ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION DES SCIENCES ET DES TECHNOLOGIES (STC)

L'OTAN ET LE CYBERESPACE : RENFORCER LA SÉCURITÉ ET LA DÉFENSE, STABILISER LA DISSUASION

Rapport général

Susan DAVIS (États-Unis)
Rapporteure générale

148 STC 19 F rév. 1 fin | Original : anglais | 13 octobre 2019

TABLE DES MATIÈRES

I. INTRODUCTION 1

II. LES CYBERATTAQUES EN CONTEXTE 2
A. LES CYBERATTAQUES ET AUTRES CYBEROPÉRATIONS MALVEILLANTES 2
B. LES RISQUES DE CYBERATTAQUES EN TEMPS DE PAIX 3
C. LES CYBERATTAQUES DANS LE CONTEXTE D'OPÉRATIONS MILITAIRES, DE CRISES ET DE CONFLITS ARMÉS 5

III. LA CYBERPOLITIQUE DE L'OTAN 6
A. LA CYBERSTRATÉGIE GÉNÉRALE DE L'OTAN 6
B. LE DÉVELOPPEMENT DES CYBERCAPACITÉS DES ALLIÉS 9
C. L'INTÉGRATION DES CYBERCAPACITÉS DANS LA PLANIFICATION OTAN 10
D. LA COOPÉRATION CONCRÈTE À L'OTAN 11
E. LES PARTENARIATS DE L'OTAN EN MATIÈRE DE CYBERDÉFENSE 12

IV. CONCLUSION 14

BIBLIOGRAPHIE SÉLECTIVE 17

I. INTRODUCTION

1. Alors que chaque sphère de la société devient de plus en plus connectée, les cybermenaces enregistrent une hausse spectaculaire. Chacun – du particulier à la communauté internationale – doit réfléchir à la façon de faire face à ces menaces chaque jour toujours plus sérieuses. L'Alliance atlantique n'y échappe pas. L'OTAN enregistre chaque jour nombre de cyberévénements suspects sur les réseaux qui lui appartiennent ou qu'elle exploite, sans parler de l'augmentation considérable d'intrusions sur les réseaux officiels et les infrastructures critiques des pays membres et partenaires de l'Alliance (Stoltenberg, 2019).

2. Il n'est donc pas surprenant que la sécurité, la défense et la dissuasion dans le cyberespace aient pris un caractère d'urgence pour l'OTAN et l'Assemblée parlementaire de l'OTAN (AP-OTAN). Ces questions figurent parmi les priorités de la commission des sciences et des technologies (STC) lors de ses réunions semestrielles et de ses visites exploratoires régulières, à l'instar des visites effectuées à Singapour et au Royaume-Uni en 2019. Ces dernières années, la STC a également examiné de façon approfondie certains aspects relatifs au cyberespace (voir encadré 1).

3. Ce rapport général ne peut raisonnablement aborder tous les types de cybermenaces auxquelles sont confrontés les membres de l'Alliance. Il se concentre donc sur celles qui touchent à la raison d'être de l'OTAN, à savoir les cyberattaques qui menacent l'intégrité territoriale, l'indépendance politique ou la sécurité nationale d'un Allié, et qui peuvent amener les membres de l'Alliance à invoquer la clause de défense collective, prévue à l'article 5 du traité de Washington. La lutte contre ces menaces se trouve au cœur de la mission de l'OTAN.

4. L'Alliance a tout d'abord reconnu publiquement la nécessité de renforcer la cybersécurité et la cyberdéfense lors du sommet de Prague en 2002. En 2008, l'OTAN a adopté sa première politique en matière de cyberdéfense. Toutefois, le véritable tournant s'est produit en 2014, lors du sommet du pays de Galles, lorsque l'Alliance a adopté sa politique de cyberdéfense renforcée. Parmi d'autres décisions clés, les responsables de l'OTAN ont explicitement indiqué qu'une cyberattaque pourrait entraîner l'invocation de l'article 5. Pour la première fois, les dirigeants des membres de l'Alliance ont indiqué clairement que « les cyberattaques peuvent atteindre un seuil susceptible de menacer la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique » (OTAN, 2014).

ENCADRÉ 1 : RÉCENTS RAPPORTS CONNEXES DE LA STC

- *Cyberespace et sécurité euro-atlantique*
- *L'internet des objets : promesses et dangers d'une technologie de rupture*
- *L'ingérence de la Russie dans les élections et les référendums des pays de l'Alliance*
- *Transactions secrètes : l'usage des messageries cryptées, du* dark web *et des cryptomonnaies par les terroristes*

5. Depuis le sommet du pays de Galles, l'OTAN et les Alliés ont clairement inclus la sécurité, la défense et la dissuasion dans le cyberespace parmi les tâches fondamentales de l'OTAN, et pris des dispositions pour que cela devienne une réalité. Aujourd'hui, tout adversaire potentiel doit savoir qu'une cyberattaque causant suffisamment de dommage à un Allié sera considérée comme une attaque armée à l'encontre de tous les Alliés, lesquels invoqueront l'article 5 pour se défendre collectivement. Lors du sommet de l'OTAN à Bruxelles en 2018, les dirigeants des membres de l'Alliance ont une fois de plus réitéré leur engagement : « Tout en réaffirmant le mandat défensif de l'OTAN, nous sommes déterminés à employer toute la gamme des capacités, y compris cyber, pour assurer la dissuasion et la défense et ainsi lutter contre l'éventail complet des cybermenaces, notamment celles qui sont exercées dans le cadre d'une campagne hybride » (OTAN, 2018a).

6. Ce rapport n'a pas pour but de donner un compte rendu exhaustif de l'ensemble des politiques, activités et discussions qui sont engagées dans les pays de l'Alliance et à l'OTAN au regard de la sécurité, la défense et la dissuasion dans le cyberespace. Son objectif est plutôt de présenter :

- le contexte des cybermenaces auxquelles est confrontée l'Alliance ;
- un aperçu des stratégies, politiques et activités actuelles de l'OTAN ayant trait au cyberespace ;
- des recommandations politiques concernant le renforcement de la cybersécurité, la cyberdéfense et la cyberdissuasion de l'OTAN.

7. La version finale de ce rapport, tel qu'amendé, a été adoptée lors de la 65e session annuelle de l'AP-OTAN en 2019. Ses recommandations de politique générale sont également reprises dans la résolution *Le renforcement de la cybersécurité, la cyberdéfense et la cyberdissuasion de l'OTAN*, également adoptée lors de cette même session.

II. LES CYBERATTAQUES EN CONTEXTE

8. Pour engager une discussion argumentée sur les cyberpolitiques menées par l'OTAN, il est indispensable de comprendre comment les cyberattaques s'inscrivent dans le paysage actuel des cybermenaces.

A. LES CYBERATTAQUES ET AUTRES CYBEROPÉRATIONS MALVEILLANTES

9. Le terme « cyberattaque » est malheureusement souvent employé à tort et à travers dans le débat public. Pour comprendre le paysage actuel des cybermenaces et concevoir des stratégies et des politiques efficaces en la matière, il est essentiel d'établir une distinction claire entre les cyberattaques et les autres types de cyberopérations malveillantes.

10. Il n'existe aucune définition universelle de ce qu'est une « cyberattaque », mais la définition proposée par le département de la défense (DoD) des États-Unis est un bon point de départ. Les **cyberattaques** peuvent être comprises comme « des actions menées dans le cyberespace qui produisent d'importants effets de déni dans cet espace (dégradation, interruption ou destruction), ou une manipulation qui produit un déni se manifestant dans un domaine physique » (US DoD, 2019). Le département définit d'autre part la **cyberexploitation** (qui inclut le cyberespionnage) comme l'ensemble des actions menées dans le cyberespace « pour acquérir des renseignements, manipuler, recueillir des informations ou exécuter d'autres actions de facilitation », ainsi que les **opérations d'information commises à l'aide d'internet** comme des actions visant à « influencer, déstabiliser, altérer ou usurper la prise de décisions des adversaires, réels ou potentiels ». Enfin, les **cyberinfractions** englobent toutes les activités criminelles commises via internet, les réseaux informatiques ou un système d'information.

11. Les **cyberattaques menées ou parrainées par des États** constituent la menace la plus importante pour l'Alliance car elles peuvent produire dans le cyberespace ou dans le domaine physique des effets militaires d'un niveau suffisant pour conduire à l'invocation par l'Alliance de l'article 5. Les États ou leurs intermédiaires ne sont pas les seuls à être en mesure de mener des cyberattaques. Des codes malveillants (voir l'encadré 2) sont amplement disponibles en ligne et les pirates informatiques peuvent en développer d'autres. Néanmoins, la planification et l'exécution des cyberattaques les plus dévastatrices nécessitent des connaissances, des compétences et des aptitudes très pointues, ainsi que des ressources considérables sur le plan financier et organisationnel (Slayton, 2017 ; Davis, 2014). À l'heure actuelle, seuls les États et leurs intermédiaires sont susceptibles de pouvoir atteindre ce seuil de ressources. Ils sont donc l'objet central de ce rapport. Bien évidemment, les Alliés doivent rester vigilants quant aux cyberattaques émanant de groupes terroristes. Pour autant, la cybersécurité et la cyberdéfense déployées par l'OTAN demeurent primordiales pour déjouer de telles attaques (les actions de dissuasion à l'encontre d'acteurs non étatiques étant très difficiles à mener, surtout dans le cyberespace).

12. Le fait que ce rapport mette l'accent sur les cyberattaques ne signifie pas que **d'autres cyberopérations malveillantes** ne représentent pas de gros risques pour l'OTAN et les membres de l'Alliance, ni que les forces armées ne jouent pas un rôle pour y faire face. Dans son rapport général 2018, la rapporteure expliquait comment les opérations d'information commises à l'aide d'internet contre des systèmes électoraux constituent une atteinte à la sécurité des membres de l'Alliance, comment elles font partie d'une menace hybride de plus grande ampleur ciblant l'OTAN, et comment les Alliés pourraient agir pour y faire face. Les services de renseignement des membres de l'Alliance – entre autres – mènent par ailleurs une lutte constante contre le cyberespionnage. D'autre part, il peut s'avérer plus facile pour des malfaiteurs d'accéder au siège de l'OTAN en passant par le cyberespace qu'en utilisant des modes d'attaque plus classiques. Dans la pratique, les frontières entre les différents types d'opérations malveillantes sont souvent floues. Par ailleurs, un nombre croissant d'Alliés sont conscients des risques stratégiques à long terme que représentent des cybercampagnes répétées composées d'un certain nombre de cyberopérations, toutes situées en dessous du seuil du conflit armé.

ENCADRÉ 2 : ÉTAPES D'UNE CYBEROPÉRATION RÉUSSIE

Une cyberopération s'effectue à l'aide d'un **code informatique malveillant**. Pour réussir, le malfaiteur doit trouver une vulnérabilité, se frayer un accès et déposer une charge (Lin, 2010).
Premièrement, le malfaiteur doit exploiter une *vulnérabilité* – un défaut ou une anomalie – dans le réseau qu'il a pris pour cible.
Deuxièmement, il doit se frayer un *accès* au réseau ciblé, que ce soit à distance, par l'intervention consciente ou inconsciente d'un initié, à l'aide d'une opération d'infiltration ou via la chaîne d'approvisionnement.
Troisièmement, le malfaiteur doit déposer une *charge* qui va exécuter l'action voulue dans le réseau visé.

Exception :
Les attaques par déni de service distribué ne reposent pas sur une défaillance du réseau visé, mais consistent à submerger le réseau avec un nombre ingérable de sollicitations.

B. LES RISQUES DE CYBERATTAQUES EN TEMPS DE PAIX

13. Certains observateurs et experts ont émis la crainte que les États ou leurs intermédiaires ne puissent commettre, en temps de paix, des **cyberattaques de grande ampleur sous le couvert de l'anonymat** en ciblant des réseaux militaires ou des infrastructures critiques civiles. Il est certain que de telles attaques ne pourront jamais être exclues, et que les stratégies et les politiques des Alliés et de l'OTAN doivent en tenir compte. Cela dit, le risque d'une attaque surprise de grande ampleur est moins grand que ne le laissent entendre les articles annonçant un « cyber 11 septembre » ou un « cyber *Pearl Harbor* ».

14. Il est possible toutefois que les attaquants essaient de brouiller les pistes en utilisant des réseaux tiers et qu'ils réussissent à commettre une attaque surprise de grande ampleur sans être inquiétés. Attribuer une attaque à un État, même lorsque les pistes remontent jusqu'à un pays en particulier, peut s'avérer complexe. D'autant que l'attaquant est susceptible de lancer des fausses pistes pour pointer du doigt quelqu'un d'autre. L'attribution peut être également délicate sur le plan technique : Le défenseur doit notamment analyser toutes sortes de données techniques, comprendre les objectifs potentiels de l'attaquant, sa motivation et ses capacités ; enfin, il doit traiter des renseignements provenant d'une multitude de sources – tout cela dans un délai limité où il est important de réagir (Davis et al., 2017). Le **problème de l'attribution** des attaques occupe par conséquent une grande place dans les débats sur la cyberpolitique.

15. Néanmoins, ces dernières années, les pouvoirs publics, les sociétés privées et les organismes de recherche ont accru leur **capacité à trouver**, avec un plus haut degré de fiabilité, **l'origine** des attaques. Les outils de la police scientifique se sont améliorés, et des analystes – privés comme publics – ont constitué des bases de données et établi des schémas d'intervention caractéristiques des attaquants connus. Sur le plan technique, les cyberattaques vraiment nuisibles sont très complexes et font intervenir de nombreux éléments mobiles. Par conséquent, plus une cyberattaque est complexe et plus l'attaquant commettra des erreurs en cours de route, ce qui permettra aux experts de la police scientifique de remonter la piste (Lindsay, 2015). En vérité, un nombre croissant de cyberincidents malveillants ciblant des membres de l'Alliance et d'autres pays sont attribués à des États et leurs intermédiaires. Cette transparence sur les cyberincidents est de plus en plus collective, coordonnée dans le temps et sur le plan politique, et indépendante de l'ampleur, la nature ou l'impact des incidents (Giles et Hartmann, 2019). La rapporteure est favorable à la nouvelle politique de dénonciation sur la place publique des auteurs d'une attaque et encourage la poursuite des discussions au sein de l'OTAN.

16. Quand bien même les États et leurs intermédiaires sont assurés de conserver leur anonymat lorsqu'ils commettent des attaques, il n'existe pas vraiment de motif stratégique valable de mener une attaque surprise de grande ampleur. Les cyberattaques anonymes **ne se prêtent pas vraiment**, en l'occurrence, **à la coercition**. En effet, une coercition ne fonctionne que si la cible de l'attaque sait à qui elle doit se rendre ou faire des concessions. Comme le relève succinctement un analyste : « La coercition totalement anonyme est presque impossible car le fait de comprendre le pouvoir de nuire et de communiquer sur le sujet implique que quelqu'un cherche à faire du mal et qu'une cible cherche à éviter d'être touchée » (Lindsay, 2015). Par conséquent, lorsqu'un adversaire veut exercer une contrainte en utilisant ses capacités de cyberattaque, il ne peut s'en cacher puisque cela nuirait à son objectif. Comment une victime peut-elle céder à des exigences si elle ne sait pas qui en est à l'origine ? (Les cybermalfaiteurs*,* en revanche*,* tiennent à rester anonymes, par exemple, lorsqu'ils essaient d'extorquer de l'argent à leurs victimes).

17. L'anonymat fournit cependant d'importants avantages sur le plan **tactique ou opérationnel.** Les États pourraient avoir recours aux cyberattaques en temps de paix et dans des situations de crise pour exécuter des actions précises et limitées évitant de franchir le seuil de l'attaque armée (Lewis, 2018). En d'autres termes, les États resteront cantonnés aux opérations hybrides, dans la zone grise située à mi-chemin entre la guerre et la paix, où il n'existe pas de normes en matière comportementale (Lewis, 2018). Ils peuvent ainsi préparer le terrain en vue de mener de futures cyberattaques dans un contexte de crise ou de conflit armé.

18. Il est très difficile de se protéger contre des cyberattaques ponctuelles visant un objectif tactique ou opérationnel, si ce n'est en mettant en place de solides dispositifs de cybersécurité et de cyberdéfense. Or, le risque stratégique le plus important que courent les différents membres de l'Alliance et l'OTAN dans son ensemble provient des **cybercampagnes répétées**. Ces campagnes consistent pour un adversaire à mener un grand nombre de cyberopérations, de manière à produire un impact stratégique en affaiblissant progressivement la puissance d'un État (Nakasone, 2019). Les Alliés ont donc entrepris d'affiner leurs politiques pour lutter contre ces cybercampagnes. Les États-Unis ont, par exemple, profondément modifié leur cyberpolitique. Le ministère de la défense a ainsi adopté une cyberstratégie novatrice, de « réaction systématique ». Selon le général Paul M. Nakasone, qui est à la tête du cybercommandement des États-Unis, « dans le cyberespace, c'est l'usage des cybercapacités qui est important sur le plan stratégique […] Donc l'avantage est à ceux qui sont dans l'action permanente » (Nakasone, 2019). Dans le cadre de cette stratégie, l'armée américaine ne se contente pas d'adopter une posture défensive pour protéger ses réseaux et réagir lorsqu'ils sont attaqués, mais met également en place une « défense en avant » en essayant de « perturber ou de stopper à la source la cyberactivité malveillante » (US DoD, 2018). Cette stratégie repose sur le maintien d'un contact permanent avec les adversaires potentiels dans le monde entier – y compris sur leurs propres réseaux – dans le but d'imposer « une confrontation tactique et des coûts stratégiques aux adversaires en les obligeant à mobiliser des ressources pour leur défense et à réduire leurs attaques » (Cybercommandement des États-Unis, 2018).

Cette doctrine comprend aussi un important volet sur le partenariat avec d'autres acteurs, notamment des organismes publics non militaires et des entreprises privées triées sur le volet (Nakasone, 2019). Un autre aspect primordial pour les concepteurs de cette nouvelle stratégie est l'innovation permanente. Comme l'a déclaré le général Nakasone, « la supériorité dans le cyberespace est temporaire ; elle peut être vraie pendant un temps, mais elle n'est qu'éphémère » (Nakasone, 2019). Un vaste débat agite actuellement les milieux américains de la cyberpolitique concernant la façon de procéder pour mettre pleinement en œuvre cette stratégie de réaction systématique. La rapporteure générale encourage une amplification et une intensification des débats sur la manière d'aborder les cybercampagnes répétées au sein de l'Alliance, tout en ayant conscience qu'il existe de grandes différences entre les Alliés. Elle se félicite donc de la réunion tenue en mai 2019 entre les conseillers nationaux des questions de sécurité des pays alliés sur le thème de la lutte contre les menaces hybrides, qui a surtout porté sur la recherche de moyens d'accroître la connaissance situationnelle de l'OTAN grâce à l'amélioration du renseignement et de l'échange d'informations.

C. LES CYBERATTAQUES DANS LE CONTEXTE D'OPÉRATIONS MILITAIRES, DE CRISES ET DE CONFLITS ARMÉS

19. De la même façon qu'aucune guerre moderne ne peut être gagnée en utilisant un seul type de capacités militaires, les cyberattaques ne peuvent à elles seules permettre de gagner une guerre. En revanche, associées à d'autres opérations militaires, elles **peuvent produire d'importants résultats sur le plan militaire.** L'OTAN et de nombreuses autres forces armées considèrent le cyberespace comme un champ d'action militaire distinct et ont commencé à intégrer des cybercapacités offensives et défensives dans leur planification opérationnelle en prenant les dispositions suivantes :

- Développement des cybercapacités ;
- Combinaison d'options cyber avec d'autres types d'opérations ;
- Remise à plat des structures de commandement ;
- Conception de doctrines cyber en les intégrant à la doctrine générale ;
- Examen de la façon dont le droit national et international peut être appliqué aux cyberopérations.

20. Lors d'opérations militaires, les cybercapacités offensives peuvent être utilisées en appui à d'autres types de capacités (et vice versa). Contrairement aux opérations cinétiques traditionnelles, les cyberattaques comportent peu de risques de causer directement un grand nombre de victimes ou des dégâts matériels importants si elles sont effectuées de manière responsable. Les cybercapacités offensives peuvent, par exemple, permettre aux forces armées de **recueillir des renseignements** ou de **préparer le champ de bataille** en dégradant, déstabilisant ou détruisant des réseaux de commandement et de contrôle militaire ou des systèmes d'armes et de capteurs, entraînant un ralentissement de la prise de décisions ou un succès tactique (Lewis, 2016). Les réseaux militaires sont volontairement isolés des autres réseaux du même type, ainsi que des réseaux civils (Lewis, 2016). Tandis qu'ils réfléchissent à la manière d'intégrer des cyberopérations aux opérations militaires, les Alliés doivent faire très attention à éviter que les cyberattaques ne se propagent et touchent aussi les réseaux civils.

21. Lorsqu'il s'agit d'un conflit de longue durée, l'infrastructure critique **civile** peut devenir une cible pour un adversaire. Un attaquant peut chercher à mettre à mal les efforts de guerre du pays attaqué, par exemple en ciblant les installations de l'industrie de la défense ou les réseaux électriques utilisés par les forces armées. Dans des cas plus rares, il peut essayer de saper la confiance de la population. Traditionnellement, les attaques contre une infrastructure critique civile en temps de guerre ont peu d'effet sur le plan militaire et entraînent généralement un renforcement de la résistance et de la résilience de la population (Lewis, 2018). En fait, elles ne produisent pas le chaos politique généralisé ni les effets stratégiques que certains redoutent ou que d'autres espèrent peut-être. Il n'en reste pas moins que les forces de l'OTAN et des membres de l'Alliance doivent rester vigilantes et opposer un mélange approprié de sécurité, de défense et de dissuasion.

Le fait que l'OTAN et les Alliés mettent de nouveau l'accent sur la résilience – notamment les sept exigences de base en matière de résilience du secteur civil adoptées lors du sommet de Varsovie en 2016 (voir encadré 3) – est à cet égard capital.

ENCADRÉ 3 :
Les sept exigences de base de l'OTAN en matière de résilience du secteur civil (OTAN, 2018b)

1. Continuité des pouvoirs publics et des services publics essentiels ;
2. Approvisionnements énergétiques ;
3. Aptitude à gérer efficacement des mouvements incontrôlés de population ;
4. Ressources en vivres et en eau ;
5. Aptitude à gérer un grand nombre de victimes ;
6. Réseaux informatiques et de télécommunications ;
7. Systèmes de transport.

22. Les milieux politiques au sein de l'Alliance et ailleurs continuent de se demander quelle incidence ont les cyberattaques sur la **stabilité pendant les crises et les conflits armés**. Quels types de cyberattaques auraient un effet neutre, d'escalade ou de désescalade ? La réponse serait-elle différente selon le moment où ces attaques auraient lieu en période de crise ou de conflit armé ? Les réponses sont-elles très différentes selon les États ? Une cyberattaque n'est généralement pas considérée par les États comme une option viable pour lancer une première frappe préventive de neutralisation. En revanche, lors d'une crise ou avant le déclenchement d'un conflit, les États peuvent juger qu'il est très « coûteux d'arriver second » (Davis, 2014). Dans ce type de situation, l'une des parties « peut tout à fait être effrayée de ce qui se passera si l'autre attaque *et* peut-être être convaincue qu'il sera avantageux de frapper la première » (Davis, 2014). Dans ce cas, les risques d'escalade sont grands. Une autre difficulté de taille est la difficulté à **déterminer la finalité** d'une cyberintrusion (Lindsay, 2015). Lorsqu'un défenseur détecte une intrusion, il ne sait pas forcément si l'attaquant a l'intention de l'épier, de pratiquer la défense en avant, de s'immiscer dans la perspective de futures mesures défensives, ou de préparer une cyberattaque imminente ou future (Slayton, 2017). Il est extrêmement difficile d'évaluer les intentions dans le cyberespace ; dès lors, les États ont tendance à supposer le pire (Hennessey, 2017). Cela peut conduire à des erreurs de perception et à une escalade sans fin (Slayton, 2017). En résumé, la dynamique de l'escalade mérite que l'on s'y intéresse de beaucoup plus près. Pour l'heure, l'Alliance doit s'efforcer de réduire les risques d'escalade par une communication et un dialogue diplomatiques clairs, un haut degré de transparence sur les cyberpolitiques, l'examen de la dynamique de l'escalade au cours des exercices, ainsi que le soutien à l'élaboration de normes et l'adoption de mesures visant à renforcer la confiance.

III. LA CYBERPOLITIQUE DE L'OTAN

23. Au niveau politique, l'Alliance continue d'adapter ses politiques de sécurité, de défense et de dissuasion dans le cyberespace en actualisant régulièrement ses plans d'action à l'aide d'objectifs et de délais concrets. Cette section examine les aspects suivants :

- Les grandes stratégies de lutte contre les cyberattaques à l'encontre de l'OTAN ;
- Le développement des cybercapacités des Alliés ;
- L'intégration des cybercapacités dans la planification OTAN ;
- La coopération concrète à l'OTAN ;
- les cyberpartenariats de l'OTAN.

A. LA CYBERSTRATÉGIE GÉNÉRALE DE L'OTAN

24. À l'heure où les forces armées du monde entier – y compris de pays pouvant devenir des adversaires – se dotent de cybercapacités, l'OTAN et ses pays membres doivent concevoir des stratégies et des politiques pour lutter contre la menace de cyberattaques graves visant des États. Face à des cyberattaques, l'OTAN utilise globalement les mêmes stratégies générales que pour faire face à d'autres types d'attaques, à savoir la **dissuasion par interdiction** et la **dissuasion par représailles**. Les Alliés doivent cependant continuer à soutenir l'élaboration de normes

internationales et engager des débats approfondis pour déterminer si et de quelle façon la stratégie générale OTAN peut être complétée par d'autres stratégies, comme par exemple, la stratégie américaine de « réaction systématique » telle que décrite au préalable.

1. Des normes pour le cyberespace

25. Du fait des caractéristiques des codes malveillants du cyberespace, la maîtrise effective des armements, le désarmement et les mesures de non-prolifération sont très probablement inutilisables pour l'instant, principalement parce que les vérifications sont, semble-t-il, impossibles. En revanche, l'élaboration ultérieure de normes applicables au cyberespace pourrait devenir un axe important de soutien contre les cyberattaques. L'OTAN continue d'affirmer que le droit international s'applique aussi au cyberespace, en ce compris le droit humanitaire international et la Charte des Nations unies. Tel est également le message du rapport du groupe d'experts gouvernementaux des Nations unies sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale, publié en 2013 (UN GGE, 2013). L'Alliance atlantique s'est également félicitée « des travaux sur des normes internationales volontaires de comportement responsable des États et sur des mesures de confiance pour ce qui est du cyberespace » (OTAN, 2016b). Les Alliés ont également précisé avoir « tout à gagner d'un cyberespace fondé sur des normes, prévisible et sûr » (OTAN, 2018a). Pour autant, il n'est pas réaliste d'espérer que l'OTAN – qui est une Alliance de 29 pays souverains – puisse devenir le principal moteur de l'élaboration ultérieure de normes. Au contraire, chaque membre de l'Alliance doit continuer à pousser la communauté internationale dans cette direction et encourager d'autres États membres à faire de même.

2. La cybersécurité et la cyberdéfense

26. Les stratégies de dissuasion par interdiction ont pour but de « dissuader l'adversaire d'effectuer une action en lui présentant une capacité crédible l'empêchant d'obtenir des gains éventuels suffisants pour l'inciter à agir » (Davis, 2014). En d'autres termes, le défenseur doit donner l'impression que l'attaque sera vaine : l'attaquant va soit échouer, soit au minimum ne tirer aucun bénéfice d'une cyberattaque (Nye, 2017). Ce type de cyberdissuasion repose directement sur une cybersécurité et une cyberdéfense fortes, qui relèvent principalement de la responsabilité des pays, même si l'OTAN doit jouer – et joue – un rôle, comme le montrent les sous-sections suivantes (voir aussi l'encadré 4).

ENCADRÉ 4 :
Définitions de la cybersécurité et de la cyberdéfense

La cybersécurité a pour but « de prévenir l'accès non autorisé, l'exploitation ou la dégradation d'ordinateurs, de systèmes de communication électroniques et autres technologies de l'information […] ainsi que des données qu'ils contiennent » (US DoD, 2019).

La cyberdéfense recouvre les actions visant « à mettre en échec les menaces ayant enfreint ou étant sur le point d'enfreindre les dispositifs de protection du cyberespace » (US DoD, 2019).

27. En théorie, le concept de la **cybersécurité et de la cyberdéfense** est simple. Les défenseurs essaient de réduire les vulnérabilités, de bloquer les points d'accès et de diminuer au maximum l'impact des charges. La cybersécurité et la cyberdéfense incluent toute une série de dispositifs préventifs, passifs et actifs. Les défenseurs souhaitant protéger leurs réseaux doivent renforcer leurs capacités dans plusieurs domaines : identification de la menace ; protection du réseau ; détection de l'intrusion ; réactions aux attaques ; enfin, résilience et récupération (US NIST, s.d. ; voir l'encadré 5). Les attaquants hardis sont souvent très agiles et s'adaptent rapidement, déjouant ainsi les nouveaux dispositifs de cybersécurité ou de cyberdéfense. Par conséquent, les membres de l'Alliance se tournent souvent vers des dispositifs plus actifs. À titre d'exemple, le concept de cyberdéfense active mis au point par le Pentagone permet de synchroniser la protection de l'ensemble des réseaux de l'administration publique et des infrastructures critiques. Autrement dit, il ne protège pas uniquement les réseaux appartenant au département de la défense et exploités par lui. Un concept encore plus novateur est celui de la « défense en avant », adopté par exemple par les États-Unis en 2018. Il consiste pour les défenseurs à intervenir sur les réseaux de l'attaquant pour mener des opérations de renseignement ; tenter de déjouer des attaques en cours, voire planifiées ; réparer rapidement les dommages causés par les attaques ; enfin, dans les situations extrêmes, punir les attaquants (Hoffman et Levite, 2017 ; US DoD, 2018).

3. La dissuasion

28. Bien que les capacités de cybersécurité et de cyberdéfense continuent de s'améliorer, la plupart des experts estiment que l'avantage est aux attaquants, et que cette situation n'est pas près de changer. En disposant de suffisamment de temps, de compétences et de ressources, les attaquants peuvent commettre une cyberattaque en détectant les points faibles du système visé, en s'y frayant un accès et en déposant une charge. C'est la principale raison pour laquelle l'Alliance doit compléter sa dissuasion avec des stratégies de dissuasion par représailles. En d'autres termes, les Alliés doivent essayer de « prévenir les attaques en menaçant de faire subir des dommages inacceptables, de sorte que *dans les calculs coûts-avantages de l'attaquant*, la meilleure option ne soit pas d'attaquer » (Morgan, 2009 ; en italique dans la version originale). Certains experts considèrent en outre que l'avantage n'est pas forcément acquis pour les attaquants. À titre d'exemple, plus les cyberarmes sont sophistiquées, plus l'attaque a des chances d'être stoppée et des erreurs commises. Qui plus est, une raison majeure pour laquelle les attaquants ont eu jusqu'ici l'avantage pourrait être des défaillances persistantes au sein des organisations (Slayton, 2017).

29. L'OTAN fonde sa **politique de la cyberdissuasion** sur l'ambiguïté. Premièrement, le seuil permettant d'établir qu'une cyberattaque est d'une gravité telle qu'elle équivaut à une attaque armée n'est pas clairement défini. Deuxièmement, il n'existe pas à ce jour de définition opérationnelle de ce que serait une réponse collective si ce seuil était franchi. Cette politique de la cyberdissuasion présente plusieurs avantages. Si l'Alliance devait définir un seuil bien précis, l'adversaire comprendrait mieux comment faire pour ne pas le dépasser. Cela aurait pour effet de renforcer la dissuasion contre les menaces dépassant ce seuil, mais encouragerait l'attaquant à aller juste en dessous de celui-ci. Un certain degré d'ambiguïté est donc bénéfique car il peut faire redouter aux adversaires d'aller trop loin dans leurs cyberattaques. L'adversaire a toujours peur de franchir la ligne invisible et préfère donc avancer prudemment. Une posture de dissuasion similaire a, d'une certaine façon, bien fonctionné pendant la guerre froide.

ENCADRÉ 5 :
PROCÉDÉS POUR AMÉLIORER LA CYBERSÉCURITÉ ET LA CYBERDÉFENSE

- Mise en place de dispositifs de cybersécurité de base
- Amélioration de la connaissance de la situation
- Augmentation des échanges d'informations
- Installation de logiciels de détection et de surveillance plus élaborés
- Investissement dans la recherche et le développement de nouvelles technologies
- Formation de la main-d'œuvre, par exemple en matière d'hygiène informatique
- Incitation de la main-d'œuvre à respecter les règles
- Organisation de formations et d'exercices sur le cyberespace
- Organisation régulière de cyberaudits
- Création d'une « équipe rouge » en matière de cybersécurité et de cyberdéfense
- Conclusion d'accords de coopération et d'assistance
- Tromperie des éventuels attaquants (par exemple, mise en place de « pots de miel » sur les installations)
- Cryptage des fichiers sensibles
- Protection des parties sensibles du réseau

30. Cela dit, l'ambiguïté quant au seuil de gravité peut, en fait, conduire un adversaire suffisamment à l'aise avec la prise de risque à exploiter en permanence les « zones grises », à tester la détermination du défenseur et à mener des cyberattaques toujours plus téméraires. D'une certaine manière, la solution contre ces attaques ne peut être uniquement la dissuasion, mais plutôt la conception d'actions politiques claires contre les opérations hybrides. Les membres de l'Alliance continuent, individuellement et collectivement, de travailler à l'élaboration de solutions de ce type. Les États-Unis ont vu ici la nécessité de mettre en œuvre une stratégie novatrice, celle de la réaction systématique. La rapporteure encourage les Alliés à déterminer si et comment cette stratégie pourrait s'avérer plus efficace en étant mise en place collectivement.

31. La politique OTAN de l'ambiguïté s'étend également au type de représailles encourues en cas de cyberattaque. L'Alliance a indiqué clairement qu'elle ne limitait pas, pas plus qu'elle ne l'excluait, des représailles sous forme de cyberattaques similaires. Elle s'autorise au contraire à utiliser toute la gamme des capacités que possèdent les Alliés pour prévenir et combattre les cyberattaques. Là encore, cette méthode instille utilement un doute dans l'esprit de l'attaquant. Une explication plus

technique à la difficulté de limiter la riposte à des cyberattaques est qu'il est difficile de menacer de façon crédible les actifs de l'attaquant en procédant de la même façon que lui. Si un attaquant porte atteinte à une centrale électrique, l'OTAN aurait-elle des possibilités d'attaquer à son tour des centrales ou une infrastructure similaire de son adversaire ? Et en admettant qu'elle puisse le faire, le voudrait-elle puisqu'elle respecte, dans toutes ses activités, le principe de la proportionnalité et le droit international ? L'ambiguïté de l'OTAN concernant le type de représailles sert un objectif réaliste. Elle sème le doute dans l'esprit du futur attaquant et permet de disposer de plusieurs options pour organiser une riposte adaptée et personnalisée et rétablir la dissuasion.

32. Une situation de dissuasion stable se caractérise essentiellement par la **capacité à montrer** ses moyens de représailles et sa détermination à faire respecter la menace de la dissuasion. Or, cet affichage devient difficile lorsqu'il est question de cyberdissuasion. Les États peuvent difficilement faire montre des codes malveillants dont ils disposent lors d'une parade militaire ou d'une exposition sur la défense. Les États doivent donc trouver d'autres façons d'afficher leurs capacités et de résoudre des conflits imminents. Ainsi, la démonstration de leurs capacités dans des situations du monde réel rend généralement la menace de la dissuasion plus plausible (Nye, 2017). En fait, de nombreux experts considèrent que des cyberattaques récentes et de faible ampleur devraient être, tout au moins en partie, perçues comme des démonstrations (Lewis, 2018). Par ailleurs, afficher aux yeux d'un adversaire que l'on investit dans des cybercapacités peut « généralement aider à montrer sa détermination » (Lindsay, 2015). En d'autres termes, la transparence sur les dispositifs de cybersécurité et de cyberdéfense est également un élément de dissuasion. Bien que limités dans les possibilités qu'ils ont d'afficher leurs capacités en matière de cybersécurité et de cyberdéfense, l'OTAN et chacun de ses pays membres semblent faire des progrès. Dans le domaine public, l'OTAN doit donc être aussi transparente que possible concernant ses cybercapacités. Dans les domaines qui requièrent plus de discrétion, la communication avec des adversaires potentiels par des canaux confidentiels doit être aussi fréquente que possible.

B. LE DÉVELOPPEMENT DES CYBERCAPACITÉS DES ALLIÉS

33. Comme le stipule l'article 3 du traité de l'Atlantique Nord, chaque membre de l'Alliance a la responsabilité de maintenir et d'accroître sa capacité individuelle et collective de résistance à des cyberattaques. Au niveau de l'Alliance, cette responsabilité s'exerce dans le cadre du processus OTAN de planification de défense (NDPP). Ce plan prévoit en effet que chaque Allié fixe ses propres objectifs de planification, et que les autres membres de l'Alliance vérifient régulièrement si ce pays a atteint ses objectifs et rempli sa mission. Les premiers objectifs en matière de capacités de cyberdéfense ont été fixés en 2013. Ils concernent notamment la gouvernance de la cyberdéfense, les capacités de réaction des réseaux de l'OTAN, ainsi que les programmes de formation et d'entraînement (Robinson, 2017).

34. Lors du sommet de Varsovie en 2016, les Alliés ont convenu que l'amélioration des moyens de cyberdéfense des réseaux et des infrastructures nationaux était devenue un objectif prioritaire. Ils ont donc, pour compléter le processus normal du NDPP, pris un engagement en faveur de la cyberdéfense, celui d'accroître le développement des capacités. Dans le cadre de cet engagement, les États membres ont promis d'améliorer leur résilience et leur capacité de réaction dans le cyberespace, ainsi que de procéder à des auto-évaluations annuelles. Les membres de l'Alliance doivent donc poursuivre sept grands objectifs (OTAN, 2016a) :

I. améliorer tout l'éventail des moyens de défense de [leurs] infrastructures et de [leurs] réseaux nationaux ;
II. prévoir au niveau national des ressources adéquates pour le renforcement de [leurs] capacités de cyberdéfense ;
III. renforcer les interactions entre les acteurs nationaux compétents en matière de cyberdéfense afin d'approfondir la coopération et l'échange des meilleures pratiques ;
IV. améliorer [leur] compréhension des cybermenaces, notamment dans le cadre de la mise en commun des informations et des évaluations ;

V. améliorer les compétences et le niveau de connaissance, entre tous les acteurs de la défense au niveau national, depuis l'hygiène informatique de base jusqu'aux moyens de cyberdéfense les plus sophistiqués et les plus robustes ;
VI. promouvoir les formations, les entraînements et les exercices en matière de cyberdéfense à l'intention de [leurs] forces, et renforcer [leurs] établissements de formation, afin de développer la confiance et les connaissances dans l'ensemble de l'Alliance ;
VII. accélérer la mise en œuvre des engagements de cyberdéfense agréés, notamment pour les systèmes nationaux dont l'OTAN est tributaire.

C. L'INTÉGRATION DES CYBERCAPACITÉS DANS LA PLANIFICATION OTAN

35. Lors du sommet de Varsovie en 2016, l'Alliance a reconnu le cyberespace en tant que domaine opérationnel. Conformément à la mission défensive de l'OTAN, les Alliés ont donc reconnu que l'OTAN devait se défendre dans le cyberespace « aussi efficacement qu'elle le fait dans les airs, sur terre et en mer » (OTAN, 2016b). Cette reconnaissance permet à l'OTAN d'être mieux à même « d'assurer une protection et de mener des opérations dans tous ces domaines, ainsi que de préserver [sa] liberté d'action et de décision, en toutes circonstances » (OTAN, 2016b). Elle constitue également, de manière plus générale, un soutien à la politique de dissuasion et de défense de l'OTAN.

36. La reconnaissance du cyberespace en tant que domaine opérationnel reflète le changement d'optique de l'OTAN qui, considérant auparavant la cybersécurité et la cyberdéfense comme une tâche de sûreté de l'information, intègre aujourd'hui les cybercapacités dans sa tâche de sûreté de la mission (Shea, 2017). En d'autres termes, l'Alliance ne se consacre plus seulement à la protection des réseaux de l'OTAN ou à l'appui des efforts déployés par les pays pour renforcer leurs dispositifs de cybersécurité et cyberdéfense. En revanche, elle se concentre de plus en plus sur la manière d'intégrer les cybercapacités – y compris les effets cyber offensifs mis volontairement à disposition par les différents Alliés – dans les opérations et les missions de l'OTAN. La raison de ce changement d'optique est la nécessité d'encourager un développement homogène des capacités ainsi que la conception d'une stratégie claire sur la façon dont ces capacités peuvent être utilisées dans un contexte opérationnel (Robinson, 2017). Les cybercapacités, qui ont commencé à ajouter de la valeur aux opérations, procurent un nouvel ensemble d'outils et permettent à l'OTAN d'agir « à la vitesse de la pertinence » (Robinson, 2017). Comme dans d'autres domaines, l'OTAN a établi clairement que l'intégration des effets cyber devait s'accompagner d'un strict contrôle politique et du respect du droit international.

37. Depuis 2016, plusieurs Alliés ont confirmé leur volonté de mettre des effets cyber offensifs – mais aussi défensifs – à la disposition des opérations de l'OTAN ; c'est le cas de l'Allemagne, du Danemark, de l'Estonie, des États-Unis, de la Lituanie, de la Norvège, des Pays-Bas et du Royaume-Uni. Les effets cyber offensifs ne seront pas placés sous le commandement et le contrôle de l'OTAN, mais du pays allié contributeur, comme c'est le cas pour les forces spéciales nationales employées dans des opérations OTAN. La rapporteure encourage d'autres Alliés à en faire de même pour accroître la crédibilité globale de l'Alliance.

38. Les principes juridiques et politiques régissant l'intégration de ces capacités ont été définis en novembre 2017. En 2018, l'Alliance a approuvé une vision et une stratégie militaires pour le cyberespace en tant que domaine opérationnel, dans le but d'élaborer une doctrine à part entière pour le cyberespace d'ici la fin 2019. Dans la pratique, cela permettra une coopération plus étroite entre le commandant suprême des forces alliées en Europe (SACEUR), le Commandement allié Opérations et l'agence OTAN d'information et de communication (NCIA) (Shea, 2017).

39. Pour permettre à la structure de commandement de l'OTAN d'intégrer effectivement des cybercapacités, les Alliés ont également décidé d'installer à Mons (Belgique) un centre des cyberopérations (CyOC), qui sera pleinement opérationnel en 2023. Ce centre sera chargé de fournir

une meilleure connaissance de la situation, de coordonner les cyberactions et de centraliser la planification des aspects cyber des opérations et des missions (Brent, 2019).

D. LA COOPÉRATION CONCRÈTE À L'OTAN

40. L'OTAN se concentre avant tout sur la protection des réseaux appartenant à l'Organisation et exploités par elle. La coopération au sein de l'Alliance sur les questions cyber consiste également à accroître la cybersécurité et la cyberdéfense dans les pays alliés au moyen de l'amélioration des connaissances, la formation, l'entraînement, l'organisation d'exercices, l'échange d'informations et l'entraide.

41. Au sein de la structure OTAN, de nombreux organes politiques, militaires et techniques jouent un rôle clé au regard de la mise en œuvre des cyberpolitiques de l'Organisation, à savoir : le Bureau de consultation, commandement et contrôle (C3B), les autorités militaires de l'OTAN, la NCIA, le Commandement allié Opérations et le Commandement allié Transformation. Par ailleurs, d'autres entités de la famille OTAN au sens large œuvrent, dans le cadre de leurs missions respectives, pour le renforcement de la cyberdéfense et la cyberdissuasion au sein de l'Alliance. C'est le cas de l'école de l'OTAN à Oberammergau, du collège de défense de l'OTAN à Rome et du centre d'excellence pour la cyberdéfense en coopération (CCD COE) à Tallinn, homologué par l'OTAN.

42. Au fil des ans, les entités de l'OTAN et la famille OTAN au sens large ont conçu et mis en œuvre une multitude d'activités et de projets ayant trait au cyberespace. En donner la liste exhaustive dépasse le champ d'observation du présent rapport, mais en voici un échantillon représentatif :

- Intégration des cybermenaces dans l'exercice de gestion de crise de l'OTAN afin d'accroître la sensibilisation à ces questions dans les capitales des pays de l'Alliance, au siège de l'OTAN, au Commandement allié Opérations et au Commandement allié Transformation ;
- Création d'un cyberpolygone de l'OTAN – fourni et hébergé par l'Estonie – pour tester les capacités de cyberdéfense ;
- Organisation de plusieurs projets de défense intelligente : une plateforme d'échange d'informations sur les logiciels malveillants ; le développement d'une capacité de cyberdéfense multinationale et de défense intelligente ; un projet multinational de formation et d'entraînement sur la cyberdéfense.

43. La NCIA répond aux besoins de l'OTAN en matière de technologie et de communications et fournit des systèmes d'information et de communications. Elle satisfait également aux besoins de technologies de l'information du siège de l'OTAN, de sa structure de commandement et de ses agences. La NCIA joue donc un rôle central dans les domaines suivants : acquisition de technologie ; expérimentation ; interopérabilité ; conception et ingénierie de systèmes et d'architectures ; essais et support technique.

44. La NCIA gère par ailleurs la capacité OTAN de réaction aux incidents informatiques (NCIRC) à Mons. La NCIRC assure en continu la protection des réseaux appartenant à l'OTAN et exploités par elle sur plus de 65 sites, à tous les niveaux et quels que soient les réseaux (statiques, mobiles ou déployés). Cette capacité fournit également l'analyse des cybermenaces, parallèlement aux travaux de la cellule d'évaluation des cybermenaces. Une autre composante importante de la NCIRC est son équipe de réaction rapide (RRT), qui peut être déployée sur des sites OTAN, des théâtres d'opérations ainsi qu'en appui à un membre de l'Alliance après accord du Conseil de l'Atlantique Nord. La RRT se compose d'un noyau de six experts, et peut intervenir dans les 24h suivant un incident.

45. La NCIA renforce actuellement ses moyens de formation. Le Portugal accueillera, au troisième trimestre 2019, l'école OTAN des systèmes d'information et de communication et du cyberespace, qui dispensera aux membres du personnel civil et militaire une formation sur les systèmes

informatiques et cyber de pointe utilisés à l'OTAN. Cette école aura également des contacts avec les centres de formation des États membres, l'industrie et les milieux universitaires.

46. En février 2019, la NCIA a créé une nouvelle plateforme OTAN sur laquelle les experts en cyberdéfense de l'ensemble de l'Alliance peuvent partager les meilleures pratiques, échanger des informations et coopérer dans un espace protégé par chiffrement. Il s'agit de la première étape vers la création d'une plateforme collaborative de cybersécurité, annoncée en 2018.

47. Le CCD COE représente un autre atout important pour les Alliés en tant que source d'expertise reconnue. Il réunit actuellement 25 États membres et pays partenaires de l'OTAN. Les centres d'excellence homologués par l'OTAN ne font pas partie de la structure de commandement de l'Organisation ; ce sont des organismes militaires internationaux qui répondent aux besoins divers de l'Alliance. Leurs principaux domaines de travail sont la recherche cyber, la formation, l'entraînement et les exercices. Les produits peut-être les plus connus sont le Manuel de Tallinn sur le droit international applicable à la cyberguerre et le Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations.

48. Les cyberexercices occupent une place importante dans l'intensification de la cyberdéfense à l'OTAN. L'exercice *Cyber Coalition,* dirigé par le Commandement allié Transformation, attire plus de 700 participants représentant les pays membres et partenaires de l'OTAN, l'UE, les milieux universitaires et l'industrie. Cet exercice vise à accroître la coopération et la coordination entre les Alliés ainsi qu'à tester les procédures OTAN et nationales en matière d'échange d'informations, de connaissance de la situation et de prise de décision. L'édition 2018 de *Cyber Coalition* était consacrée plus spécialement à l'intégration des effets cyber souverains mis volontairement à disposition par les Alliés (Brent, 2019). Le CCD COE organise deux autres exercices importants. Le premier, *Locked Shields*, teste les compétences des experts en cyberdéfense dans un scénario d'affrontement entre une équipe rouge et une équipe bleue. Le second, *Crossed Swords*, permet aux participants (des experts provenant des États membres, des pays partenaires et de l'industrie) de protéger les réseaux et les systèmes informatiques contre des cyberattaques simulées ayant lieu en temps réel.

E. LES PARTENARIATS DE L'OTAN EN MATIÈRE DE CYBERDÉFENSE

49. Dans un monde de plus en plus interconnecté, l'existence d'un solide réseau de partenaires est extrêmement importante, et cela s'applique en particulier au domaine de la cybersécurité et la cyberdéfense. L'OTAN collabore donc avec un large éventail de partenaires : industrie, universités, pays partenaires et autres organisations internationales.

50. L'industrie joue à cet égard un rôle central, comme l'a appris une délégation de la STC lors d'une visite au Centre national de cybersécurité du Royaume-Uni en juin 2019. Elle peut fournir des solutions techniques et des innovations, investir massivement dans des produits de cybersécurité, et détenir des renseignements précis sur les cybermenaces. Elle possède en outre – ou gère – une part non négligeable des systèmes d'information alliés. Avec le cyberpartenariat OTAN-industrie (NICP), l'Alliance fournit un cadre dans lequel des entités OTAN et des experts nationaux collaborent avec des représentants de l'industrie (et des universités) des États membres. Le NICP vise à faciliter l'échange d'informations sur les cybermenaces et à améliorer la capacité des Alliés à détecter, prévenir et résoudre les cyberincidents. Ce partenariat couvre 12 domaines prioritaires, parmi lesquels : la gestion de la chaîne d'approvisionnement ; les pratiques exemplaires ; l'amélioration de la connaissance ; la formation, l'entraînement et les exercices ; enfin, l'innovation.

51. La coopération en matière de cybersécurité et de cyberdéfense est très souvent une composante essentielle de la collaboration de l'OTAN avec les pays partenaires. L'Organisation a noué des partenariats particulièrement étroits avec la Géorgie et l'Ukraine, qui incluent de vastes initiatives de coopération en matière de cyberdéfense. Dans le cadre du paquet substantiel OTAN-Géorgie, l'Alliance apporte son soutien aux cybercapacités du pays, à son interopérabilité et

à sa coopération avec les différents membres de l'Alliance. S'agissant de l'Ukraine, l'OTAN a établi avec elle en 2014 un fonds d'affectation spéciale pour la cyberdéfense. Ce fonds a pour but de mettre au point des capacités strictement défensives dans le domaine de l'intervention en cas de cyberincident, notamment la création de deux centres de gestion des incidents. L'Ukraine bénéficie en outre d'une formation de l'OTAN sur l'utilisation des technologies et des équipements liés à ce fonds. D'autres initiatives de coopération en matière de cyberdéfense ont également été lancées récemment avec des pays partenaires, notamment des accords avec la Finlande, la République de Moldova, la Jordanie et l'Iraq.

52. Si l'OTAN coopère avec l'Organisation pour la sécurité et la coopération en Europe (OSCE) et les Nations unies, c'est avec l'Union européenne qu'elle entretient le partenariat international le plus étroit. La coordination et la coopération en matière de cybersécurité et de cyberdéfense sont les principaux domaines du partenariat stratégique OTAN-UE. Ce cyberpartenariat a reçu un nouvel élan en 2016 lorsque le président du Conseil européen, le président de la Commission européenne et le secrétaire général de l'OTAN ont, dans une déclaration commune, décidé « d'étendre [leur] coordination dans le domaine de la cybersécurité et de la cyberdéfense, y compris dans le cadre de [leurs] missions et opérations, de [leurs] exercices, et en matière de formation et d'entraînement » (Tusk, Juncker et Stoltenberg, 2016).

53. L'OTAN et l'UE mettent actuellement en œuvre 74 propositions de coopération, dans lesquelles la cybersécurité et la cyberdéfense occupent une grande place. Les axes concrets d'intensification de la coopération OTAN-UE sont notamment les suivants :

- Intégration de la cyberdéfense dans la planification ;
- Promotion de la recherche et de l'innovation technologique dans le domaine cyber ;
- Échange des meilleures pratiques en matière de gestion de crise et d'intervention au niveau opérationnel ;
- Analyse des informations relatives aux menaces et aux logiciels malveillants ;
- Mise en évidence des possibles synergies, notamment entre la NCIRC et l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE), qui ont déjà signé un arrangement technique pour faciliter l'échange d'informations ;
- Renforcement de la coopération dans le domaine des entraînements et des exercices.

54. Un rapport de 2018 sur la mise en œuvre des diverses propositions de coopération OTAN-UE relevait des interactions et des échanges d'informations dynamiques et efficaces entre les fonctionnaires des deux organisations, notamment sur les sujets suivants : concepts et doctrines ; formations et entraînements existants ; indicateurs de menaces ; alertes et évaluations des menaces ; gestion de crise.

55. S'agissant des exercices, le personnel de l'UE spécialisé dans la cyberdéfense a participé pour la première fois à l'édition 2017 de *Cyber Coalition* et à l'édition 2018 de *Locked Shields.* En 2017, *l'exercice de gestion de crise de l'OTAN* et l'*exercice parallèle et coordonné* de l'UE ont eu lieu simultanément. Cela a permis aux deux organisations d'évaluer la compatibilité de leurs dispositifs de réaction aux crises, notamment en cas de menaces informatiques et hybrides. En novembre 2018, l'UE a en outre organisé un exercice de gestion de crise civilo-militaire en parallèle avec l'exercice de poste de commandement de l'OTAN ayant lieu dans le cadre de *Trident Juncture*.

56. De son côté, l'UE a reconnu la cybersécurité comme une constituante fondamentale de la sécurité communautaire globale et a intensifié son adaptation en conséquence, renforçant sensiblement la cyberrésilience de l'OTAN. Ainsi, l'UE peut désormais s'appuyer sur plusieurs entités importantes pour aller plus loin dans les mesures de cybersécurité (voir encadré 6).

ENCADRÉ 6 : PRINCIPALES ENTITÉS EUROPÉENNES DU DOMAINE DE LA CYBERSÉCURITÉ ET LA CYBERDÉFENSE

- Agence de l'UE chargée de la sécurité des réseaux et de l'information
- Équipe d'intervention en cas d'urgence informatique de l'UE
- Centre européen de lutte contre la cybercriminalité
- Agence européenne de défense
- Collège européen de sécurité et de défense

Par ailleurs, l'UE étant un organe de réglementation, ses initiatives peuvent faire sensiblement progresser la cybersécurité et la cyberdéfense des réseaux nationaux, y compris des infrastructures critiques. Les autres avancées politiques récentes les plus notables sont notamment les suivantes :

- Adoption de la directive sur la sécurité des réseaux et des systèmes d'information – premier ensemble de règles communautaires sur la cybersécurité –, dont le but est d'atteindre un haut niveau commun de sécurité pour les réseaux et les systèmes d'information de l'UE, afin de permettre le bon fonctionnement du marché intérieur ;
- Mise au point d'un cadre permettant une réponse conjointe de l'UE face aux actes de cybermalveillance : cette boîte à outils cyberdiplomatique offre toutes sortes d'instruments pour lutter contre les cybermenaces, comme l'imposition de sanctions ;
- Élaboration de deux projets axés sur le cyberespace dans le cadre de la nouvelle coopération structurée permanente de l'UE, à savoir : une plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques ; des équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité ;
- Renforcement de la mission de l'agence de l'UE chargée de la sécurité des réseaux et de l'information ; et
- Avancée politique concernant l'élaboration d'un cadre européen de certification de cybersécurité pour les services en ligne et les appareils grand public.

IV. CONCLUSION

57. S'ils se contentaient de lire les mauvaises nouvelles sur le cyberespace qui affluent dans les médias, les responsables politiques pourraient facilement perdre espoir. Or, dans ce rapport, l'analyse approfondie des stratégies, politiques et activités mises en œuvre par l'OTAN et les Alliés concernant le cyberespace montre que l'OTAN est en train de renforcer sa cybersécurité, sa cyberdéfense et sa cyberdissuasion dans toutes les directions. La nouvelle doctrine pour le cyberespace, qui doit être adoptée d'ici la fin 2019, sera une autre étape majeure.

58. Ces progrès ne doivent pas pour autant faire place à de la complaisance. L'OTAN doit rester très vigilante quant aux cyberattaques qui pourraient menacer l'intégrité territoriale, l'indépendance politique ou la sécurité de l'un de ses membres, et donc conduire les Alliés à invoquer l'article 5. Le texte de la résolution 459 de l'AP-OTAN adopté lors de la session annuelle présente les recommandations générales de l'Assemblée en matière de cyberpolitique. La commission a cependant également approuvé la série de recommandations ci-dessous. La rapporteure invite donc instamment les membres de cette commission à suivre de près, à l'aide de tous les instruments disponibles, les avancées qui seront faites sur les points en question.

Cybersécurité et cyberdéfense

59. Chaque membre de l'Alliance a la responsabilité de maintenir et d'accroître sa capacité individuelle et collective de résistance à des cyberattaques. Il doit donc, pour assumer cette responsabilité, respecter les engagements pris dans le cadre du processus OTAN de planification de défense ainsi que l'engagement en faveur de la cyberdéfense. Les Alliés et, le cas échéant, l'OTAN dans son ensemble, doivent donc redoubler leurs efforts concernant :

- le développement de cybercapacités ;
- les dépenses en matière de cyberdéfense ;
- l'adaptation des structures alliées et OTAN ;
- l'intégration des effets cyber dans les opérations militaires ;
- l'amélioration des cyberstratégies et des cyberpolitiques au niveau des pays et de l'OTAN ;
- la coopération et l'échange des meilleures pratiques ;
- la connaissance de la situation, l'échange d'informations et l'évaluation ;
- l'amélioration des compétences et du niveau de connaissance de tous les acteurs concernés des pays membres et de l'OTAN ;
- la promotion des formations, des entraînements et des exercices ;
- le renforcement des cyberpartenariats efficaces avec l'industrie, le monde universitaire, les pays partenaires (et notamment les pays candidats à l'OTAN) et d'autres organisations internationales, en particulier l'UE dans le cadre du partenariat stratégique OTAN-UE.

60. Les Alliés doivent en outre envisager sérieusement la mise à disposition, sur la base du volontariat, d'effets cyber offensifs et défensifs pour les opérations OTAN, si tel engagement n'a pas encore été pris.

Cyberdissuasion

61. L'Alliance doit continuer de compléter ses dispositifs de cybersécurité et de cyberdéfense avec des stratégies de cyberdissuasion. Elle doit continuer d'appliquer une politique de la cyberdissuasion fondée sur l'ambiguïté. Elle ne doit pas fixer de seuil permettant d'établir qu'une cyberattaque est d'une gravité telle qu'elle équivaut à une attaque armée, ni définir ce que serait une réponse collective si ce seuil était franchi.

62. Les Alliés et l'OTAN doivent continuer d'afficher leur détermination et leur crédibilité pour prévenir les cyberattaques. L'OTAN doit donc être aussi transparente que possible concernant ses cybercapacités. Dans les domaines qui requièrent de la discrétion, la communication avec des adversaires potentiels par des canaux confidentiels doit être aussi fréquente que possible.

63. L'Alliance doit continuer d'essayer de réduire les risques d'escalade par une communication et un dialogue diplomatiques clairs, un haut degré de transparence sur les cybercapacités et les politiques y afférentes, ainsi qu'apporter un soutien à l'élaboration de normes et l'adoption de mesures visant à renforcer la confiance dans le cyberespace.

Cybercampagnes répétées

64. L'Alliance doit reconnaître le risque stratégique à long terme que représentent les cybercampagnes répétées. L'OTAN et les Alliés doivent lutter contre ces cybercampagnes à l'aide d'une combinaison adaptée de mesures de sécurité, de défense et de dissuasion, y compris une préparation et une résilience accrues du secteur civil. Un débat plus approfondi doit avoir lieu au sein de l'Alliance sur le sujet des cybercampagnes répétées. Les Alliés doivent continuer à affiner leurs stratégies de lutte contre les menaces hybrides, notamment grâce à une meilleure connaissance de la situation rendue possible par l'amélioration de la collecte de renseignements et de l'échange d'informations et par d'autres moyens.

65. Dans la mesure du possible, les Alliés doivent dénoncer sur la place publique les auteurs de cyberopérations malveillantes, dans un délai réduit et – de préférence – de façon coordonnée. Ils doivent aussi engager un débat approfondi sur l'amélioration de la transparence au niveau de l'OTAN.

BIBLIOGRAPHIE SÉLECTIVE

Ce rapport s'appuie en outre largement sur des informations accessibles au public provenant de l'OTAN, d'agences OTAN, ainsi que des divers sites internet de l'Union européenne. Pour de plus amples renseignements, veuillez vous adresser au directeur de la commission des sciences et des technologies au secrétariat international de l'AP-OTAN.

Brent, Laura, "NATO's Role in Cyberspace", *NATO Review*, 2019

Davis II, John S. et al., *Stateless Attribution: Toward International Accountability in Cyberspace*, RAND Corporation, 2017

Davis, Paul K., "Deterrence, Influence, Cyber Attack, and Cyberwar", *New York University Journal of International Law and Politics*, vol. 47, no. 2, 2014

Giles, Keir and Hartmann, Kim, *"'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict"*, in: Minarik, Tomas et al. (eds), 2019 11th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications, 2019

Hennessey, Susan, "Deterring Cyberattacks: How to Reduce Vulnerability", *Foreign Affairs*, vol. 96, no. 6, 2017

Hoffman, Wyatt et Levite, Ariele E., *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, Carnegie Endowment for International Peace, 2017

Lewis, James A., "Cyberspace and Armed Forces: The rationale for Offensive Cyber Capabilities", *Strategic Insights*, Australian Strategic Policy Institute, 2016

Lewis, James A., "Deterrence in the Cyber Age", *Global Forecast 2015*, Center for Strategic and International Studies, 2014

Lewis, James A., *Rethinking Cybersecurity: Strategy, Mass Effect, and States*, Center for Strategic and International Studies, 2018

Lin, Herbert S, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law & Policy*, vol. 4, no. 63, 2010

Lindsay, Jon R., "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", *Journal of Cybersecurity*, vol. 1, no. 1, 2015

Morgan, Patrick M., *Deterrence Now*, Cambridge: Cambridge University Press, 2009

Nakasone, Paul M., "An Interview with Paul M. Nakasone", *Joint Forces Quarterly*, vol. 92, no. 1, 2019

OTAN, Déclaration du sommet de Bruxelles, 2018a

OTAN, Préparation du secteur civil, 2018b

OTAN, Engagement en faveur de la cyberdéfense, 2016a

OTAN, Déclaration du sommet du pays de Galles, 2014

OTAN, Communiqué du Sommet de Varsovie, 2016b

Nye, Joseph S. (Jr.), "Deterrence and Dissuasion in Cyberspace", *International Security*, vol. 41, no. 3, 2017

Pernik, Piret, *Preparing for Cyber Conflict Case Studies of Cyber Command*, International Centre for Defence and Security, 2018

Robinson, Neil, "Cyber Defence at NATO: from Wales to Warsaw, and Beyond", *Turkish Policy Quarterly*, 2017

Shea, Jamie, "How is NATO Meeting the Challenge of Cyberspace?", *Prism,* vol. 7, no.2, 2017

Slayton, Rebecca, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment", *International Security*, vol. 41, no. 3, 2017

Stoltenberg, Jens, *Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London*, NATO, 23 mai 2019

Tusk, Donald, Juncker, Jean-Claude, and Stoltenberg, Jens, *EU-NATO Joint Declaration*, 2016

UN GGE (United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2013

US Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, 2018

US DoD (Département américain de la Défense), *DOD Dictionary of Military and Associated Terms*, DoD, 2019

US DoD, *Summary: Department of Defense Cyber Strategy*, US DoD, 2018

US NIST, (National Institute of Standards and Technology), *Cybersecurity Framework*, s.d.