repoussées, ce qui n'entame en rien notre humilité. La gouvernance du dispositif cyber à partir d'un centre de sécurisation opérationnelle unique en assure la sécurité.

M. Patrick Guyonneau. D'abord, une petite remarque sémantique, nous ne neutralisons pas les attaques, mais leurs effets.

Orange est partenaire premium du Cojop. Nous sommes l'opérateur chargé d'assurer la connectivité et la transmission du signal vidéo. Jamais un opérateur, dans l'histoire des Jeux, n'avait été chargé d'un tel périmètre – lors de la précédente édition, ils étaient quatre.

Nous avons prévu des mesures de sécurité et de résilience des réseaux pour faire face aux menaces cyber et aux actes de sabotage. Les réseaux des opérateurs rassemblés au sein de la Fédération française des télécoms (FFTélécoms) subissent chaque année plusieurs milliers d'actes de malveillance.

Les 120 sites olympiques, du quartier général du Cojop au Village des Médias en passant par les sites des épreuves et ceux des délégations, bénéficient tous d'adductions au réseau de télécommunication, dont au moins une est sécurisée par de nouvelles serrures et, dans quelques semaines, par des patrouilles d'équipes de sécurité privée et d'agents de la Préfecture de police de Paris, ainsi que par des vidéopatrouilles.

S'agissant des menaces cyber, l'Anssi, qui fait confiance à nos audits, a émis des préconisations sur les systèmes d'information spécifiques aux JOP, que nous appliquons. La coopération avec le Cojop et avec Atos, qui est le prestataire de sécurité du Comité international olympique (CIO), est constructive. Nous avons organisé des exercices de crise. Jusqu'à présent, tous ont été réussis. En outre, le CIO réalise des tests de chaque structure.

Par ailleurs, nous sommes fournisseur de l'État pour la téléphonie mobile, le réseau interministériel de l'État (RIE), la téléphonie fixe et l'intranet de gestion de crise. Nous fournissons certains systèmes sensibles ou critiques de l'État et des ministères, qui demanderont sans doute des prestations supplémentaires – plus tôt ils en demanderont, mieux nous pourrons en assurer la sécurité et la supervision. Je ne dis pas que tout ira bien ni que nous sommes pleinement confiants et sereins, mais nous tenons compte des pires scénarios et nous y travaillons.

La directive NIS 2 a été publiée à la fin de l'année 2022. Nous en avions anticipé plusieurs dispositions, notamment celles relatives à l'authentification multifacteurs, d'ores et déjà incluse dans les procédures de la plupart des opérateurs. La question est de savoir de combien de temps nous disposerons pour adapter nos systèmes, dont les technologies varient selon qu'il s'agit de réseau cuivre ou du réseau mobile 5G.

Nous serons très attentifs au délai de conformité. La directive sera transposée d'ici le mois d'octobre. Nous avons mené des consultations avec l'Anssi, sur la directive NIS, et avec le SGDSN, sur la directive REC. Nous élaborons actuellement des observations sur l'avant-projet de loi.

Le premier risque est la surtransposition, non seulement pour d'évidentes raisons de concurrence, mais aussi parce que la directive NIS prévoit deux catégories d'entités, importantes et essentielles. S'agissant des premières, le droit applicable sera celui du pays où se trouve le siège. Ainsi, certaines activités d'Orange en Pologne ou en Roumanie relèveront du droit français. L'Anssi étant l'une des agences les plus exigeantes en Europe, nous risquons d'y perdre nos marchés B2B. La cohérence à l'échelle européenne s'impose. S'il importe de fixer des exigences élevées, il faut aussi être attentif à ne pas s'aligner sur le moins-disant sécuritaire.

Le deuxième risque est la coexistence de multiples catégories – OIV et OSE à l'échelle française, entités essentielles (EE), entités importantes (EI) et entités critiques (EC) à l'échelle européenne. Nous saluons l'effort consenti par la France pour rassembler les dispositions dans une loi unique. Nous espérons qu'elle sera lisible, indiquant clairement les mesures applicables à telle et telle catégorie sans multiplier les renvois, faute de quoi nous seront perdus et le régulateur aussi.

Nous espérons aussi que le principe *non bis in idem* s'appliquera et que nous ne serons pas punis trois fois pour une même faute, au titre des directives NIS et REC puis au titre du règlement général sur la protection des données (RGPD), d'autant que les amendes peuvent atteindre des montants élevés. Je comprends que l'État se préoccupe d'éviter toute lacune en matière de sanctions, mais nous préférons travailler sur le mode de la coopération. L'avant-projet de loi comporte de nombreuses dispositions relatives à la commission des sanctions, et aucune, curieusement, relative aux sanctions applicables à l'État.

Concernant la fermeture du réseau cuivre, les réseaux point à point sont certes plus résilients que les technologies internet, mais nous ne pouvons pas revenir à l'âge de la draisienne et du vélo. Nous réfléchissons à des dispositifs de redondance permettant d'obtenir un degré de résilience satisfaisant. Par essence, internet n'aura jamais la solidité fondamentale du téléphone commuté.

M. le président Thomas Gassilloud. Aucun système n'est plus résilient que l'opératrice à laquelle on demandait le 22 à Asnières, indépendante de tout serveur centralisé.

M. Pierrick Berteloot (RN). En ce début de XXI^{e} siècle, on ne peut que constater l'hybridité des conflits. La guerre ne se fait plus uniquement par les armes. Porter atteinte à un OIV permet de nuire gravement à la population, en l'empêchant de se nourrir et d'accéder à l'eau potable, voire à l'électricité. La paralysie de tout un pays met en cause sa défense.

Le conflit russo-ukrainien en offre un exemple. La cyberattaque de Kyivstar, principal opérateur de télécommunication ukrainien, a gravement nui aux capacités d'action ukrainiennes. L'attaque par drones de la centrale nucléaire de Zaporijia fait peser une lourde menace, en raison de la radioactivité et de la privation d'électricité, sur la population civile et militaire.

Cela doit nous inciter à redoubler de vigilance s'agissant de nos OIV, d'autant que nous pouvons être victimes d'attaques même en temps de paix, comme le prouve le vol de données personnelles dont a été victime France Travail les 5 et 6 mars derniers. Nous devons aussi être préparés aux conséquences des intempéries, en protégeant les barrages et les parcs nucléaires.

La France compte 249 OIV, dont les activités vont des transports à l'alimentation et de la communication à l'énergie. Leur champ d'action est large et varié. Plus de 60 % de l'électricité consommée en France est fournie par nos centrales nucléaires. Compte tenu de la

nécessité vitale de ce produit, nous avons tout intérêt à préserver et à entretenir notre parc nucléaire.

La centrale nucléaire de Gravelines, située dans ma région des Hauts-de-France et surnommée « la géante », est la plus grande d'Europe. Un projet de construction de deux réacteurs EPR 2 sera soumis au débat public d'ici l'été. Bien qu'il puisse contribuer à la création de plus de 30 000 emplois et au développement de la centrale, des inquiétudes pèsent. Deux anomalies de niveau 1 ont été recensées en janvier 2024 ; le nombre d'accidents du travail est en hausse. À Flamanville, un groupe d'activistes de Greenpeace s'est introduit dans la centrale en 2022. Les habitants des alentours des centrales nucléaires s'interrogent à juste titre sur leur sécurité si celle des centrales est menacée.

Sécuriser notre parc nucléaire est d'une importance capitale, non seulement pour la santé des Français, mais également pour notre souveraineté et notre indépendance énergétique. Plus nous produisons d'électricité, moins nous en importons. La situation inflationniste, qui dure depuis plus d'un an, n'a pas épargné les prix de l'énergie. Quels sont les moyens consacrés par EDF à la protection de nos centrales des accidents et des intrusions ? Comment les concilier avec d'éventuels travaux d'expansion ?

M. Stanislas Martin. Les centrales nucléaires sont conçues pour résister à des agressions d'origine naturelle, accidentelle et malveillante. Cette résistance, prévue dès la conception, est assurée pour tous les bâtiments-réacteurs, piscines de stockage comprises.

Nous faisons régulièrement évoluer le niveau de sûreté des bâtiments en fonction du contexte. Après Fukushima, les centrales ont été mises à niveau pour tenir compte d'événements externes qui n'ont pas été prévus lors de leur conception.

Nos sites ont connu plusieurs intrusions de Greenpeace, qui nous prévient toujours à l'avance. La réponse d'EDF et des pouvoirs publics, qui assurent la protection permanente des sites nucléaires grâce aux pelotons spécialisés de protection de la gendarmerie (PSPG), est proportionnée à l'intrusion. Aucune n'a franchi la première barrière de protection et n'a duré plus de dix minutes.

EDF condamne ces intrusions, qui peuvent mettre des vies en péril. Maîtriser une situation tendue, dans le noir qui plus est, n'est pas évident. Quinze militants de Greenpeace font l'objet d'une plainte d'EDF et sont et en attente de jugement.

Les PSPG rassemblent mille gendarmes, disponibles en permanence. Nos équipes de sécurité et de protection, qui sont présentes en permanence sur nos sites, travaillent en coordination avec eux et avec les pouvoirs publics. Par ailleurs, la direction générale de l'aviation civile (DGAC) surveille l'espace aérien et mobilise des moyens en cas de transgression de la loi, qui dispose que l'espace aérien, dans un rayon de cinq kilomètres autour d'un site nucléaire, est constamment surveillé et interdit de survol.

M. Frédéric Mathieu (LFI-NUPES). J'ai visité, en Estonie, une entreprise qui construit des miroirs parfaits de systèmes d'information, ce qui permet de réaliser des exercices dans des situations aussi réalistes que possible.

Lors d'un exercice, l'équivalent estonien de l'Anssi est allé jusqu'à simuler le *black-out* d'un centre de production d'électricité. Les salariés n'avaient pas été informés. Les agents de cybersécurité sont donc intervenus dans une situation de tension extrême, le désordre s'ajoutant au choc des cultures pour provoquer des conflits entre agents et salariés. Le Retex a démontré l'importance du facteur humain. Il a notamment démontré que certains

réflexes allant de soi dans le cadre d'une simulation ne sont pas automatiques en cas de crise véritable.

Quel est le niveau de réalisme de vos exercices ? Allez-vous aussi loin que les Estoniens, qui ont l'expérience des attaques russes ? Si tel n'est pas le cas, pourquoi ? Quel est le Retex de vos exercices ?

M. Patrick Guyonneau. Nous ne disposons pas de jumeaux numériques, mais nous déployons des scénarios de crise, qui n'incluent pas tous une attaque, et des *Purple Teams* constituées d'attaquants et de défenseurs chargés de simuler des attaques selon ce que nous appelons les scénarios redoutés, qui sont élaborés avec les métiers. Cela permet d'entraîner les salariés des centres de sécurité des opérations (SOC) et d'améliorer la réactivité ainsi que les processus de défense.

En 2022 et en 2023, deux opérateurs de télécommunication, Vodafone au Portugal et A[1] en Autriche, ont subi des attaques de sabotage et ont été mis à genoux. Or il s'agit d'entreprises de bon niveau et non d'opérateurs alternatifs investissant peu dans la cybersécurité, ce qui oblige à l'humilité.

M. Stanislas Martin. Les exercices sont essentiels pour assurer la continuité d'activité. Nous n'allons pas aussi loin que les Estoniens, car EDF produit de l'électricité mais n'est pas responsable de son transport, dévolu à RTE. De surcroît, nos systèmes industriels sont séparés des systèmes de gestion. Ils sont donc impénétrables de l'extérieur. Faire cesser la production d'une centrale d'EDF de l'extérieur est impossible.

Au début de la crise ukrainienne, 6 000 éoliennes d'Europe se sont soudainement arrêtées en raison de la propagation d'un virus cyber par satellite. Les réseaux ont une marge pour absorber un choc de cet ordre, d'autant qu'ils sont interconnectés d'un pays à l'autre, ce qui autorise l'entraide. Lorsque la production de la centrale de Zaporijjia est tombée, nous avons couplé, en application d'une décision européenne, le réseau ukrainien au réseau européen pour lui permettre de fonctionner.

Notre dernier exercice cyber a rassemblé 400 personnes de tous les métiers du groupe. Nous avons fait tomber les systèmes de gestion et les systèmes de communication les uns après les autres. Le Retex a démontré que, dans une crise cyber, le premier vecteur de la crise est le facteur humain, et que sa gestion dépend de la capacité à assurer la continuité d'activité.

Les entités doivent être résilientes à l'isolement de leurs capacités pendant un certain temps. Après l'invasion de l'Ukraine, nous avons fait en sorte que les PCA permettent à chaque entité de fonctionner environ une semaine de façon isolée. Sur la base de ce Retex, nous avons porté cette période à quinze jours.

Pendant les JOP, nous doublerons les astreintes cyber pour garantir la continuité d'activité des sites olympiques.

Mme Geneviève Darrieussecq (Dem). J'ai pris note qu'il faut distinguer la production – pour EDF – et la distribution – pour les deux opérateurs.

J'ai vécu, en tant que maire d'une commune des Landes, une crise climatique majeure : la tempête Klaus de 2009. Celle-ci a démontré à quel point il est difficile de conserver un accès à ce que les populations considèrent comme vital. Les fils électriques et les fils de cuivre étaient à terre ; plus aucune route n'était praticable en raison des chutes

d'arbres. Heureusement, les tronçonneuses n'étaient pas électriques et nous avons rapidement reçu des groupes électrogènes.

Cette crise, comme d'autres, a fait l'objet d'un Retex, qui a inspiré une organisation et des plans de sauvegarde, prévoyant notamment que chaque maire dispose d'un téléphone fonctionnant sur le réseau hertzien. Lors de cette crise, des communes ont été isolées pendant plusieurs jours, voire plusieurs semaines.

Un tel choc climatique donne une idée de ce qui pourrait arriver en cas de choc guerrier ou sécuritaire majeur. Vous avez parlé de mode dégradé socialement acceptable. Quel est le mode dégradé vital minimal nécessaire au fonctionnement d'un pays, d'une région ou d'un territoire subissant une attaque particulière ?

Les exercices associent-ils tous les acteurs des crises, le fonctionnement en silos étant inefficace ? Y a-t-il des freins, réglementaires ou dus au manque d'articulation entre processus ? Si oui, comment les lever ?

De quelle surveillance particulière les câbles sous-marins font-ils l'objet ? Les accidents sont-ils fréquents ? Quel est leur impact sur l'activité des pays concernés ?

M. Stanislas Martin. La tempête Klaus a eu des impacts durables sur les populations. Les tempêtes Ciaran et Domingos, qui ont récemment frappé la Bretagne et le Nord de la France, ont été encore plus dévastatrices. Nous n'avons jamais vu un réseau dans un tel état. Il n'était pas coupé à certains endroits, comme en 1999 ou en 2009, mais haché. Il a fallu tout refaire, très rapidement.

Nous avons mobilisé des moyens exceptionnels pour reconstruire les réseaux, sous le pilotage et la coordination d'Enedis et des pouvoirs publics locaux. Nous avons même envoyé la Farn. Les réseaux ont été reconstruits à 95 % en cinq jours, ce qui est exceptionnel. Il n'a fallu que quelques jours supplémentaires pour reconstruire les lignes dans leur intégralité.

Pendant l'hiver 2022-2023, nous avons travaillé avec les pouvoirs publics sur d'éventuels délestages. Depuis lors, nous avons également travaillé avec les opérateurs. En raison de notre incapacité à raccorder autant de centrales au réseau que nécessaire, compte tenu des conséquences de la crise du covid et de la corrosion sous contrainte de certaines centrales, le risque de délestage était accru. Nous nous sommes organisés avec les réseaux de transport et de distribution, en imaginant les conséquences des délestages sur la vie publique et sociale.

Nous avons réalisé un exercice de crise avec l'État en octobre, en lui demandant de réunir tous les opérateurs autour de la table. Nous sommes fournisseurs d'électricité, mais nous avons besoin de moyens de communication. Nous avons fait l'exercice sans les autres opérateurs, ce qui a démontré que, sans Orange, sans les fontainiers et sans les transporteurs, nous ne parviendrions pas à gérer la crise en anticipation. Nous avons donc fait d'autres exercices incluant tous les opérateurs d'activités essentielles à la vie économique et sociale.

En 2022, l'exercice Blackout a été réalisé avec l'État, RTE et d'autres fournisseurs d'électricité. Nous sommes toujours preneurs d'une représentation complète de l'écosystème autour de la table lors de la cinquantaine d'exercices que nous organisons chaque année, pour travailler en coordination avec nos partenaires et les OIV.

M. le président Thomas Gassilloud. Il vous serait sans doute utile de participer à Orion, exercice majeur des armées.

M. Patrick Guyonneau. S'agissant des freins, j'en identifie trois : le temps ; l'élaboration du savoir-faire pour organiser des exercices interopérateurs réalistes et complexes ; le partage d'informations classifiées entre opérateurs aux niveaux d'accréditation et aux architectures distincts. Les opérateurs travaillent à lever ces freins.

S'agissant des câbles sous-marins, nous les surveillons quotidiennement. Nous en sommes les gestionnaires bien davantage que les propriétaires, car ils coûtent très cher. Le dernier câble transatlantique a exigé plusieurs milliards de dollars d'investissement. Seuls les Gafam ont de tels moyens. En général, les câbles sous-marins sont des copropriétés.

Le câble le plus long que nous utilisons relie Singapour à Marseille, et rassemble une trentaine d'opérateurs de télécommunication au sein d'un syndic, ce qui en complexifie la gouvernance. Nous les utilisons et en assurons la maintenance, par le biais de notre filiale Orange Marine, mais nous en sommes rarement propriétaires.

Leur surveillance proprement dite est impossible, compte tenu de la profondeur à laquelle ils se trouvent – 6 000 mètres dans l'océan Atlantique –, à laquelle aucun sous-marin ne peut accéder. Des capteurs disposés le long des câbles permettent de savoir s'ils fonctionnent ou non. Notre connaissance de la sismologie permet de déterminer si une coupure est normale ou non.

Les coupures de câbles sont fréquentes ; elles occupent notre filiale Orange Marine, qui les dépose, les répare et en assure la maintenance. Les principales menaces pesant sur les câbles sont les éboulements sous-marins – le plus récent en a coupé quatre au large de l'Afrique – et, plus près des côtes, les arrachages par des filets de pêche.

Pour les années à venir, la capacité des câbles est insuffisante. Il faudra en poser d'autres. Toutefois, il est toujours possible de basculer le trafic d'un câble à un autre pour en assurer la redondance et l'écoulement. L'été dernier à La Réunion, deux des trois câbles étaient en maintenance ou en panne, et quatre câbles ont récemment été coupés au large de l'Afrique, mais de telles situations sont très rares.

M. Loïc Kervran (HOR). Le rapprochement entre l'énergie électrique et la téléphonie est intéressant, s'agissant de deux grandes activités de réseaux.

Je partage la préoccupation du groupe Renaissance au sujet de la fermeture, parfois assumée et souvent dissimulée, notamment en zone rurale, du réseau cuivre. Élu local et député, je constate que les délais de réparation d'Enedis et de RTE, d'une part, et d'Orange, d'autre part, sont très différents – c'est même le jour et la nuit : quelques heures ou quelques jours pour le réseau électrique, quelques semaines voire quelques mois pour Orange, en conditions normales. Lorsque nous interrogeons le groupe Orange, il répond souvent qu'il dépend de sous-traitants.

Je m'interroge donc sur l'externalisation du travail sur le réseau. La relation contractuelle avec les sous-traitants inclut-elle des clauses permettant d'assurer la résilience du réseau téléphonique ? Le groupe Orange dispose-t-il, comme Enedis, d'équipes dédiées à la réparation des réseaux endommagés, en cas de tempête par exemple ?

S'agissant du matériel utilisé sur les réseaux, nous avons été amenés à légiférer. En France, Orange a renoncé à utiliser du matériel fabriqué par Huawei. Utilisez-vous d'autres matériels étrangers, notamment américain, sur des segments stratégiques du réseau téléphonique ?

M. Patrick Guyonneau. Sans être spécialiste de la réparation du réseau, je puis indiquer qu'un câble téléphonique, si petit soit-il, est constitué de dizaines de paires de fils de cuivre pour chaque abonné. Ce qui est long, lors de son remplacement, n'est pas le déroulement du câble mais son raccordement.

Certaines activités de réparation et de maintenance sont sous-traitées. Par ailleurs, nous avons une équipe propre et une force d'action rapide dédiée aux crises téléphoniques et appelée Cristel. L'ampleur des réseaux des quatre opérateurs oblige à recourir à des sous-traitants, qui sont parfois les mêmes, pour ces travaux.

Ils sont soumis à des clauses de résilience et de réactivité, mais le rétablissement d'un réseau téléphonique prend inévitablement du temps. Une réunion se tiendra demain à la direction générale des entreprises (DGE) pour faire le point et étudier les pistes d'amélioration.

S'agissant du matériel de télécommunication, il n'y a plus d'équipementier français. Je dois choisir mes dépendances entre les pays nordiques, ceux d'Asie et les États-Unis. La gestion des risques du groupe Orange inclut l'étude de ces dépendances aux fournisseurs qualifiés de vendeurs à haut risque.

Mme Isabelle Santiago (SOC). L'article 67 de la LPM 2024 – 2030 modifie les règles de fonctionnement des opérateurs de communications électroniques et des OIV. Vous semble-t-il suffisant ? Correspond-il à vos attentes ? Soulève-t-il des problèmes ?

Les câbles sous-marins sont un enjeu stratégique majeur. Leur surveillance a longtemps été inexistante, même au point de départ. Sommes-nous désormais dans le bon spectre de surveillance et de gestion ? Sommes-nous capables d'assurer un bon niveau de résilience et de sécurité ?

À Djibouti, les bases françaises, américaines et japonaises sont situées du même côté du port. La base chinoise leur fait face. Elle est située à l'aplomb de câbles par lesquels transite une bonne part de la communication mondiale. Je suis étonnée par la naïveté dont nous avons fait preuve pendant si longtemps.

M. le président Thomas Gassilloud. Les Chinois ont offert à la ville de Djibouti un système de vidéosurveillance.

M. Patrick Guyonneau. En raison du coût des câbles sous-marins, tous les opérateurs s'efforcent de les poser au plus court – de même que les participants à une course à pied prennent les virages au plus court. À certains endroits, notamment au large de la corne de l'Afrique et à l'entrée de la mer Rouge, les câbles suivent tous le même tracé. Instruits par l'incident survenu récemment au large de l'Afrique, nous essaierons d'éloigner les prochains câbles que nous poserons les uns des autres pour éviter qu'un éboulement en coupe plusieurs.

S'agissant de l'atterrage des câbles, il est soumis à une enquête d'utilité publique, ce qui en dévoile la localisation exacte – au demeurant, l'emplacement de ceux qui courent sous les trottoirs est connu des mairies. Nous sommes soumis à des injonctions contradictoires. En nous prêtant à des enquêtes d'utilité publique, nous satisfaisons aux exigences de transparence, mais nous permettons au grand public de savoir exactement où arrivent nos câbles, et donc aussi aux potentiels acteurs malveillants.

Là où cela est possible, nous installons des clôtures, mais la loi littoral limite fortement cette démarche. Dans les abords maritimes, nous avons placé quelques câbles dans

des coquilles de protection, avec des conséquences catastrophiques sur la maintenance. Nous sommes toujours à la recherche d'une solution technique.

Les câbles sous-marins et pas davantage les réseaux terrestres correspondent mal à la notion de PIV, car nous nous inscrivons dans un monde de flux, qui transitent par des milliers de kilomètres de réseau. Nous ne pouvons que demander des patrouilles de gendarmerie ou de police, et travailler avec les préfectures dans le cadre des plans de protection externes (PPE). Nous ne disposons d'aucune autre garantie.

L'article 67 de la LPM 2024 – 2030 modifie notamment l'article L. 2321-2-1 du code de la défense s'agissant des marqueurs techniques. Nous souhaitions, sans vouloir tendre la sébile, que la loi prévoie une indemnisation, dans la mesure où nous ne collectons pas les données personnelles de nos abonnés.

Or cette noble assemblée a autorisé l'Anssi à déployer des marqueurs de contenu pour détecter les cyberattaques, même s'il s'agit d'hameçonnage. En ce qui nous concerne, nous n'avons pas le droit de collecter les données personnelles. Pour parvenir à un dispositif optimal, il faut adapter nos réseaux, car les données de connexion représentent des volumes importants.

De plus, l'application de l'article L. 33-14 du code des postes et des communications électroniques modifié par ce même article 67 patine. Lorsque nous recevons une réquisition de l'Anssi, nous transmettons ce dont nous disposons, mais nous sommes techniquement limités s'agissant des marqueurs techniques.

M. le président Thomas Gassilloud. Dans le cadre du suivi de l'exécution de la LPM 2024 – 2030, le rapporteur rédigera un rapport à ce sujet.

Nous en venons aux interventions des autres orateurs.

M. Yannick Chenevard (RE). J'ai eu le plaisir de visiter la cellule de crise d'EDF. Son mode de fonctionnement est rassurant. Notre niveau de préparation à la gestion de crise est excellent.

Orange Marine fait de la France l'un des leaders mondiaux de la pose et de la réparation des câbles sous-marins, ce qui est un atout en matière de surveillance et de sécurité. Le groupe Orange prévoit-il un véritable mode dégradé si les réseaux tombent ?

Le partage de la sous-traitance ne me rassure pas, dans la mesure où tout le monde formulera la même demande au même moment. Par ailleurs, quels sont les niveaux de sûreté appliqués aux sous-traitants, compte tenu du fait qu'ils ont accès à certaines données ?

Mme Natalia Pouzyreff (RE). Les actes de vandalisme contre les armoires téléphoniques de rue ont un effet délétère sur les populations. Outre le sentiment d'impunité que suscite la vue d'armoires ouvertes et détériorées, elles ont l'impression que les réparations ne sont pas effectuées en temps et en heure, dans la mesure où les opérateurs de réseaux et les opérateurs de services se renvoient la balle. Comment améliorer cet état de fait, qui donne une image dégradée de la résilience et de la sécurité que les Français sont en droit d'attendre ?

Mme Lysiane Métayer (RE). Messieurs, vos groupes respectifs jouent un rôle critique dans divers aspects de la vie quotidienne, notamment les communications gouvernementales, les services d'urgence et, en ce qui concerne Orange, les câbles sous-marins. Rapporteure d'une mission flash sur les fonds marins et auditrice de l'Ihedn, j'ai visité plusieurs installations.

La protection et la sécurisation des réseaux des OIV sont une priorité, car ils peuvent être ciblés par des attaques cybernétiques ou des actions hostiles visant à perturber les services essentiels. Comment les directives du SGDSN sont-elles intégrées dans les stratégies de sécurité pour garantir la résilience des infrastructures critiques ? Quelles sont les mesures prises pour anticiper et répondre aux menaces cybernétiques émergentes ?

M. Patrick Guyonneau. La dégradation des armoires de rue porte aussi un coup au moral de nos salariés, dont certains sont agressés verbalement, voire physiquement. Nous signalons systématiquement ces incidents en portant plainte pour mise en danger de la vie d'autrui, car ces dégradations entravent le fonctionnement des numéros d'urgence. La FFTélécoms en tient le compte chaque mois.

Nous avons des conventions avec les services de police, de gendarmerie et de justice de chaque département, mais aucune suite pénale n'est donnée à nos signalements. Toutes les plaintes, qu'il s'agisse de vols de cuivre ou de dégradations malveillantes, sont classées sans suite. En revanche, un bel effort a été réalisé, depuis deux ou trois ans, en matière d'atteintes aux antennes mobiles, qui ont donné lieu à des arrestations.

S'agissant du mode dégradé, le système des télécommunications est constitué de boucles. S'il est coupé à un endroit, il continue de fonctionner. Toutefois, à l'échelle de l'abonné, le lien avec la boucle est unique. Si une armoire brûle ou si quelqu'un coupe un câble, la ligne est coupée. Certains clients, prioritaires ou sensibles, obtiennent une double adduction, coûteuse et complexe en matière de travaux publics.

En l'absence d'accident grave, tel qu'une panne, le système fonctionne. La crise dite des numéros d'urgence n'en était pas vraiment une. Un équipement de reroutage entre les réseaux modernes et le réseau cuivre est tombé en panne, suivi de tous les autres, en raison de la propagation rapide d'une anomalie logicielle due à une mise à jour.

Nous prenons des précautions, notamment en testant les procédures de maintenance sur des plateformes de préproduction, qui toutefois sont peu représentatives des plateformes de production.

Face aux cybermenaces, nous prenons de nombreuses mesures. La sensibilisation de nos salariés, notamment à la fraude au président, au hameçonnage et à la solidité des mots de passe, est notre premier niveau de défense. Par ailleurs, nous allions défense périphérique ou périmétrique et défense dans la profondeur, en empilant les systèmes et les couches de défense, avec des technologies variées, ce qui limite la vulnérabilité de l'ensemble.

Ces actions figurent dans les directives de l'Anssi et dans la directive NIS 2. Nous les adaptons au domaine des télécommunications, dans le cadre d'une politique applicable à toutes les entités et à toutes les filiales du groupe. Nous contrôlons son application et son efficacité *in situ*, essentiellement par des audits de conformité et de type *pain test*. Il s'agit d'un travail colossal, compte tenu de notre patrimoine – Orange compte plus de 100 millions d'adresses IP.

M. Stanislas Martin. La résilience de nos entreprises et de nos activités est l'un des objectifs essentiels de la gestion des risques et de la gestion de crise, en anticipation et en situation réelle. En matière de résilience, nous adoptons une posture d'humilité. Il faut disposer d'un dispositif solide et entraîné, mais nous ne pouvons pas imaginer toutes les crises qui peuvent survenir.

Il faut donc prendre les crises avec un certain degré d'humilité et se remettre en question en permanence, en conservant l'ouverture d'esprit nécessaire à l'intégration des

événements et au Retex. Le projet de loi relatif à la résilience, qui intégrera toutes les directives européennes, renforcera encore nos systèmes et nos capacités de réaction, pourvu qu'il simplifie le millefeuille des obligations qui s'imposeront à nous.

M. le président Thomas Gassilloud. Messieurs, merci de vos propos, qui nous rassurent sur notre capacité à avoir de l'électricité et à communiquer. Nous devons être fiers de ce que nous faisons en France, ainsi que du bon niveau de sûreté et des pépites industrielles dont nous disposons.

*

* *

La séance est levée à douze heures quarante-sept.

*

* *

Membres présents ou excusés

Présents. – M. Jean-Philippe Ardouin, M. Mounir Belhamiti, M. Pierrick Berteloot, M. Benoît Bordat, M. Yannick Chenevard, Mme Caroline Colombier, Mme Geneviève Darrieussecq, M. Thomas Gassilloud, Mme Anne Genetet, M. Frank Giletti, M. Christian Girard, M. José Gonzalez, M. Pierre Henriet, M. Laurent Jacobelli, M. Jean-Michel Jacques, M. Philippe Juvin, Mme Gisèle Lelouis, Mme Patricia Lemoine, M. Frédéric Mathieu, Mme Lysiane Métayer, M. Pierre Morel-À-L'Huissier, M. Christophe Naegelen, Mme Natalia Pouzyreff, M. Julien Rancoule, M. Aurélien Saintoul, Mme Isabelle Santiago, M. Bruno Studer, M. Michaël Taverne

Excusés. – Mme Valérie Bazin-Malgras, M. Christophe Blanchet, M. Frédéric Boccaletti, Mme Yaël Braun-Pivet, M. Steve Chailloux, Mme Martine Etienne, M. Jean-Marie Fiévet, M. Bastien Lachaud, M. Jean-Charles Larsonneur, Mme Anne Le Hénanff, Mme Murielle Lepvraud, Mme Pascale Martin, Mme Valérie Rabault, Mme Marie-Pierre Rixain, M. Fabien Roussel, M. Mikaele Seo, Mme Nathalie Serre, M. Jean-Louis Thiériot, Mme Mélanie Thomin