Commission des Affaires étrangères et de la Défense – 6 février 2019
Communication au sujet de la cyberattaque de la plateforme Ariane, par les sénateurs Rachel Mazuir et Olivier Cadic

Monsieur le Président,
Chers collègues,

Le ministère des affaires étrangères a mis en place, depuis 2010 une plateforme de service ARIANE qui permet aux ressortissants français qui s'inscrivent en ligne de recevoir lors de leurs voyages à l'étranger des consignes de sécurité.

Chacun peut donc, sur le site « diplomatie.gouv.fr », créer un « compte utilisateur » et avant chaque voyage s'enregistrer en précisant ses lieux de passage, son numéro de téléphone portable et son adresse électronique, mais aussi dans les données du compte utilisateur les personnes à prévenir en cas d'urgence. Au cours du séjour à l'étranger et si la situation du pays le justifie, l'usager reçoit des recommandations de sécurité du centre de crise et de soutien du ministère, par SMS ou par courriel, et peut être contactée en cas de crise. C'est donc un service très utile et très utilisé.

Le Centre de crise et de soutien du ministère, est le service responsable du traitement. Ce Centre et les postes diplomatiques et consulaires français sont destinataires des données. La plateforme est maintenue par la direction des systèmes d'information.

Le 5 décembre 2018, la plateforme Ariane a été victime d'une cyberattaque. Cette attaque a été détectée par un dispositif de protection mis en place par l'ANSSI en périphérie des systèmes d'information du ministère. Ce dispositif a pu constater qu'une partie des données stockées dans cette base de données a été piratée.

Des données personnelles enregistrées lors de l'inscription sur la plateforme ont été dérobées. Selon le ministère des affaires étrangères, il s'agit de données extraites de la table des personnes à contacter en cas d'urgence : nom, prénom, adresse électronique et d'une partie des identifiants téléphoniques pour lesquels il avait été sagement prévu un stockage fractionné dans deux tables différentes ce qui empêche leur exploitation frauduleuse. Au total, ce sont 540 563 personnes qui sont concernées par ce vol de données. Ni les autres données des titulaires de comptes, ni leur mot de passe, ni les dates et destinations de leurs voyages n'ont été compromises et les données dérobées ne permettent pas de faire de lien entre les contacts et les titulaires de compte. En outre, il a été constaté lors de l'opération d'information des personnes concernées qui a consisté en l'envoi d'un courriel, que plus de 200 000 de ces adresses n'étaient plus actives.

Le service n'a pas été interrompu et la sécurisation des données a été restaurée, des mesures correctives ont été prises pour empêcher la reproduction d'une attaque selon les mêmes procédures.

L'incident a été connu du grand public le 13 décembre, date à laquelle le ministère a adressé un courriel d'information aux personnes concernés et un communiqué de presse. Ce communiqué annonçait que le ministère avait saisi la CNIL ainsi que la justice des faits constatés.

Sitôt l'incident connu, parce que nous avions souligné depuis deux ans dans notre avis budgétaire sur l'ANSSI, les résultats insuffisants de la mise en œuvre de la politique de protection et de sécurité des systèmes d'information de l'Etat (PSSIE) et que la cyberattaque touchait un ministère sur lequel la commission était légitime à assurer un contrôle, **nous avons demandé au président de pouvoir organiser des auditions pour recueillir des éléments d'information** sur cette attaque et plus largement sur la sécurité de systèmes d'information du ministère des affaires

étrangères. La commission a validé cette démarche lors de sa réunion du 16 janvier. Nous nous sommes naturellement concentrés dans un premier temps sur cette cyberattaque dans l'intention, non de chercher des coupables et des responsables, mais de susciter un retour d'expérience dont le ministère et au-delà les services de l'Etat pourraient tirer des enseignements pour les prochains incidents qui ne manqueront pas de se produire compte tenu des vulnérabilités de nos systèmes, d'une part, de la fréquence, de l'ampleur et de la sophistication des attaques, d'autre part.
Nous avons donc entendu, dès le 19 décembre, le directeur général de l'ANSSI, le directeur des systèmes d'information et le directeur de la sécurité diplomatique du ministère des affaires étrangères, la direction générale de la sécurité intérieure qui est l'un des services disposant des capacités d'investigation pour rechercher l'origine d'une cyberattaque, la CNIL et enfin la section spécialisée du parquet de Paris. Nous entendrons dans les prochains jours, lorsqu'elle aura rendu son rapport, la mission interministérielle d'inspection que le Premier ministre a chargé de cartographier les moyens budgétaires et en effectifs des ministères dédiés à l'action numérique, dont la sécurité, et nous attendons le retour des réponses à des questions complémentaires que nous avons adressées à l'ANSSI et au ministère des affaires étrangères.
Ces éléments nous permettrons de compléter notre analyse et peut-être de préciser ou nuancer certaines des observations et appréciations que nous allons vous livrer selon les points d'attention suivants :

1. La capacité du ministère à éviter cette attaque, que je traiterai.

2. La déclaration du vol de données personnelles à la CNIL et ses conséquences,
3. La communication sur l'attaque et ses conséquences
4. L'attribution de l'attaque et ses suites judiciaires
5. Le pilotage de la gestion de crise en cas de cyberattaque. Points que traitera Olivier Cadic.

1. Je commence donc par **la capacité du ministère à éviter cette attaque.** Les attaquants ont profité d'une faille dans une brique logicielle utilisée pour construire cette plateforme. L'éditeur du logiciel avait identifié cette faille et livré à la DSI le correctif nécessaire. La mise à jour n'avait pas encore été installée. Elle nécessite en effet une programmation de moyens, notamment en effectifs, et n'avait pas été considérée comme une absolue priorité. De cette situation nous tirons deux enseignements. Premièrement : quelques attaquants connaissent les failles, l'édition d'un correctif révèle plus largement l'existence de failles et suscite des appétits, plus on tarde à installer une mise à jour, plus un système d'information est vulnérable. Deuxièmement, comme d'autres ministères, le ministère des affaires étrangères dispose d'un budget dédié au système d'information et d'effectifs en stagnation, alors qu'il s'est lancé dans une politique de numérisation et de mise à disposition de services en ligne ce qui créé une interface de vulnérabilité, il consacre des moyens globalement insuffisants à la cybersécurité et concentre ceux-ci - on ne peut le lui reprocher - sur les systèmes d'information et de communication les plus stratégiques comme la sécurité des postes et des réseaux diplomatiques. La circulaire interministérielle de 2014 sur la politique de sécurité des systèmes d'information de l'Etat (PSSIE) est appliquée de façon hétérogène ce qui montre le caractère très limité des interventions réglementaires. Sans affectation de moyens, elle demeure un seul instrument de communication. De surcroît les fonctions clefs de la chaîne de sécurité, haut fonctionnaire de défense et de sécurité (HFDS) et fonctionnaire de sécurité des systèmes d'information (FSSI) ont été, ces derniers mois, exercées de façon

intermittente. Tout cela pose concrètement la question d'un pilotage interministériel par affectation de moyens notamment par le respect d'un ratio obligatoire consacré à la cybersécurité. L'ANSSI n'a pas aujourd'hui de telles capacités.
Je laisse la parole à Olivier Cadic.

2. J'aborde, comme vous l'a annoncé Rachel Mazuir, **la déclaration du vol de données personnelles à la CNIL et ses conséquences.** L'application Ariane a fait l'objet d'une déclaration à la CNIL. La notice de l'application indique que « *le service Ariane conçu en concertation avec la CNIL offre toutes les garanties de sécurité et de confidentialité des données personnelles* » et que « *les données sont effacées un mois après la date retour* ». S'entend les données relatives aux déplacements, non les données de base du dossier, dont les données relatives au contact puisque plus de 500 000 noms étaient stockés dans cette table depuis l'origine semble-t-il. Cela pose au demeurant une question, qui aura quelques conséquences lors de la communication sur la cyberattaque, celle du statut des données personnelles des contacts enregistrées par leurs proches avec ou sans leur consentement, présumé tacite.
En outre, depuis l'entrée en application du Règlement général sur la protection des données (RGPD), la compromission de données personnelles doit faire l'objet d'une déclaration à la CNIL dans les 72 heures de sa détection. Cette déclaration a été faite via un formulaire en ligne dès le 7 décembre. La question s'est alors posée pour le ministère de savoir si cette attaque, présentait des risques tels qu'outre son signalement, il doive faire l'objet d'une communication aux personnes concernées d'une part, au public d'autre part. Du dialogue entre les deux parties, la DSI et la CNIL, et parce qu'il y avait un risque d'utilisation des données pour des opérations d'hameçonnage ou d'escroquerie, la décision a été prise de communiquer. On constatera que ce dialogue est resté confiné, autant que nous le sachions entre la DSI et la CNIL, sans autre appréciation externe ou évaluation de l'éventualité d'un autre motif de l'attaque qui pouvait être simplement l'atteinte à la réputation du ministère en affichant la vulnérabilité de ses applications, ni prise en compte du fait que les personnes concernées pouvaient découvrir leur présence dans cette base à cette occasion. Ceci aurait permis, le cas échéant, d'orienter différemment la communication. La DSI expérimentait ces nouvelles obligations avec une certaine appréhension, leur non-respect pouvant entraîner des sanctions pénales. Le secrétariat général de la CNIL restait sur une vision juridique et factuelle ne disposant pas d'appréciations complémentaires que les simples éléments transmis par la DSI.

3. La communication sur l'attaque et ses conséquences. Le 13 décembre était adressé un courriel aux personnes concernées dont nous n'avons pas pu prendre connaissance à ce stade. Nous savons par l'ANSSI et par la CNIL qui ont reçu, dans la foulée, des dizaines de demandes d'information, qu'il a eu pour effet d'inquiéter nombre de destinataires qui, soit n'étaient pas informés de leur présence sur ce fichier, soit n'avaient aucune idée des données contenues dans celui-ci, et qui pensaient être victime d'une opération d'hameçonnage sous couvert d'un message falsifié du ministère, ou que leurs données bancaires ou d'autres données personnelles pouvaient être altérées. Ceci constitue à mes yeux, un début de trouble à l'ordre public. A échelle réduite, les personnes contactées ont pu être rassurées mais personne dans les organisations concernées n'avait envisagé un retour de cette nature et n'y était préparé. L'ANSSI tout particulièrement qui a été informé de la communication lorsqu'elle a été confrontée à ces appels.

De même un communiqué de presse a été adressé, repris parfois de façon alarmiste par les médias et complété sur le site du ministère par « une foire aux questions ». On notera, en premier lieu, qu'il y a eu deux communiqués successifs, le premier impliquant l'ANSSI sans son consentement et sans qu'elle ait été associée ni à la mise en place des correctifs, ni dans la préparation de cette communication, le second ayant retiré la mention la concernant. Ce communiqué a été mis au point par le service de la communication du ministère à partir d'éléments technique fournis la DSI. Ensuite, à notre connaissance le Centre de crise et de soutien, responsable du traitement n'a pas été partie prenante. De principe, il nous semble compte tenu de l'effet de cette communication, qu'il y a lieu de s'interroger sur un élargissement du nombre de partie prenante à la décision et au contenu de la communication. Enfin, nous nous interrogeons également sur l'intérêt de relativiser les faits en indiquant que la cyberattaque n'a rien d'un évènement exceptionnel, que « *le ministère fait l'objet d'attaques de toutes natures et de toutes origines et s'est organisé en conséquence avec l'aide de ses partenaires interministériels, notamment l'ANSSI* », au moment où il affiche la vulnérabilité d'une de ses plateformes.

4. L'attribution de l'attaque et ses suites judiciaires. Le communiqué du 13 décembre indique que le ministère a déposé une plainte auprès du Procureur. Ceci est tout à fait souhaitable même si l'attaque ne se traduit pas par un dommage matériel pour le ministère, reste l'atteinte à la réputation du ministère. Il faut d'ailleurs féliciter le ministère pour cette décision qui reste exceptionnelle au sein des administrations pourtant victimes régulières de cyberattaques, alors même que le discours de la puissance publique est d'inciter les entreprises à porter plaintes. En outre, il s'agit d'infraction, de délits voire de crimes dont la commission doit être portée à la connaissance de la justice, obligation sanctionnée pénalement pour les fonctionnaires en application de l'article 40 du code de procédure pénale.
Nous avons donc souhaité dans le strict respect de l'indépendance et des compétences de l'autorité judiciaire comprendre comment fonctionnait ce que la Revue stratégique de cybersécurité de février 2018 appelle la chaîne « investigation judiciaire » et comment s'articulait la mise en œuvre de cette chaîne lorsque des attaques concernent des administrations de l'Etat. Nous avons reçu la section spécialisée du parquet de Paris créée en 2014 et dotée d'une compétence concurrente nationale depuis 2016, qui reçoit 2000 à 2500 plaintes par an, est en mesure de déclencher des procédure d'entraide internationale et jouit d'une solide réputation puisqu'il coordonne à l'échelon européen l'enquête sur la cyberattaque *Notpetya* et un service de police, en l'occurrence la DGSI, qui peut être actionnée pour constater les faits, rechercher des preuves et les auteurs.
De ces entretiens, il ressort une absence de concertation et de procédure formalisée. Le Parquet a été informé le 14 décembre en lisant la presse suite à la publication du communiqué du 13, lequel indiquait la saisine du Procureur. En réalité, la plainte ne sera déposée au Parquet que le 7 janvier soit un mois après la détection de l'attaque et la DGSI sera officiellement saisie le 10. Ceci montre à l'évidence que personne ne savait quelle conduite tenir et n'était préparé à ce qui devrait être un réflexe ordinaire. Même si les données relatives à l'attaque ont pu être conservées sans être altérées, on imagine que l'intervention dans les premières heures peut avoir un intérêt pour recueillir des preuves, ou des traces qu'un attaquant peut effacer progressivement, ceci nous a été confirmé par les magistrats du Parquet, ou, en tous cas, pour vérifier si les données font l'objet d'un commerce sur le *darknet*.

Sans doute, la mise en place du RGPD permettra-t-elle d'avancer grâce à l'obligation de déclaration et de publicité, mais manifestement, un travail d'information et de coordination semble nécessaire auprès des décideurs des administrations de l'Etat.

5. Le pilotage de la gestion de crise en cas de cyberattaque. Enfin et ce n'est pas une surprise parce que nous sommes au début d'une ère de turbulence. Nous voyons bien, à l'examen de ce dossier, que les administrations, à l'exception de l'ANSSI, ne sont guère préparées, qu'à chaque étape, elles hésitent sur la conduite à tenir parce qu'elles n'ont pas expérimenté les difficultés, parce que les précédents sont peu nombreux, et qu'elles n'ont pas anticipé des scénarios de crise.
En fait, on constate qu'une réflexion au sein des ministères et sans doute, au moins dans la phase initiale au niveau interministériel car l'implication de l'ANSSI est nécessaire, doit être engagée en matière de gestion de crise : quels sont les acteurs internes et externes concernés ? quels sont les niveaux de décisions adéquats ? qui pilote ? selon quelles procédures ? comment communiquer à quel moment pour ne pas ajouter une crise à la crise ?... Beaucoup de chose restent à construire et à éprouver sous forme d'exercices. Il existe des plans à l'échelle interministérielle pour des attaques du haut du spectre pilotés par le SGDSN, mais pour des attaques de moyenne ampleur, les ministères restent démunis.
Voici nos premières conclusions, alarmistes mais surtout réalistes. Elles doivent contribuer à la prise de conscience des risques et de leur caractère multiforme. En déroulant modestement le fil d'Ariane, nous mettons en évidence, le sous-investissement de nos administrions publiques en matière de cybersécurité et nous rejoignons le cri d'alarme lancé récemment par Guillaume Poupard sur les conséquences que pourraient avoir des attaques massives contre nos administrations. Un redressement est nécessaire et ce dossier doit être porté au plus haut niveau de l'Etat. Le Premier ministre a lancé plusieurs missions dans cette direction que nous allons suivre avec attention. En attendant et en y associant naturellement les rapporteurs du programme 105, nous souhaiterions poursuivre cette mission à la fois pour compléter la documentation du dossier Ariane mais aussi pour vérifier les efforts entrepris pour la sécurité de l'ensemble des systèmes d'information du ministère des affaires étrangères. Nous solliciterons des entretiens au niveau appropriés du ministère des affaires étrangères et du SGDSN pour partager ce RETEX et inciter les services de l'Etat à progresser pour mieux se prémunir des attaques et de leurs conséquences.