ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION SUR LA DIMENSION CIVILE DE LA SÉCURITÉ (CDS)

RAPPORT*

Visite virtuelle en Estonie

22 avril 2021

098 CDS 21 F | Original : anglais | 21 mai 2021

* Ce rapport de mission est présenté à titre informatif uniquement et ne représente pas le point de vue officiel de l'Assemblée. Il a été établi par Nathan Robinson Grison, directeur de la commission sur la dimension civile de la sécurité.

I. INTRODUCTION

1. Le 22 avril 2021, 18 parlementaires de 14 pays membres et partenaires de l'OTAN et du parlement européen ont participé à une visite virtuelle de la commission sur la dimension civile de la sécurité (CDS) en Estonie. Les parlementaires ont entamé des discussions soutenues avec des experts du gouvernement, de l'armée, des universités et de la société civile sur l'expérience de l'Estonie en matière de :

- renforcement de la résilience sociétale face à la désinformation ;
- lutte efficace contre les cyberattaques ;
- facilitation des interactions pratiques, directes et sécurisées entre les citoyens et les institutions publiques par des moyens électroniques.

2. Le président de la CDS, **Angel Tilvar** (Roumanie), salue les membres et remercie la délégation estonienne d'accueillir la commission en Estonie, et ce, malgré le déroulement en ligne de cette rencontre. Il note que la désinformation et les cyberattaques constituent des menaces majeures pour la sécurité des sociétés alliées. Des acteurs mal intentionnés utilisent de plus en plus ces méthodes de guerre hybride pour promouvoir leurs intérêts stratégiques et compromettre la sécurité et la résilience démocratique des Alliés. L'exemple de l'Estonie donne des indications sur la manière dont les pays de l'OTAN peuvent développer davantage leur capacité à répondre à ces défis.

3. La cheffe de la délégation estonienne auprès de l'AP-OTAN, **Oudekki Loone**, souhaite la bienvenue aux membres pour cet événement et évoque la question de la définition et de la classification des cybermenaces et de la désinformation. Elle ajoute que l'Estonie a mis au point une série de pratiques exemplaires en matière de lutte contre ces menaces et qu'elle contribue aujourd'hui à l'élaboration d'approches communes à l'égard de celles-ci avec l'OTAN.

4. La réunion s'est déroulée conformément aux règles de Chatham House. Ainsi, le rapport suivant passe en revue les principaux thèmes abordés sans attribuer de positions ou de points de vue aux participants.

II. L'EXPÉRIENCE DE L'ESTONIE EN MATIÈRE DE RÉSILIENCE FACE À LA DÉSINFORMATION

A. LES MENACES AUXQUELLES LA SOCIÉTÉ ESTONIENNE EST CONFRONTÉE DANS L'ESPACE D'INFORMATION

5. Les activités d'information hostiles constituent une menace majeure pour l'Estonie. La Russie a utilisé ces activités contre le pays balte dans le cadre de sa stratégie de guerre hybride. En infiltrant et en corrompant l'environnement informationnel local, Moscou vise avant tout à façonner l'opinion publique vis-à-vis de la Russie, à engendrer une polarisation sociétale, ainsi qu'à créer et exacerber le mécontentement à l'égard des autorités. En définitive, les campagnes de désinformation et de propagande de la Russie visent à saper la légitimité des autorités nationales et la résilience de la société estonienne.

6. Représentant environ 25 % de la population du pays, les russophones s'appuient principalement sur les médias en langue russe pour accéder à l'information. Ils sont donc plus exposés à la désinformation et à la propagande de Moscou. La Russie tente d'exploiter cette exposition substantielle en diffusant de la désinformation visant spécifiquement la minorité

russophone. Toutefois, 30 ans après l'indépendance de l'Estonie, la population russophone se sent davantage intégrée dans la société estonienne et ses habitudes de consommation des médias se déplacent des chaînes basées en Russie vers les chaînes nationales. En 2015, la radiotélévision publique estonienne a lancé ETV+, la première chaîne de télévision publique en langue russe et en accès libre en Estonie. La Russie est donc de moins en moins capable d'atteindre et d'instrumentaliser la minorité russophone comme elle l'a fait en 2007.

7. Cette année-là, après que le gouvernement estonien a décidé de déplacer un monument aux troupes soviétiques du centre de Tallinn vers un cimetière militaire voisin, la Russie a lancé une campagne de désinformation intensive. Cette campagne, qui s'est étendue sur plusieurs mois, visait principalement la minorité russophone et est parvenue à provoquer des émeutes dans les rues. Elle s'est déroulée en parallèle à tout une série de cyberattaques, constituant le premier cas connu d'attaques du genre perpétrée par un pays contre un autre.

8. La Russie a réussi à diffuser sa désinformation dans l'ensemble de l'espace d'information estonien à plusieurs autres occasions. Par exemple, en 2008, les médias russes ont relayé des allégations selon lesquelles l'Estonie était impliquée dans le conflit en Géorgie, allégations qui ont été prises pour argent comptant par certains médias estoniens. Au cours des années suivantes, les médias estoniens ont tiré les leçons de leurs erreurs et renforcé leur capacité à distinguer les fausses nouvelles des vraies en vue d'éviter toute nouvelle propagation de la désinformation russe.

9. Certains citoyens restent toutefois vulnérables à la manipulation et susceptibles de se transformer en vecteurs de désinformation. Des niveaux insuffisants d'éducation aux médias et d'éducation numérique amplifient la circulation de la désinformation (la diffusion par inadvertance d'informations inexactes) et de la mésinformation. Cela est devenu d'autant plus flagrant pendant la pandémie, certains Estoniens ayant contribué à la diffusion de diverses théories du complot liées au virus sur les réseaux sociaux. Les acteurs russes diffusant des informations hostiles se servent de la confusion du public et de son incapacité à faire la distinction entre le vrai et le faux pour propager auprès de la population estonienne nombre de propos mensongers et préjudiciables.

10. Des outils sophistiqués tels que les *deep fakes* (ou hypertrucages) sont devenus une source de préoccupation pour les autorités du monde entier, y compris en Estonie. Ils ne semblent toutefois pas encore constituer une menace majeure dans l'espace d'information, car des solutions pour les identifier et les exposer existent. Au contraire, les acteurs de désinformation et de propagande ont tendance à privilégier des outils moins avancés et moins techniques, et qui devraient dès lors être au centre de la riposte face aux activités d'information hostiles.

B. L'APPROCHE MULTIDIMENSIONNELLE DE L'ESTONIE POUR LUTTER CONTRE LA DÉSINFORMATION

11. Au cours des deux dernières décennies, l'Estonie a développé un cadre institutionnel et stratégique solide pour lutter contre la désinformation. Ce cadre a continuellement évolué et fait l'objet d'améliorations basées sur les défis auxquels le pays a été confronté dans ce domaine et les leçons qu'il en a tirées.

12. La défense psychologique et la communication stratégique sont les pierres angulaires de la réponse de l'Estonie face aux activités d'information hostiles. Elles constituent l'un des six piliers du concept de sécurité nationale de l'Estonie. La défense psychologique désigne les efforts visant à informer et à sensibiliser le public à la désinformation qui cherche à saper l'ordre constitutionnel et les principes sociétaux du pays. La communication stratégique consiste à assurer la cohérence de tous les messages et actions politiques, économiques et

de défense de l'Estonie et à les communiquer avec succès au public. La défense psychologique et la communication stratégique se complètent et sont essentielles pour neutraliser les activités d'information hostiles.

13. Une équipe dédiée à la communication stratégique a été créée au sein du bureau du gouvernement en 2018. Les trois principaux piliers de son travail sont le développement de la connaissance de la situation, l'amélioration de la résilience face aux activités d'information hostiles et la garantie de l'efficacité et de l'efficience des communications gouvernementales en cas de crise.

14. La connaissance de la situation est essentielle à la communication stratégique, car elle donne aux décideurs une vue d'ensemble de la situation et les aide à réagir aux évolutions en cours. Les autorités estoniennes développent leur connaissance de la situation à travers deux axes de travail. Premièrement, ils analysent et surveillent l'espace d'information en Estonie, en Russie et dans certains pays alliés. Deuxièmement, ils entreprennent des recherches sur les convictions et les comportements sociaux des Estoniens. Si les efforts en matière de connaissance de la situation se concentrent généralement sur les questions de sécurité, ils se sont étendus au cours de l'année écoulée pour inclure les thématiques liées à la Covid-19.

15. La communication stratégique et la transparence sont au cœur de la stratégie des autorités estoniennes pour lutter contre la désinformation. Son évaluation de la menace qui pèse sur la société estonienne est régulièrement rendue publique. Une approche qui garantit une compréhension commune au public et aux autorités des risques de désinformation auxquels le pays est confronté. Les services de sécurité publient des rapports annuels sur les menaces auxquelles le pays fait face, notamment dans l'espace de l'information, et font preuve d'une volonté d'exposer les acteurs à l'origine des campagnes de désinformation et les méthodes utilisées à ces fins, lorsque cela est possible.

16. Les autorités estoniennes ont intensifié leur capacité à communiquer efficacement avec la population pendant la pandémie de Covid-19. Ils ont établi une liste de réserve d'experts des secteurs public et privé, formés à la communication de crise. En cas d'urgence, ces experts peuvent soutenir les autorités et contribuer à leurs efforts de communication.

17. Il est essentiel de développer l'éducation aux médias au sein du public pour éviter que les citoyens ne deviennent des propagateurs involontaires de désinformation et/ou de mésinformation. L'Estonie a donc développé des solutions innovantes pour favoriser la résilience face à la désinformation. Le programme d’études secondaires comprend un cours obligatoire sur la manipulation des médias et met l'accent sur l'enseignement de la cyberhygiène et de l'hygiène de l'information. Les autorités estoniennes organisent également une semaine nationale d'éducation aux médias et distribuent à la population des brochures sur la préparation du secteur civil.

18. Enfin, les autorités comptent sur les organisations de la société civile pour soutenir le développement de la résilience de la société face à la désinformation. Les organisations non gouvernementales sont des acteurs clés dans les efforts déployés par l'Estonie pour renforcer ses capacités de défense psychologique contre les activités d'information hostiles.

III. L'EXPERTISE DE L'ESTONIE DANS LA LUTTE CONTRE LES CYBERMENACES

A. L'EXPÉRIENCE CYBER DE L'ESTONIE : CONTEXTE ET INFRASTRUCTURES CLÉS

19. Depuis les années 1990, l'Estonie est devenue un leader mondial dans le développement de solutions en ligne et la construction d'une société numérique. Après que le pays a retrouvé son indépendance en 1991, les autorités ont promu les technologies de l'information et de la communication en tant que moteur de croissance sociale et économique et d'efficacité administrative. Aujourd'hui, la plupart des services publics sont disponibles en ligne grâce à l'infrastructure numérique estonienne. L'Estonie est même devenue en 2015 le premier pays au monde à introduire le vote électronique pour les élections. La manière dont le public estonien a adopté le vote électronique illustre le succès de la numérisation de la société estonienne : en 2005, 1,9 % des électeurs utilisaient des moyens numériques pour voter ; pour les élections parlementaires estoniennes de 2019, le pourcentage d'électeurs utilisant des moyens numériques a atteint 43 %.

20. Le succès remarquable de l'Estonie dans le développement d'une société numérique impose à l'État des responsabilités croissantes pour assurer la sécurité de tous les services en ligne. Un succès qui a également accru le risque de cyberattaques contre le pays et augmenté leur impact potentiel. La plus notable de ces attaques a eu lieu en 2007 lorsque, comme nous l'avons vu plus haut, l'Estonie a été confrontée à la première campagne coordonnée connue de cyberattaques visant un État-nation.

21. À l'époque, de multiples entités étaient visées en Estonie, notamment des banques, des chaînes de médias, des sites internet gouvernementaux et des sites de partis politiques. Cette attaque a conduit l'Estonie à mieux conceptualiser et à renforcer la cybersécurité au niveau national. L'année suivante, le pays a adopté sa première stratégie nationale en matière de cybersécurité. L'incident a également placé les cybermenaces au premier rang des préoccupations d'organisations internationales telles que l'OTAN et a conduit à la création du centre d'excellence pour la cyberdéfense en coopération (CCDCOE) de l'OTAN à Tallinn.

22. Un deuxième incident a poussé l'Estonie à intensifier ses efforts en matière de cybersécurité. En 2017, un chercheur de l'université Masaryk en République tchèque a découvert une faille de sécurité dans les puces électroniques des cartes d'identité électroniques estoniennes, utilisées par les citoyens et les résidents pour accéder à la plupart des services publics. La faille a affecté environ 800 000 cartes émises depuis 2014, les rendant théoriquement vulnérables. En réponse, l'Estonie a suspendu les certificats des cartes d'identité électroniques concernées et a renouvelé 94 % de toutes les cartes d'identité électroniques existantes. La découverte de cette faille et la réaction de l'Estonie ont souligné l'importance du partage d'informations et de la coopération internationale pour remédier aux vulnérabilités numériques et contrer les cybermenaces.

23. Aujourd'hui, le système national de services en ligne de l'Estonie est un organisme complexe en constante évolution. La plateforme fournie par le gouvernement fonctionne selon une architecture sécurisée et permet aux agences gouvernementales, aux entreprises et aux citoyens d'accéder au même environnement d'échange de données. L'épine dorsale de l' « e-société » estonienne est constituée de deux éléments : les cartes d'identité électroniques susmentionnées et le X-Road. Les cartes d'identité électroniques permettent aux résidents de prouver leur identité lorsqu'ils voyagent, se connectent à des comptes bancaires, fournissent des signatures numériques, votent en ligne, vérifient des dossiers médicaux, soumettent des demandes de remboursement d'impôts, utilisent des ordonnances électroniques, etc. Le système X-Road est un logiciel sécurisé de partage d'informations et de données qui assure

l'interopérabilité entre les différentes organisations et systèmes d'information qui fournissent eux-mêmes environ 3 000 services en ligne aux citoyens estoniens. Outre ces deux caractéristiques essentielles, d'autres éléments viennent compléter l'approche nationale en matière de cybersécurité : l'élaboration de politiques, l'éducation, la recherche, les systèmes de certification, les normes, la gestion de crise, la prévention de la cybercriminalité et les opérations militaires jouent tous un rôle dans la prévention et la réponse aux cybermenaces.

24. L'Estonie a développé une structure organisationnelle complète et solide en matière de cybersécurité. La responsabilité de la coordination générale de la politique de cybersécurité incombe au ministère des affaires économiques et des communications. Au sein du ministère, l'autorité estonienne des systèmes d'information est chargée du développement, de l'administration et de la protection des systèmes d'information de l'État. Elle répond également aux incidents de cybersécurité par l'intermédiaire de son équipe d'intervention en cas d'urgence informatique. Le ministère de la défense est chargé de la cyberdéfense dans le domaine de la défense nationale et supervise le travail des forces de défense estoniennes et de la Ligue de défense estonienne dans ce domaine. Le ministère de l'intérieur et le service de sécurité intérieure jouent également un rôle dans la prévention, la lutte et la réponse aux cyberattaques. Une entité inter-agences, le Conseil de cybersécurité du comité de sécurité du gouvernement, assure une coordination efficace entre ces différents organes gouvernementaux et supervise la mise en œuvre de la stratégie nationale de cybersécurité.

B. CYBERDÉFIS ACTUELS ET FUTURS

25. Les cybermenaces représentent un défi croissant et de plus en plus complexe en matière de sécurité. En Estonie, au cours des trois dernières années, le nombre de cyberincidents signalés à l'Autorité des systèmes d'information a augmenté. Dans le même temps, cependant, le nombre de ces incidents ayant eu un impact sur la sécurité n'a pas augmenté.

26. Les cybermenaces peuvent prendre de nombreuses formes, ce qui les rend difficiles à contrer. La plupart sont liées à des réseaux robotisés (bots ou botnets), qui compromettent de nombreux appareils, tels que des ordinateurs ou des smartphones, connectés à l'internet et qui sont contrôlés par un tiers. Les bots sont principalement utilisés par des acteurs malveillants pour mener des attaques par déni de service distribué ou pour subtiliser des données. Ils peuvent causer des dommages considérables. Ces dernières années, on a également constaté une augmentation des attaques par hameçonnage - des tentatives frauduleuses de collecte d'informations personnelles ou sensibles telles que les détails de paiement et les mots de passe. La généralisation du télétravail lors de la pandémie de Covid-19 a conduit à une augmentation notable de ces attaques en 2020-2021.

27. Au niveau mondial, le nombre d'acteurs impliqués dans des cyberattaques est à la hausse. La plupart sont menées par des individus et des groupes aux motivations financières, et peuvent donc être classées dans la catégorie cybercriminalité. D'autres proviennent d'acteurs étatiques, la Russie, la Corée du Nord et la Chine étant les sources suspectes les plus fréquemment citées.

28. Au cours de la dernière décennie, les cyberattaques sont devenues de plus en plus sophistiquées, et de ce fait, de plus en plus complexe à combattre. Même des pays qui sont bien préparés et dotés de capacités avancées peuvent être touchés. À titre d'exemple, la complexité de la cyberattaque de SolarWinds en 2020 a affecté de nombreuses agences d'État, départements, services de sécurité et entreprises aux États-Unis. On ne connait toujours pas la quantité d'informations qui ont été acquises par l'attaquant au cours de

l'incident. L'un des principaux problèmes est que les attaques sont rarement découvertes à temps : le délai moyen de découverte d'un cyberincident est de 200 jours, et dans le cas de SolarWinds, il était de près d'un an. La protection des systèmes d'information représente ainsi un défi important, car les attaquants ne doivent trouver qu'un seul moyen d'entrer dans les systèmes, alors que les défendre nécessite une protection de tous les points d'entrée possibles.

29. Les efforts pour contrer les cyberattaques se situent à plusieurs niveaux, notamment l'éducation, les mesures de sécurité, les approches de l'ensemble de la société et les solutions technologiques spécifiques telles que l'authentification à plusieurs niveaux et la gestion efficace des systèmes de données. Il reste encore de nombreux efforts à déployer au niveau national aux moyens de cadres juridiques et politiques solides. La coopération internationale est toutefois également cruciale.

30. Lorsque la responsabilité d'un État a été établie, le droit international offre plusieurs options possibles en réponse à une cyberattaque. Des contre-mesures peuvent être prises de manière concrète, mais celles-ci doivent rester proportionnelles et avoir pour objectif principal de stopper cette attaque. Il est cependant incontestablement difficile de lutter efficacement contre une cyberattaque. D'un point de vue académique, les progrès sont manifestes et les pays se montrent plus ouverts à la discussion sur les aspects juridiques et techniques de l'attribution de l'attaque et sur le partage de méthodes qui leur ont permis d'y faire face. L'attribution représente néanmoins une question politique, et la question de la gestion de la réponse à opposer face à une attaque fait l'objet de nombreux débats.

31. La confiance qui est nécessaire dans la technologie et ses fournisseurs pose un autre défi contemporain. Une inspection technique individuelle de l'ensemble des équipements et des logiciels est tout bonnement impossible et c'est pourquoi les pays qui dépendent fortement des solutions numériques et cybernétiques se doivent d'élaborer et de mettre en œuvre des critères rigoureux pour garder une certaine confiance dans les fournisseurs de technologie. Le rôle des fournisseurs de services sur le cloud soulève des préoccupations supplémentaires, surtout lorsqu'ils sont situés dans un pays tiers, notamment concernant la confidentialité (l'utilisation de nouveaux services sur le cloud nécessite de révéler des informations aux opérateurs de systèmes), la disponibilité des données (les informations stockées dans des centres de données peuvent pâtir d'un incident physique et/ou cybernétique) et l'intégrité des données (il est nécessaire de s'assurer que les données ne sont pas modifiées par le fournisseur de services ou partagées avec des tiers).

C. CENTRE D'EXCELLENCE POUR LA CYBERDÉFENSE EN COOPÉRATION DE L'OTAN

32. En 2004, l'Estonie a proposé la création d'un centre d'excellence de l'OTAN axé sur la cyberdéfense. Le CCD CoE de l'OTAN a été créé en 2008, après que les cyberattaques menées en 2007 contre l'Estonie ont mis en évidence la nécessité d'un partage accru des informations et d'une plus grande coopération entre les membres de l'OTAN et les pays partenaires.

33. Le centre rassemble des pays partageant la même optique et s'efforçant de créer un cyberespace plus sûr ainsi que de renforcer la résilience face aux menaces dans le domaine numérique. Vingt-neuf nations membres et partenaires ont désormais rejoint le CCD CoE, et cinq autres pays sont en passe de le faire.

34. Le CCD CoE, qui ne fait pas partie de la structure de commandement de l'OTAN, mène les activités suivantes :

- Recherche : le CCD CoE produit le *Manuel de Tallinn*, une étude académique qui analyse comment les traités de droit international existants s'appliquent dans le cyberespace. Une étude de suivi, le *Manuel de Tallinn 3.0*, a récemment été lancée pour tenir compte des dernières évolutions.

- Formation : le CCD CoE propose plus de 20 modules de cours sur des sujets tels que la cybersécurité des cadres stratégiques, le droit international, la planification opérationnelle, ainsi que plusieurs cours techniques.

- Exercices : À la mi-avril 2021, le CCD CoE a organisé son exercice annuel *Locked Shields*, qui est devenu le plus grand exercice au monde de cyberdéfense à tir réel avec plus de 30 nations participantes. L'exercice repose sur la construction d'ensembles d'objectifs réalistes comportant des cybercomposants essentiels tels que des centrales électriques, des réseaux électriques, des systèmes de défense aérienne et des liaisons par satellite. Ainsi, les équipes de défense acquièrent une expérience complète sur la manière de défendre leurs nations et leurs systèmes vitaux en cas de cyberattaque majeure. L'exercice *Locked Shields* favorise également la coopération en réunissant des représentants militaires, civils, universitaires, gouvernementaux et industriels.

IV. ASSURER LA TRANSFORMATION NUMÉRIQUE DE LA SOCIÉTÉ ESTONIENNE

35. La plupart des services publics étant disponibles en ligne en Estonie, la protection des données est primordiale pour le pays. De grandes quantités d'informations personnelles et de données sur les citoyens estoniens doivent pouvoir être stockées en toute sécurité. En outre, étant donné que les personnes et les entreprises non basées en Estonie ont la possibilité de devenir e-résident dans le pays, les autorités doivent également protéger ces données étrangères.

36. L'Estonie a donc développé une infrastructure numérique à la fois vaste et sûre, mais aussi flexible et efficace. Comme mentionné précédemment, le logiciel X-Road est au cœur de cette infrastructure. Il est utilisé pour échanger des données en toute sécurité entre différents services. Il fonctionne selon le principe de l'unicité, ce qui signifie qu'une seule agence peut demander un certain type de données à un utilisateur. Ainsi, si un serveur est piraté, un seul type d'information sera compromis. Cette compartimentation du réseau intégré rend ce dernier plus résilient aux cybermenaces.

37. Cette approche ne rend pas seulement le logiciel X-road plus sûr, elle le rend également plus convivial. Les citoyens n'ont qu'à saisir une seule fois les informations dans le système, comme un changement d'adresse, pour que toutes les agences et organisations concernées soient informées. La convivialité du système et l'omniprésence des services en ligne ont entraîné une forte adhésion des Estoniens, qui, par exemple, remplissent 96 % de leurs déclarations fiscales en ligne.

38. Le développement des services numériques a sensibilisé la population à l'importance de la protection des données. Les autorités ont dès lors pris des mesures pour assurer la transparence dans la manière dont les informations et les données personnelles des citoyens sont utilisées. Plus spécifiquement, le logiciel X-road intègre des mesures de confiance sous la forme d'un traqueur de données grâce auquel les citoyens peuvent connaître l'autorité

gouvernementale qui a accédé à des données personnelles spécifiques les concernant dans le système et la raison de cette consultation. Les Estoniens ont ainsi le sentiment d'être propriétaires de leurs données et les autorités font preuve de responsabilité et de transparence.

39. Pour assurer la continuité des services publics numériques en cas de choc majeur affectant l'Estonie, tel qu'une cyberattaque de grande ampleur, une catastrophe naturelle ou une attaque classique contre un centre de données, le pays a créé en 2017 une ambassade de données au Luxembourg. Il s’agit du premier pays au monde à ouvrir ce type ambassade. L'e-ambassade sert de site de secours à l'extérieur des frontières de l'Estonie, où sont stockées des copies des données les plus critiques et les plus confidentielles des Estoniens. Ce site vient compléter les installations de stockage de données de secours déjà existantes sur le territoire estonien.