Office de surveillance des activités en matière de sécurité nationale et de renseignement

National Security and Intelligence Review Agency

TRÈS SECRET//SI//CEO [redacted]

GOUVERNANCE DU CST S'APPLIQUANT AUX CYBEROPÉRATIONS ACTIVES ET DÉFENSIVES

(EXAMEN DE L'OSSNR N^{O} 20-02)

C.P. 2430, Succursale D
Ottawa, Canada K1P 5W5
Tél : 1-833-890-0293 Téléc. : 613-907-4445

I SOMMAIRE 3
II FONDEMENTS LÉGISLATIFS 5
III INTRODUCTION 5
Contexte de l'examen et méthodologie 5
Que sont les cyberopérations actives et défensives? 6
Fondements juridiques des cyberopérations 7
Cadre politique s'appliquant aux cyberopérations 9
Préparation d'un cadre de consultation entre AMC et le CST 9
Structure de gouvernance du CST 9
IV CONCLUSIONS ET RECOMMANDATIONS 10
Clarté des autorisations ministérielles 10
Informations recueillies au titre d'autorisations précédentes en appui des cyberopérations 10
Consultation du ministre des Affaires étrangères par le CST 11
Portée et étendue des autorisations ministérielles 12
Élaboration des demandes d'AM [redacted] 16
Orientation stratégique des cyberopérations 17
Seuil pour la conduite de COD préventives 20
Collecte de renseignement dans le cadre d'une cyberopération 21
Gouvernance interne du CST 22
Gouvernance des opérations 23
Formation sur le nouveau cadre pour les cyberopérations 24
Cadre de mobilisation entre le CST et AMC 26
Évaluation des risques liés à la politique étrangère par AMC 27
Conformité au droit international et aux cybernormes 28
Communication bilatérale de l'information pertinente 30
V CONCLUSION 32
ANNEXE A : Types de COA/COD 33
ANNEXE B : COA et COD (2019-2020) 34
ANNEXE C : Cadre de travail pour le CST et AMC 35
ANNEXE D : Conclusions et recommandations 36
Conclusions 36
Recommandations 37

I SOMMAIRE

1. (NC) La *Loi sur le CST* confère au Centre de la sécurité des télécommunications (CST) le pouvoir de mener des cyberopérations actives et des cyberopérations défensives (COA/COD). Tel qu'il est stipulé dans la Loi, une COD a pour but de stopper ou de gêner les cybermenaces étrangères qui pourraient peser sur les réseaux ou les systèmes du gouvernement fédéral désignés comme étant importants pour le Canada par le ministre de la Défense nationale (MinDN). Pour leur part, les COA ont pour vocation de restreindre la capacité des adversaires à porter atteinte aux relations internationales, à la défense ou à la sécurité du Canada. Les COA/COD sont autorisées par voie d'autorisations ministérielles (AM) et, en raison de leurs répercussions potentielles sur la politique étrangère, les COA nécessitent l'approbation du ministre des Affaires étrangères (MAE), alors que les COD ne requièrent que l'avis du MAE.

2. (NC) Pendant le présent examen, l'OSSNR s'est fixé pour objectif d'évaluer le cadre de gouvernance qui oriente la conduite des COA/COD. L'OSSNR a également cherché à savoir si le CST prenait suffisamment en compte ses obligations légales, mais aussi les répercussions de ses opérations sur la politique étrangère de l'État canadien. En outre, l'OSSNR a analysé les documents portant sur les politiques et les procédures, sur la gouvernance et sur les opérations, de même que la correspondance entre le CST et AMC. L'examen a débuté par l'analyse des tout premiers documents portant sur les COA/COD et s'est conclu à l'échéance de la période de validité des premières autorisations ministérielles visant des COA/COD.

3. (NC) Dans le présent examen, l'OSSNR a tenu compte de l'apport d'Affaires mondiales Canada (AMC) en considération du rôle important que ce ministère tient dans la structure de gouvernance des COA/COD conçue conformément aux exigences établies par la loi relativement au rôle du MAE à l'égard des AM. Par conséquent, l'OSSNR a été en mesure d'acquérir les éléments de connaissance lui permettant de bien comprendre les structures de gouvernance et de reddition de compte qui ont été mises en place pour ces activités, et ce, en étant exposé à des témoignages uniques de la part de représentants des deux ministères, qui ont fait état de leurs rôles et de leurs responsabilités respectifs.

4. (NC) La nouveauté de ces pouvoirs a contraint le CST à élaborer de nouveaux mécanismes et processus tout en tenant compte des pouvoirs et contraintes nouvellement établis par la Loi. L'OSSNR a d'ailleurs constaté l'important travail effectué par le CST et par AMC pour l'édification de la structure de gouvernance s'appliquant aux COA/COD. Dans le présent contexte, l'OSSNR a remarqué que certains aspects de la gouvernance pouvaient être améliorés en les rendant plus transparents et en les énonçant plus clairement.

5. (NC) En outre, l'OSSNR a noté que le CST pourrait donner une information plus détaillée aux intervenants prenant part au processus décisionnel et à la gouvernance des COA/COD, particulièrement dans les documents comme les AM qui autorisent ces opérations et dans les plans opérationnels établis pour la direction desdites opérations. De plus, l'OSSNR a trouvé que le CST et AMC n'avaient suffisamment pris en compte ni les nombreuses lacunes, qui ont été recensées dans le cadre du présent examen, ni les recommandations visant les éléments suivants :

- la nécessité de mobiliser d'autres ministères pour s'assurer que les opérations suivent les priorités globales du gouvernement du Canada;
- l'absence d'un seuil de démarcation entre une COA et une COD préventive;
- la nécessité d'évaluer la conformité au droit international de chacune des opérations;
- la nécessité de communiquer bilatéralement les informations nouvellement acquises qui renseignent sur le niveau de risque d'une opération.

6. (NC) Les lacunes observées par l'OSSNR sont de celles qui seraient porteuses de risques si elles ne devaient pas être résolues. Par exemple, en raison de leur nature vaste et générale, les catégories d'activités, de techniques et de cibles faisant partie des COA/COD [redacted] pourraient donner lieu à l'interception non intentionnelle d'éléments concernant des activités et des cibles [redacted] Au reste, étant donné que l'apport d'AMC n'est pas le même pour les COA et les COD, le fait de classifier par erreur une COA en tant que COD préventive pourrait donner lieu à un accroissement du risque pour les relations internationales du Canada, dans la mesure où l'on pourrait ne pas avoir suffisamment consulté AMC.

7. (NC) Certes, le présent examen s'est concentré sur les structures de gouvernance en vigueur pour ce qui concerne les COA/COD, mais il faut savoir qu'il sera encore plus important de voir comment ces structures sont appliquées et observées dans la pratique. Nous avons déjà formulé plusieurs observations concernant l'information contenue dans les documents qui ont été produits à ce jour en matière de gouvernance mais, à l'occasion d'un prochain examen portant sur les COA/COD, nous nous pencherons plutôt sur la façon dont les dispositions énoncées dans ces documents sont concrètement mises en œuvre.

8. (NC) L'information fournie par le CST n'a pas été vérifiée de façon indépendante par l'OSSNR. Or, des travaux sont en cours pour établir des politiques opérantes et des pratiques exemplaires favorisant la vérification indépendante d'une multiplicité d'informations, en accord avec l'engagement de l'OSSNR à appliquer une approche qui soit axée sur la confiance, mais renforcée par des mesures de vérification.

II FONDEMENTS LÉGISLATIFS

1. (NC) Le présent examen est effectué en vertu des alinéas 8(1)a) et 8(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (*Loi sur l'OSSNR*).

III INTRODUCTION

Contexte de l'examen et méthodologie

2. (NC) Depuis l'entrée en vigueur de la *Loi sur le Centre de la sécurité des télécommunications* (*Loi sur le CST*), le 1er août 2019, le CST est désormais autorisé à mener en toute autonomie des cyberopérations actives (COA) et des cyberopérations défensives (COD). Au cours des premières séances d'information tenues à l'automne de 2019, l'OSSNR a appris [redacted] Or, des représentants du CST ont ensuite apporté des précisions en indiquant [redacted] Dans ce contexte, l'OSSNR évaluera les COA et les COD suivant une approche progressive. En premier lieu, le présent examen a pour objet de mieux saisir la façon dont s'est développée la structure de gouvernance du CST pour ce qui concerne les COA et les COD. L'OSSNR enchaînera avec un nouvel examen portant, cette fois, sur les opérations. Cet examen ultérieur est en cours et devrait se terminer en 2022.

3. ~~(TS)~~ À l'occasion de ce premier examen, nous avons porté une attention particulière aux structures dont la vocation est de gouverner la conduite des COA et des COD. En l'occurrence, la gouvernance pourrait correspondre à l'établissement de processus servant à guider et à gérer la planification, les engagements interministériels, la conformité, la formation et la surveillance, mais aussi d'autres questions globales qui influent sur la conduite des COA et des COD. L'OSSNR reconnaît que ces structures sont appelées à évoluer en fonction des enseignements tirés de l'expérience acquise en cours d'opérations. En outre, les alliés du Canada, qui disposent de pouvoirs semblables en matière de cyberopérations depuis déjà un certain temps, [redacted][1]. Dans le présent contexte, l'OSSNR s'est donné pour objectif de déterminer si, pendant ces premières étapes d'élaboration d'une structure de gouvernance applicable aux COA et aux COD, le CST avait raisonnablement pris en compte et défini ses obligations juridiques de même que les aspects des COA et des COD qui pourraient influer sur la politique étrangère.

4. ~~(S)~~ Dans le cadre du présent examen, l'OSSNR a évalué les documents faisant état des politiques, des procédures, du système de gouvernance et de la planification des opérations, mais aussi les évaluations des risques ainsi que la correspondance entre le CST et Affaires mondiales Canada (AMC) (dont le rôle déterminant est décrit plus loin). L'OSSNR a examiné les tout premiers documents portant sur l'élaboration de la structure de gouvernance s'appliquant aux COA et aux COD. En l'occurrence, la fin de la période d'examen a coïncidé avec l'échéance des premières autorisations ministérielles visant des COA et des COD, soit le 24 août 2020. Ainsi, les conclusions et les recommandations formulées dans le présent rapport concernent la structure de gouvernance en vigueur pendant la période d'examen.

[1] Mémoire d'AMC, [redacted] 21 août 2019, p. 4.

Que sont les cyberopérations actives et défensives?

5. (NC) Tel qu'il est énoncé dans la *Loi sur le CST*, les cyberopérations défensives (COD) ont pour vocation de stopper ou de contenir les cybermenaces étrangères avant qu'elles n'atteignent les systèmes et les réseaux du gouvernement ou les systèmes désignés par le ministre de la Défense nationale (MinDN) comme étant importants pour le pays, notamment les infrastructures essentielles du Canada et les partis politiques canadiens inscrits[2]. Quant aux cyberopérations actives, elles permettent au gouvernement de recourir aux capacités en ligne du CST pour mener, dans le cyberespace, un vaste éventail d'activités dont l'objet est d'affaiblir furtivement la capacité d'un adversaire à nuire aux activités du Canada en matière, notamment, de relations internationales, de défense ou de sécurité. À titre d'exemple, les COA peuvent comprendre des activités visant à désactiver les dispositifs de communication dont les membres d'un réseau de terroristes étrangers se servent pour communiquer ou pour planifier leurs attaques[3]. Les répercussions des COA et des COD [redacted] d'une COA ou d'une COD.

6. ~~(TS//SI)~~ Pour mener des COA ou des COD, le CST mise sur ses accès à l'infrastructure mondiale d'information (IMI), sur une expertise en matière de renseignement étranger, et sur les partenariats nationaux et internationaux pour acquérir du renseignement apte à favoriser le déroulement des COA et des COD. Les activités menées dans le cadre du volet « renseignement étranger » et du volet « cybersécurité » du mandat du CST permettent au Centre de collecter des informations ayant pour objet de renseigner sur les intentions, les plans et les activités d'auteurs malveillants qui cherchent à nuire aux intérêts du Canada. Selon le CST, la collecte préliminaire de renseignement, le développement des capacités [redacted] constituent la majeure partie du travail nécessaire à la tenue des COA et des COD, alors que les activités qui ont lieu dans le cyberespace ne constituent approximativement que [redacted] de la charge de travail[4].

[2] Les dispositions du paragraphe 21(1) de la *Loi sur le CST* permettent au Ministre de désigner des organisations et des institutions comme étant importantes. Prière de consulter le document « Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada ».
[3] Consulter l'Annexe A pour obtenir un résumé plus détaillé des différences entre les COA et les COD.
[4] Présentation du CST, « Approche évolutive en matière de cyberopérations », mars 2020, p. 9.

Fondements juridiques des cyberopérations

7. (NC) La *Loi sur le CST* fait état des pouvoirs légaux dont jouit le CST pour mener des COA/COD. D'ailleurs, la figure 1 présente des extraits de la Loi qui décrivent ces deux volets. En outre, le régime des autorisations ministérielles dont il est question dans la *Loi sur le CST* confère au Centre les pouvoirs nécessaires à l'exercice des activités ou des catégories d'activités qui sont énumérées à l'article 31 de la *Loi sur le CST* et qui concernent les COA/COD[5].

Cyberopérations défensives (COD)

- Article 18 de la *Loi sur le CST*
- En ce qui a trait au volet de son mandat touchant les cyberopérations défensives, le Centre mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin d'aider à protéger :
  - (a) l'information électronique et les infrastructures de l'information des institutions fédérales;
  - (b) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telle [...].

Cyberopérations actives (COA)

- Article 19 de la *Loi sur le CST*
- En ce qui a trait au volet de son mandat touchant les cyberopérations actives, le Centre mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités.

Figure 1 : Pouvoirs conférés en vertu de la *Loi sur le CST*

8. (NC) Il importe de souligner que la Loi impose des contraintes sur les COA/COD. En l'occurrence, il leur est interdit de cibler des Canadiens ou quiconque se trouve sur le territoire du Canada; elles doivent respecter les termes de la Charte canadienne des droits et libertés[6]; et il leur est interdit de cibler l'IMI au Canada[7].

9. (NC) Les COA/COD doivent être menées au titre d'une autorisation ministérielle (AM) délivrée par le MinDN conformément aux dispositions du paragraphe 29(1) (COD) ou à celles du paragraphe 30(1) de la *Loi sur le CST*[8]. Les AM autorisant les COA/COD habilitent le CST à mener des activités de COA/COD malgré toute autre loi fédérale ou loi d'un État étranger[9]. Pour délivrer une AM, le MinDN doit conclure qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle, et doit également conclure que l'objectif de la cyberopération ne pourrait pas être raisonnablement atteint par d'autres moyens[10]. De plus, le MinDN doit consulter le ministre des Affaires étrangères (MAE) avant de délivrer une AM pour les COD, mais doit obtenir le consentement du MAE avant de délivrer une AM pour les COA[11]. Toute activité de COA/COD autorisée ne peut causer, intentionnellement ou par négligence criminelle, des lésions corporelles à une personne physique ou la mort de celle-ci; ne peut tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie[12]. Il importe d'ajouter que, contrairement aux AM délivrées pour le volet renseignement étranger de même que pour le volet cybersécurité et assurance de l'information du mandat du CST, les AM visant les COA et les COD ne sont pas assujetties à l'approbation du commissaire au renseignement.

---

[5] Les activités autorisées en vertu de l'article 31 de la *Loi sur le CST* sont : 1) accéder à des portions de l'infrastructure mondiale de l'information; 2) installer, maintenir, copier, distribuer, rechercher, modifier, interrompre, supprimer ou intercepter quoi de ce soit dans l'infrastructure mondiale de l'information ou par son entremise; 3) prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète de l'activité; 4) mener toute autre activité qui est raisonnable dans les circonstances et est raisonnablement nécessaire pour faciliter l'exécution des activités ou des catégories d'activités visées par l'autorisation.

[6] *Loi sur le CST*, paragr. 22(1).

[7] *Loi sur le CST*, alinéa 22(2)a).

[8] *Loi sur le CST,* alinéa 22(2)b).

[9] *Loi sur le CST*, paragr. 29(1) et 30(1).

[10] *Loi sur le CST*, paragr. 34(1) et 34(4). Le MinDN doit également conclure que l'objectif des COA/COD ne pourrait pas être raisonnablement atteint d'une autre manière, et qu'aucune information ne sera acquise au titre de l'autorisation, sauf conformément à une autorisation de renseignement étranger, de cybersécurité ou de mesures d'urgence.

[11] *Loi sur le CST*, paragr. 29(2) et 30(2).

[12] *Loi sur le CST,* paragr. 32(1).

10. (NC) En plus des volets COA/COD prévus par son mandat[13], le CST peut également fournir une assistance technique et opérationnelle à d'autres ministères du gouvernement du Canada (GC). Le CST peut assister les organismes fédéraux chargés de l'application de la loi et de la sécurité (OALS) aux fins de prévention de la criminalité, d'atténuation des menaces pour la sécurité du Canada et de soutien à des missions militaires autorisées par le GC. Lorsqu'il prête son assistance, le CST agit en vertu des autorisations légales – et des restrictions afférentes – conférées aux organismes ou aux ministères faisant appel à ladite assistance. De même, les personnes agissant au nom du CST jouissent des mêmes mesures d'exemption, de protection et d'immunité que celles qui agissent au nom des OALS demandeurs. Les activités menées aux fins de ce type d'assistance seront analysées dans le cadre d'examens ultérieurs de l'OSSNR.

11. (NC) Outre la *Loi sur le CST*, le droit international[14] est pris en compte dans le cadre juridique s'appliquant aux activités de COA/COD. Les activités du CST sont liées par le droit international coutumier dans la mesure où le droit canadien adopte *ipso facto* le droit international coutumier par l'intermédiaire de la common law, sauf en cas d'incompatibilité entre les lois[15].

12. (NC) L'OSSNR note que le droit international en matière de cyberespace est un domaine en développement. Dans cette sphère du droit, la pratique des États est limitée, les opinions de droit (postulats selon lesquels les États estiment que ce type de pratique correspond à une obligation juridique) sont rares et le droit des traités (précisions sur les *modalités* d'application du droit international au cyberespace) n'en est qu'à ses balbutiements. De plus, bien qu'il ait fait valoir que le droit international s'appliquait au cyberespace, le Canada n'a pas encore défini sa propre vision quant à l'application du droit international aux activités du cyberespace[16]. Or, le Canada s'est engagé à promouvoir l'établissement d'une vision commune à tous les États pour ce qui a trait à des normes volontaires et non contraignantes favorisant le comportement responsable des États dans le cyberespace[17]. Ainsi, l'OSSNR suivra de près le développement de cette sphère du droit international, notamment, les pratiques observées par les États à l'égard des activités de COA/COD du CST. Dans le cadre du prochain examen visant les activités de COA/COD, l'OSSNR se penchera, cette fois, sur la façon dont le CST et AMC tiennent compte du droit international en vigueur.

---

[13] Conformément à l'article 15 de la *Loi sur le CST*, le mandat du Centre se décline en cinq volets : le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives (COD), les cyberopérations actives (COA), et l'assistance technique et opérationnelle.

[14] Le droit international se fonde sur quatre sources, comme l'énonce le paragraphe 38(1) du Statut de la Cour internationale de justice : les conventions internationales, soit générales, soit spéciales, établissant les règles expressément reconnues par les États en litige; la coutume internationale comme preuve d'une pratique générale acceptée comme étant le droit; les principes généraux de droit reconnus par les nations civilisées; […] les décisions judiciaires et la doctrine des publicistes les plus qualifiés des différentes nations, comme moyen auxiliaire de détermination des règles de droit. Extrait du jugement dans l'affaire *Nevsun Resources Ltd.* c. *Araya*, 2020 CSC 5, paragr. 76 [*Nevsun*].

[15] *Nevsun*, paragr. 85 à 90.

[16] Par exemple, bon nombre d'États se sont prononcés publiquement sur l'applicabilité du droit international à l'égard du cyberespace, notamment l'Allemagne (2021), le Japon (2021), l'Australie (2020), la Nouvelle-Zélande (2020), la Finlande (2020), la France (2019), les Pays-Bas (2019) et le Royaume-Uni (2018).

[17] Le Canada et les autres États membres de l'ONU ont approuvé les rapports consensuels de 2013 et de 2015 du Groupe d'experts gouvernementaux (de l'ONU) chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité nationale (GEG de l'ONU). Bien que les rapports de 2013 et de 2015 aient permis d'établir un consensus sur des libellés confirmant l'application du droit international et mettant en évidence certaines sphères pertinentes du droit, c'est le rapport de 2015 qui est considéré comme étant représentatif de la perspective mondiale en matière d'utilisation des cybercapacités. L'Assemblée générale de l'ONU a adopté le rapport de 2013 (A/RES/68/243) ainsi que le rapport de 2015 (A/RES/70/237). En outre, le rapport de 2015 fait également état de l'adoption de onze normes volontaires et non contraignantes favorisant le comportement responsable des États dans le cyberespace. Par ailleurs, le Canada prend part à d'autres forums multilatéraux dans le but de promouvoir l'établissement d'une vision commune des règles devant inciter les États à se comporter de façon responsable dans le cyberespace.

Cadre politique s'appliquant aux cyberopérations

Préparation d'un cadre de consultation entre AMC et le CST

13. ~~(TS)~~ Il est possible que les COA/COD accroissent le niveau de risque pour la politique étrangère et les relations internationales du Canada. Bien que le volet renseignement étranger du CST ne vise qu'à collecter des informations, les COA/COD [redacted][18], [redacted] Comme AMC est le ministère responsable des affaires internationales et de la politique étrangère du Canada, le MAE est appelé, en vertu de la loi, à tenir un rôle lorsqu'il s'agit de consentir à ce que le MinDN délivre une autorisation ministérielle pour des COA.

14. ~~(S)~~ Conformément aux directives du MAE, le CST et AMC ont uni leurs efforts pour créer un cadre de collaboration sur les questions ayant trait aux COA/COD. Le CST et AMC se sont mobilisés sur ces questions avant l'entrée en vigueur de la *Loi sur le CST*, de sorte à recenser les exigences énoncées dans la Loi en matière de consultation et de consentement. Ensemble, le CST et AMC ont mis sur pied divers organes interministériels appelés à se pencher sur les COA/COD dans le but de faciliter le processus de consultation aux divers niveaux, notamment, les groupes de travail constitués au niveau des directeurs généraux et du sous-ministre adjoint[19].

Structure de gouvernance du CST

15. (NC) L'Ensemble des politiques relatives à la mission (EPM) du CST décrit en détail les pouvoirs permettant d'orienter les COA/COD, les activités interdites en cours de COA/COD – de même que les consignes permettant d'interpréter ces interdictions – et le cadre de gouvernance suivant lequel il convient de surveiller le déroulement et la conduite des COA/COD, cadre désigné par l'appellation Cadre de pouvoirs et de planification commun (CPPC)[20]. La structure générale du cadre de gouvernance et des processus connexes a été conçue pour être employée dans toutes les COA/COD, tous niveaux de risque confondus. Toutefois, c'est en fonction du niveau de risque que ledit cadre établit les divers niveaux d'approbation.

16. ~~(TS)~~ Pendant la période consacrée à l'examen, le CPPC comportait plusieurs des éléments nécessaires à la planification, à l'approbation et à la conduite des opérations. Le principal instrument de planification était [redacted] lequel décrit les [redacted] de même que [redacted] tout en mettant en évidence les risques et les mesures d'atténuation correspondantes. [redacted] sert à déterminer et à énoncer l'éventail des risques associés à toute nouvelle activité. Durant la période d'examen, le CST a élaboré [redacted] L'OSSNR a également reçu des documents semblables [redacted] ne coïncidant pas avec la période d'examen, mais contenant des informations pertinentes sur la structure de gouvernance et le niveau opérationnel.

17. ~~(TS)~~ Deux principaux groupes de travail ont pour objet d'évaluer et, le cas échéant, d'approuver, les plans internes visant les COA/COD. Le Groupe pour les cyberopérations (GCO) est un organe d'approbation au niveau des directeurs; il regroupe les principaux intervenants et est présidé par le directeur du secteur opérationnel ayant initié ou parrainé la demande de cyberopérations. Le rôle du GCO est d'examiner le plan opérationnel et d'en jauger les risques ainsi que les avantages. Le GCO peut approuver [redacted] il peut

[18] Mémoire d'AMC, [redacted] 21 août 2019, p. 2.
[19] Consulter l'Annexe C pour obtenir un aperçu des pratiques de mobilisation établies entre le CST et AMC.
[20] Ensemble des politiques relatives à la mission (EPM), chapitre sur les cyberopérations, 22 septembre 2020.

également faire approuver ces éléments par le Groupe de gestion des cyberopérations (GGCO), s'il y a lieu. Le GGCO est un organe d'approbation qui se situe au niveau des directeurs généraux (DG) et qui est mis sur pied [redacted] a été examiné et recommandé par le GCO[21].

18. ~~(TS)~~ Ensuite, le CST prépare [redacted] est examinée en interne pour s'assurer qu'elle correspond à la teneur [redacted] elle est ensuite approuvée au niveau des directeurs, bien que le CST ait indiqué que l'approbation pourrait être déléguée à un gestionnaire[22].

IV CONCLUSIONS ET RECOMMANDATIONS

Clarté des autorisations ministérielles

19. (NC) L'OSSNR avait entrepris de déterminer si les exigences au titre de la *Loi sur le CST* relativement aux COA/COD se traduisent convenablement dans les AM du MinDN autorisant la tenue d'activités de COA/COD et si le CST a bien consulté le MAE et obtenu son consentement, comme l'exige la Loi.

20. ~~(TS)~~ L'OSSNR s'est penché sur deux AM portant respectivement sur des COA et des COD et valides du [redacted] Notamment, les deux AM n'approuvaient que des CAO/COD [redacted][23]. De plus, l'OSSNR a examiné des documents en appui des AM, y compris les demandes présentées par le chef au MinDN[24] et les lettres de confirmation connexes du MAE, ainsi que les documents de travail et la correspondance fournis par le CST et Affaires mondiales Canada (AMC).

21. ~~(TS)~~ Les AM examinées par l'OSSNR énonçaient les nouveaux pouvoirs conférés au titre de la *Loi sur le CST* et définissaient les conditions s'appliquant à la tenue des COA/COD, ainsi que les interdictions indiquées dans la Loi. De plus, les AM demandaient que les activités de COA/COD soient harmonisées aux priorités du Canada en matière de politique étrangère et tiennent compte des priorités stratégiques du gouvernement du Canada en matière de sécurité nationale, de politique étrangère et de défense[25].

Informations recueillies au titre d'autorisations précédentes en appui des cyberopérations

22. (TS[redacted]) Le CST a reçu l'autorisation de mener des COA/COD à l'époque où la collecte de renseignements électromagnétiques (SIGINT) étrangers était autorisée par

[21] CST – Examen du CPPC des COA/COD de 2020, p. 2.
[22] Présentation du CST, Séance d'information à l'intention de l'OSSNR sur les cyberopérations actives et défensives, mars 2020, diapositive 3. Présentation du CST, « Séance d'information à l'intention de la chef du CST [redacted] p. 9. Document du CST : [redacted] p 11.
[23] Au cours de la période à l'examen, les autorisations ministérielles dont disposait le CST ne lui permettaient [redacted] L'OSSNR a examiné toutes les autorisations ministérielles disponibles visant cette période.
[24] Comme l'énonce la *Loi sur le CST*, le chef du CST présente une demande d'AM au MinDN, qui s'y appuie pour émettre ou refuser une AM. L'OSSNR tient à souligner que les demandes d'AM avaient tendance à être plus exhaustives que les AM en soi et comprenaient de l'information qui ne se trouvait pas dans les AM. Ce fait est important, puisque le CST n'est pas lié à la demande d'AM et, par conséquent, tout détail absent de l'AM définitive a une incidence sur les restrictions imposées au CST.
[25] Autorisations des cyberopérations actives et défensives, [redacted]

des AM délivrées en application de la *Loi sur la défense nationale*[26]. [redacted][27], [redacted][28] [redacted][29]. Le CST a confirmé à l'OSSNR que les COA/COD [redacted] reposaient uniquement sur des informations recueillies au titre des AM délivrées en application de la *Loi sur le CST*[30]. [redacted] le CST a fait valoir que [redacted] L'OSSNR le confirmera dans le cadre de son examen ultérieur de COA/COD précises.

Consultation du ministre des Affaires étrangères par le CST

23. ~~(TS)~~ Le CST a fourni à AMC les dossiers complets de demande d'AM pour les COA/COD en place durant la période à l'examen[31]. De plus, les représentants d'AMC et du CST ont noué le dialogue à différents niveaux avant l'entrée en vigueur de la *Loi sur le CST* et pendant l'élaboration des AM, particulièrement pour ce qui est de l'évaluation des catégories d'activités qui y sont autorisées[32]. Dans sa réponse au dossier de demande d'AM du CST, le MAE a fourni des lettres confirmant qu'il avait été consulté et qu'il consentait aux AM de COA et de COD respectivement. L'OSSNR est ravi de constater cette collaboration rapide et rigoureuse de la part des deux organisations, étant donné le lien entre leurs mandats respectifs dans le contexte des COA/COD.

24. ~~(TS)~~ Les deux lettres du MAE soulignent l'utilité des COA/COD [redacted] du gouvernement du Canada, expliquant l'importance de faire preuve de prudence concernant ce moyen dans les premières étapes. Notamment, le MAE attire l'attention sur les catégories d'activités « soigneusement définies » dans l'AM de COA pour garantir que les activités autorisées au titre de l'AM présentaient [redacted][33]. Enfin, le MAE a chargé ses représentants de travailler avec le CST pour mettre en place un cadre de collaboration entourant les [redacted][34]. Cette directive du MAE concorde avec le point

[26] La *Loi sur le CST* a établi une exigence selon laquelle les AM doivent être examinées et approuvées par le nouveau rôle du commissaire au renseignement, alors que les AM demandées en application de la *Loi sur la défense nationale* n'étaient pas assujetties à une telle exigence.
[27] Par exemple, [redacted]
[28] [redacted]
[29] [redacted]
[30] Dans ce contexte, [redacted] Voir la réponse du CST, « ACO/DCO Governance review - RFI-4 responses », 22 janvier 2021, Q1.
[31] Les deux lettres du MAE qu'a examinées l'OSSNR renvoyaient aux AM et aux demandes en appui du chef. De plus, l'OSSNR a remarqué que le CST avait fourni à AMC les deux AM et les demandes. L'OSSNR souligne qu'il est important que le MAE et AMC continuent de recevoir les demandes, puisque celles-ci contiennent davantage de détails.
[32] AMC, réunion, 16 février 2021.
[33] Lettre du ministre des Affaires étrangères au ministre de la Défense nationale concernant l'AM de COA 2019-2020, p. 1.
[34] *Ibid.*

de vue d'AMC sur l'importance d'assurer la cohérence des activités du CST avec la politique étrangère du Canada et le fait que l'AM ou un autre mécanisme devrait le garantir[35].

Portée et étendue des autorisations ministérielles

25. ~~(TS)~~ L'AM de COA **concerne la politique opérationnelle du CST** délivrée en vertu de l'article 31 de la *Loi sur le CST* a autorisé des catégories d'activités, y compris :

a. [redacted] se mêler des [redacted] d'une cible ou des éléments de l'infrastructure mondiale de l'information;
b. [redacted]
c. [redacted]
d. perturber la capacité d'un auteur de menace d'utiliser certaines infrastructures.

26. ~~(TS)~~ L'AM pour la COD **concerne des opérations du CST** autorisait les mêmes activités, à l'exception de la dernière catégorie, [redacted][36].

27. ~~(TS)~~ Les AM pour les COA/COD stipulaient que le CST devait mener les COA/COD [d'une certaine façon] [redacted][37]. Selon l'AM de COA, ce sont ces conditions qui, si elles sont respectées, font en sorte que les COA/COD menées au titre de ces AM comportent [redacted][38]. Bien qu'AMC évalue les risques en matière de politique étrangère plutôt sur le plan opérationnel[39], les AM élaborées pendant la période à l'examen n'imposaient que deux conditions à respecter lors de la tenue des COA/COD. De plus, c'est au CST qu'il revient de déterminer les critères permettant de respecter ces conditions générales; l'AM demande seulement au CST d'en faire rapport. L'OSSNR ajoute que ces conditions ne comprennent aucune variable sur le plan de la politique étrangère, [redacted] Pour que soit confirmé le risque [redacted] d'une opération pour la politique étrangère, l'OSSNR est d'avis qu'il est important que les AM établissent le calcul des facteurs de risque en matière de politique étrangère.

28. (TS[redacted] indiquant :

[redacted]

[35] AMC, [redacted] mémoire, 21 août 2019, p. 1.
[36] Autorisations ministérielles de COA et de COD, 2019-2020, paragraphes 2(b)(ii) et 2(b)(iv), respectivement. Voir aussi la demande d'obtention d'une autorisation ministérielle de COA présentée par le CST, 2019-2020, p. 1.
[37] *Ibid.*
[38] CST, « CSE Act: Ministerial Authorizations for Cyber Operations », présentation, août 2019, p. 9. Pour que les opérations de l'AM soient considérées [redacted]
[39] Cette évaluation a lieu dans le cadre de l'évaluation des risques en matière de politique étrangère qui se déroule au cours de la planification d'une opération. Ce processus est expliqué plus en détail plus loin dans le présent rapport.

[redacted][40]

29. ~~(TS)~~ Le CST semble avoir répondu [redacted] **concerne des opérations du CST** [redacted] En outre, la capacité du ministre à évaluer les activités autorisées aux termes de la *Loi sur le CST* pourrait également être touchée[41]. Pour cette évaluation, la demande d'AM doit contenir suffisamment de détails pour que le ministre soit convaincu que les exigences sont remplies.

30. ~~(TS)~~ Les catégories des activités de COA/COD, dont certaines sont exposées au paragraphe 27, sont grandement généralisées. Par exemple, presque toutes les activités menées dans le cyberespace peuvent être raisonnablement placées dans la catégorie [redacted] ou se mêler [redacted] **concerne des opérations du CST** [redacted] des éléments de l'infrastructure mondiale de l'information ». [redacted]

31. ~~(TS)~~ Effectivement, les discussions préliminaires entre le CST et AMC ont attiré l'attention sur le fait que [redacted] et de contenu [traduction] « soulevaient des questions complexes[42] », bien que l'OSSNR précise que de telles activités sont néanmoins autorisées dans l'AM définitive de COA dans la catégorie d'activités [traduction] [redacted][43] Autrement dit, l'autorisation d'une catégorie d'activités [redacted] a été intégrée dans une catégorie encore plus vaste d'activités, sans [redacted] évidente [redacted] qui y étaient liés. Ce type de catégorisation ne permet pas une communication suffisante de l'information pour que le ministre saisisse les activités [redacted] qui pourraient être menées au titre de l'AM.

32. ~~(TS)~~ En revanche, les techniques et exemples connexes énoncés dans les demandes sont les seuls moyens qui permettent de préciser les types d'activités pouvant avoir lieu dans le cadre d'une COA/COD. Ces exemples servent de fondement au MinDN pour évaluer les catégories d'activités dont il est question dans la demande d'AM. Dans les échanges préliminaires entre le CST et AMC, les catégories d'activités étaient décrites et analysées conjointement avec les techniques employées dans leur exécution[44]. Par exemple, il a été noté que **concerne des opérations du CST** [redacted][45], ce qui a fourni plus d'information à l'OSSNR en ce qui a trait aux actions qui se trouvaient exactement dans la catégorie d'activités. L'OSSNR ajoute que même ces techniques

---

[40] [redacted] Soulignement par l'OSSNR.
[41] Paragraphes 34(1) et 34(4) de la *Loi sur le CST*.
[42] AMC, « Pre-briefing for 9 May CSE/GAC ADM meeting », présentation, diapositive 4. Dans un autre document, AMC explique plus en détail, dans le contexte [redacted] Voir AMC, « ACO FP considerations thoughts », courriel, 30 avril 2019.
[43] CST, réponse à la DI-08, 12 mars 2021.
[44] AMC, « ACO FP considerations thoughts », courriel, 30 avril 2019.
[45] AMC, « Pre-briefing for 9 May CSE/GAC ADM meeting », présentation, diapositive 4.

et exemples sont décrits dans les demandes comme faisant partie d'une liste non exhaustive, ce qui pourrait permettre au CST de mener des activités qui ne sont pas précisément définies dans les demandes[46].

33. ~~(TS)~~ De même, la cible des activités de COA/COD est habituellement désignée comme un « acteur étranger », ce qui pourrait englober un large éventail de **concerne des opérations du CST** [redacted][47]. Dans les débuts de l'élaboration de l'AM, le CST et AMC avaient abordé [redacted] directement dans les AM, mais AMC a précisé que [redacted] visaient principalement [redacted] étant donné [redacted][48]. AMC a précisé que l'AM de COA [traduction] « définirait [mieux] [redacted] dans une certaine mesure[49] ». Ni l'une ni l'autre de ces considérations ne figurait dans les AM définitives [redacted][50] qui, d'après les explications du CST, ne se limitent pas aux activités [redacted], c'est-à-dire que [redacted][51]. L'OSSNR estime que les AM devraient définir clairement les cibles des activités de COA/COD, [redacted] les COA/COD [redacted] à des ensembles précis de cibles [redacted] afin que les activités permises par l'AM traduisent le [redacted]

34. ~~(TS)~~ L'OSSNR souligne que seules les AM, et non les demandes connexes, donnent au CST l'autorisation de mener ses activités. Par conséquent, l'exclusion de cette information des AM signifie que seules les grandes catégories d'activités, telles qu'elles sont décrites dans les AM, guident les mesures que peut prendre le CST dans le cadre de COA et non pas les techniques et exemples énoncés dans les demandes qui servent de fondement à la norme sur laquelle s'appuie le risque des activités. Selon l'OSSNR, les catégories décrites dans les AM ne restreignent pas suffisamment les activités du CST **concerne des opérations du CST** [redacted] Même si, aux dires d'AMC, les processus de consultation interministérielle entre les deux organisations peuvent servir de mécanisme limitant les activités du CST[52], ces processus n'ont pas été nettement consignés dans les AM les autorisant. L'OSSNR est d'avis que des AM pour les COA/COD plus précises réduiraient la possibilité de confusion relativement aux activités précisément autorisées.

35. ~~(TS)~~ La méthode visant à préciser les catégories d'activités concorde avec la façon de faire habituelle du CST liée à l'obtention d'autorisations larges de la part de hauts dirigeants comme le

---

[46] Autorisation ministérielle de COA, 2019-2020, paragr. 29; et Autorisation ministérielle de COD, 2019-2020, paragr. 18.
[47] Par exemple, AMC indique qu'[redacted] (voir le cadre de référence du CST-GAC, p. 7).
[48] AMC, « Pre-briefing for 9 May CSE/GAC ADM meeting », présentation, diapositive 3. [redacted]
[49] AMC, « Pre-briefing for 9 May CSE/GAC ADM meeting », présentation, diapositive 6.
[50] Par exemple, la justification liée au [redacted] dans la demande de COA décrit [redacted] sans préciser [redacted] Il pourrait s'agir d'un large éventail d'entités étrangères possibles, y compris celles [redacted] Toutefois, la demande cherche par la suite à obtenir l'autorisation de contrecarrer et de perturber ces activités en [redacted] situées à l'extérieur du Canada », sans préciser [redacted] Voir l'Autorisation ministérielle de COA, 2019-2020.
[51] CST, commentaires sur l'exactitude des faits, 13 août 2021.
[52] AMC, commentaires sur l'exactitude des faits, 18 août 2021.

ministre, accompagnées de mesures de contrôle plus précises qui guident les opérations à exécuter en fonction des limites de l'activité autorisée. AMC note la tendance à s'appuyer sur des autorisations plus précises selon [redacted] visée par la demande d'autorisation. Le CST a expliqué que son approche lui permettait d'obtenir l'autorisation de mener des activités de façon à [traduction] « apporter une souplesse maximisant les occasions, mais également des réserves suffisantes pour assurer l'atténuation appropriée des risques[53]. »

36. ~~(TS)~~ Bien que l'OSSNR reconnaisse que les AM doivent donner au CST suffisamment de jeu pour qu'il mène des COA/COD [redacted] s'il le faut, il est important que le CST ne mène pas d'activités qui n'étaient pas envisagées ni autorisées par le MinDN ou le MAE lors de la délivrance des AM applicables. Toujours selon l'OSSNR, dans le contexte des COA/COD [redacted], le CST peut adopter une approche plus transparente qui préciserait les catégories d'activités qu'il demande au ministre d'autoriser. C'est tout particulièrement important étant donné que le CST utilise ces nouvelles autorisations depuis peu. L'autorisation de catégories d'activités, de techniques connexes et d'ensembles de cibles plus précis diminuerait la possibilité que les COA/COD [redacted] dans les AM.

37. ~~(TS)~~ Le CST a indiqué que [traduction] « des objectifs clairs permettent fondamentalement de montrer le caractère raisonnable et la proportionnalité[54]. » L'OSSNR partage le même avis et croit que les catégories d'activités et les objectifs décrits dans les AM et les demandes connexes devraient être plus explicites afin que le MinDN puisse confirmer le caractère raisonnable et la proportionnalité des COA/COD, d'autant plus que les AM étudiées dans le cadre du présent examen ne se rapportaient pas précisément à une opération. Dans le cadre de l'autorisation, le ministre exige également que le CST lui fournisse un rapport trimestriel sur les activités qui ont été menées[55].

38. ~~(TS)~~ De plus, pour délivrer une autorisation, le MinDN doit être convaincu que les activités sont raisonnables et proportionnelles, et qu'il y a des motifs raisonnables de croire que l'objectif de la cyberopération ne peut raisonnablement être atteint d'une autre manière[56]. Cette exigence met davantage l'accent sur la nécessité que le MinDN comprenne, dans une certaine précision, les types d'activités et les objectifs exécutés en application de l'autorisation.

39. ~~(TS)~~ Dans le cas des deux AM examinées, le ministre a conclu que les exigences énoncées au paragraphe 34(4) de la *Loi sur le CST* étaient satisfaites[57]. De plus, les AM énoncent les objectifs à atteindre par les COA/COD. Toutefois, la justification selon laquelle les objectifs ne pourraient être raisonnablement atteints d'une autre manière dans les limites de l'AM de COA est très vague et se concentre sur les stratégies d'atténuation générales des activités de cybermenace. Étant donné la rareté des détails fournis au ministre dans le présent cadre, il pourrait être difficile pour le MinDN de satisfaire à cette exigence législative. En ce qui a trait au seuil établi par le paragraphe 34(4) de la *Loi sur le CST*, le Centre a indiqué que [traduction] « la demande d'autorisation doit énoncer les faits qui expliquent comment chacune des activités décrites dans l'autorisation fait partie d'un plus grand ensemble d'activités individuelles ou d'une catégorie d'activités qui atteint un objectif ne pouvant pas être raisonnablement atteint d'une autre manière[58]. » Dans son prochain examen des COA/COD, l'OSSNR tentera de déterminer si les COA/COD concordent avec les objectifs établis dans l'AM et se

[53] Dossier de réunion, « GAC-CSE Meeting April 17, 2019 ».
[54] Dossier de réunion, « GAC-CSE meeting May 3, 2019 ».
[55] CST, commentaires sur l'exactitude des faits, 13 août 2021.
[56] *Loi sur le CST*, paragraphes 34(1) et 34(4).
[57] Autorisation ministérielle de COA, 2019-2020, paragraphe 2(c); et Autorisation ministérielle pour la COD, 2019-2020, paragraphe 2(c).
[58] CST, « NSIRA ACO/DCO governance review: Response to RFI-7 », réponse, 5 février 2021, Q9.

penchera sur la détermination, par le CST, qu'ils n'auraient pas pu être raisonnablement atteints d'une autre manière.

(NC) Conclusion nº 1 : Les demandes d'autorisation ministérielle pour les cyberopérations actives et défensives n'offrent pas suffisamment de détails pour que les ministres concernés comprennent l'étendue des catégories d'activités demandées dans l'autorisation. De même, l'autorisation ministérielle ne définit pas suffisamment les catégories d'activités, les techniques connexes et les ensembles de cibles à utiliser dans l'exécution des opérations.

(NC) Conclusion nº 2 : L'évaluation des risques pour la politique étrangère exigée suivant deux conditions des autorisations ministérielles pour les cyberopérations actives et défensives repose trop sur la détermination technique des risques au détriment des éléments qui caractérisent la politique étrangère du gouvernement du Canada.

(NC) Recommandation nº 1 : L'OSSNR recommande que le CST définisse plus précisément les catégories d'activités, les techniques connexes et les ensembles de cibles employés dans le cadre des cyberopérations actives et défensives, ainsi que les motifs et objectifs sous-jacents, tant dans les demandes que dans les autorisations ministérielles pour ces activités.

(NC) Recommandation nº 2 : L'OSSNR recommande qu'AMC inclue, dans les autorisations ministérielles, un mécanisme d'évaluation de tous les paramètres des risques pour la politique étrangère découlant des cyberopérations actives et défensives.

Élaboration des demandes d'AM [redacted]

40. ~~(TS//SI)~~ Au cours de la période à l'examen, le CST a préparé des demandes d'AM pour ce qu'il considérait comme étant des COA/COD [redacted] dont l'élaboration a été prioritaire [redacted] **concerne des opérations du CST** [redacted][59]. Alors que se développent les moyens dont le CST dispose pour mener des COA/COD et que le Centre commence à [redacted][60]. L'OSSNR a constaté que le CST et AMC envisageaient les COA représentant un [redacted][61],

[59] AMC, « Explanatory Note for NSIRA », réponse à la DI-02, 5 mars 2021.
[60] Dans ce contexte, AMC a indiqué [traduction] : « AMC et le CST ont convenu que le Canada devrait commencer son incursion dans le monde des cyberopérations par [redacted] Au fur et à mesure que le gouvernement gagne en expérience, [redacted] Voir AMC, [redacted] mémoire, 21 août 2019, p. 4.
[61] CST [traduction] : [redacted]
CST, « Proposed Agenda for GAC-CSE Meeting », courriel, 16 janvier 2020.

lesquelles, si elles sont exécutées, [redacted] selon la méthodologie d'AMC[62].

41. ~~(TS)~~ Bien que les AM que l'OSSNR a obtenues à ce jour, lesquelles ne se rapportent pas précisément à une opération, permettent au CST de mener [redacted], l'OSSNR estime que leur nature générale ne se transfère pas [redacted] [AM potentielles de nature différentes] [redacted] Par exemple, [description d'une inquiétude de l'OSSNR concernant l'habilité du Ministre à analyser pleinement certains facteurs des cyberopérations dans un contexte particulier] [redacted] Dans le cadre de l'élaboration de la demande d'AM de COA de 2019-2020, AMC a indiqué que [traduction] « d'autres fins demanderaient d'autres AM. Elles ne seront pas complètement générales; elles seront précises pour un contexte donné[63]. »

42. ~~(TS)~~ En outre, dans le régime législatif actuel, les demandes d'AM représentent un mécanisme clé donnant au MAE l'occasion d'évaluer les activités de COA/COD. En raison des [redacted] COA/COD [redacted] pour la politique étrangère et les relations internationales du Canada, l'OSSNR estime que le MAE devrait participer plus directement à l'élaboration et à l'exécution à l'échelle ministérielle, en plus de l'engagement sur le terrain des opérations entre le CST et AMC. Les deux ministres peuvent assurer plus efficacement leur responsabilisation[64] relative à de telles opérations au moyen d'AM individuelles qui donnent des détails précis sur l'opération et sa justification, et sur les activités, outils et techniques employés. Par conséquent, lorsque le CST se penche sur des COA [redacted] l'OSSNR l'encourage à élaborer des demandes d'AM propres à ces opérations et à veiller à ce que ces documents contiennent tous les détails opérationnels pertinents permettant à chaque ministre d'évaluer pleinement les répercussions et les risques liés à chaque cyberopération et d'en prendre la responsabilité.

Orientation stratégique des cyberopérations

43. (NC) L'article 19 de la *Loi sur le CST* régit les pouvoirs du CST quant à la conduite de COA qui se rapportent aux affaires internationales, à la défense ou à la sécurité, donc à des domaines qui peuvent faire appel à la responsabilité d'autres ministères et organismes. Qui plus est, les AM examinées par l'OSSNR exigent que les COA soient [traduction] « harmonisées aux priorités du Canada en matière de politique étrangère et tiennent compte des priorités stratégiques du gouvernement du Canada liées à la sécurité nationale, à la politique étrangère et à la défense[65] ».

---

[62] AMC, « FP risks of Cyber Ops », courriel, 22 mai 2019. Parmi les considérations soulignées par AMC, notons les suivantes s'appliquant à ce contexte : [redacted]

[63] AMC, « Pre-briefing for 9 May CSE/GAC ADM meeting », présentation, diapositive 8.

[64] CST, « RE: ACO/DCO Governance Review: RFI-09 », réponse, 30 mars 2021. Le CST a expliqué que les COA/COD comportent inévitablement des répercussions et des risques faisant en sorte qu'il faille fournir au MAE [traduction] « l'information dont il a besoin pour examiner les répercussions de l'autorisation. » Au bout du compte, comme l'a indiqué le MinDN devant le Comité permanent de la sécurité publique et nationale « lorsqu'il s'agit de menaces et de mesures éventuelles que nous, le gouvernement, pouvons prendre, il n'y a pas qu'un seul ministre qui intervienne. »

[65] Autorisation ministérielle de COA, 2019-2020, paragraphe 29; et Autorisation ministérielle pour la COD, 2019-2020, paragraphe 11(f). Soulignement par l'OSSNR.

L'établissement de ces priorités fait intervenir plusieurs ministères fédéraux du Canada, comme le Bureau du Conseil privé (BCP), le MDN et Sécurité publique Canada (SP), qui sont responsables de la coordination et de la surveillance de différentes parties de l'établissement des priorités dans le présent contexte[66]. Tout au long du présent examen de la gouvernance, on a noté que le CST atteste la conformité à ces exigences par un énoncé indiquant que l'AM répond aux grandes priorités du gouvernement du Canada, sans élaborer sur la façon dont ces priorités sont satisfaites[67].

44. ~~(S)~~ Les processus interministériels du gouvernement du Canada relativement à la coordination d'activités et d'opérations de sécurité nationale ne datent pas d'hier. Par exemple, lorsque le MAE requiert une collecte de renseignements étrangers au Canada, il présente une demande au ministre de la Sécurité publique afin que le Service canadien du renseignement de sécurité (SCRS) facilite la collecte conformément à l'article 16 de la *Loi sur le SCRS*. Un comité composé de représentants [redacted] se penche ensuite sur le type de demande. Le comité examine ensuite les questions au niveau du sous-ministre adjoint, [redacted] **concerne les processus décisionnaire du GC** [redacted][68]. De même, un processus interministériel peut également confirmer la conformité d'une COA aux priorités plus larges et l'impossibilité d'atteindre raisonnablement les objectifs d'une autre manière[69]. Autrement dit, les consultations interministérielles sont une façon d'évaluer les objectifs des COA et leur conformité aux priorités plus larges du gouvernement du Canada, et de déterminer s'il existe une autre manière d'atteindre les objectifs fixés, comme l'exige la *Loi sur le CST*.

45. ~~(TS)~~ L'établissement de priorités plus larges pour le gouvernement du Canada est ressorti comme élément clé de la structure de gouvernance de ce nouveau pouvoir dans les premières discussions entre le CST et AMC. Au cours de la période à l'examen, le CST a monté des COA avec AMC, qui a participé à certains aspects du processus de planification. AMC a encouragé le MAE à demander l'élaboration d'un mécanisme de gouvernance en vue d'atténuer le risque que [traduction] « le CST décide, par lui-même, de lancer [redacted] et a ajouté que [redacted][70]. »

46. ~~(TS)~~ Des évaluations internes préliminaires d'AMC se démarquent du mandat touchant le renseignement étranger du CST, qui répond aux priorités en matière de renseignement approuvées par le Cabinet[71], et rendent bien l'essence de cet écart par l'énoncé suivant :

> **citation d'AMC concernant une discussion sur les objectifs et priorités stratégiques des cyberopérations** [redacted]

[66] Par exemple, le BCP et SP sont responsables de différents aspects des objectifs et priorités en matière de sécurité nationale, tandis que le MDN est responsable des priorités du Canada en matière de politique de défense. Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Chapitre 3 : Examen du processus d'établissement des priorités en matière de renseignement », *Rapport annuel 2018*, 8 avril 2019.
[67] Autorisation ministérielle de COA, 2019-2020, paragraphe 29; et Autorisation ministérielle pour la COD, 2019-2020, paragraphe 3.
[68] AMC, commentaires sur l'exactitude des faits, 18 août 2021.
[69] *Loi sur le CST*, paragraphe 34(4).
[70] AMC, [redacted] mémoire, 21 août 2019, p. 4.
[71] *Ibid*. De plus, le volet du renseignement étranger du mandat du CST, tel qu'il est décrit à l'article 16 de la *Loi sur le CST*, demande au CST de fournir des renseignements étrangers en conformité avec les priorités du gouvernement fédéral en matière de renseignement.

[redacted][72]

47. ~~(TS)~~ Dans un autre cas, AMC a décrit l'établissement de telles priorités comme étant [traduction] « une question importante qui n'a pas encore été réglée avec le CST » et a expliqué qu'à ce moment un organisme dont le mandat touchait notamment la cyberopération devrait décider s'il s'agit du bon outil pour atteindre un objectif en particulier[73]. AMC a expliqué que ses représentants avaient ultimement accepté d'aller de l'avant sans se consacrer davantage à ce sujet pour autant qu'un mécanisme de gouvernance était mis en place avec le CST[74].

48. ~~(TS)~~ Dans ce contexte, le paragraphe 34(4) de la *Loi sur le CST* exige que les objectifs d'une cyberopération ne puissent pas être raisonnablement atteints d'une autre manière et que les cyberopérations répondent aux priorités dans divers domaines. Étant donné ces exigences, l'OSSNR indique que les ministères fédéraux, et non seulement le CST et AMC, peuvent fournir des indications pertinentes sur d'autres possibilités ou des activités en cours qui pourraient atteindre les objectifs en question.

49. ~~(TS)~~ De plus, AMC a souligné le fait que le Cabinet établissait les besoins permanents en matière de renseignement (BPR) qui limitent et dirigent plus précisément les activités de collecte de renseignements étrangers du CST[75]. À ce sujet, le CST a répondu que [traduction] « ces discussions ont conduit le CST et AMC à accepter de commencer par une autorisation ministérielle comportant [redacted] appuyée par une structure de consultation et un cadre de gouvernance entourant les COA/COD du CST et d'AMC[76]. »

50. ~~(TS)~~ Selon l'OSSNR, la *Loi sur le CST* et l'AM de COA établissent directement un lien entre les COA et les grands objectifs et priorités du gouvernement du Canada qui touchent directement les mandats de ministères comme le MDN, le BCP, le SCRS et SP, en plus de ceux du CST et d'AMC. Il ne suffit pas au CST de déclarer qu'une AM et ses activités connexes concordent avec ces priorités sans élaborer ou consulter d'autres parties, étant donné que le MDN, le BCP et SP sont responsables des priorités stratégiques du Canada en matière de sécurité nationale et de défense ou en assurent la coordination. Ces ministères et organismes seraient les mieux placés pour offrir des commentaires et une confirmation concernant l'alignement d'une COA sur les objectifs du Canada afin d'atténuer les risques que peuvent poser ces opérations et de contribuer à la responsabilisation globale de ces opérations.

51. (NC) [redacted] **concerne des sujets du GC liés à la sécurité nationale** [redacted] Par conséquent, le processus de gouvernance appelle l'inclusion, ou à tout le moins leur consultation, d'autres ministères dont les mandats sont de chapeauter les grands objectifs stratégiques

[72] AMC, « Pre-briefing for 9 May CSE/GAC ADM meeting », présentation, diapositive 6. Soulignement ajouté par l'OSSNR.
[73] [redacted] Par exemple, « si une cyberopération sert à contrecarrer une cyberattaque en cours contre un ministère, la décision serait prise par le Centre canadien pour la cybersécurité. Si la cyberopération sert à répondre à de l'ingérence dans les élections, la décision est prise par le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections. »
[74] AMC, commentaires sur l'exactitude des faits, 18 août 2021.
[75] *Ibid.*, p. 4.
[76] CST, « RE: ACO/DCO Governance Review: RFI-08 », réponse, 12 mars 2021, Q1.

du Canada. Ainsi, les grands intérêts du Canada et les risques possibles seraient suffisamment examinés et transparaîtraient dans l'élaboration des COA.

(NC) Conclusion nº 3 : Le cadre de gouvernance actuel ne comprend pas de mécanisme permettant de confirmer la conformité d'une cyberopération active (COA) aux grandes priorités stratégiques du gouvernement du Canada, comme le demandent la *Loi sur le CST* et l'autorisation ministérielle. Bien que les objectifs et priorités ne relèvent pas uniquement du CST et d'AMC, ceux-ci dictent les COA sans l'apport de la communauté globale du gouvernement du Canada prenant part à la gestion des objectifs généraux du Canada.

(NC) Recommandation nº 3 : L'OSSNR recommande que le CST et AMC établissent un cadre de consultation des intervenants clés, notamment, le conseiller à la sécurité nationale et au renseignement auprès du premier ministre et les autres ministères concernés, dont les mandats touchent les cyberopérations actives proposées afin que celles-ci s'harmonisent aux grandes priorités stratégiques du gouvernement du Canada et que les exigences énoncées dans la *Loi sur le CST* soient respectées.

Seuil pour la conduite de COD préventives

52. ~~(TS//SI)~~ Le CST établit une différence entre les COD menées en réponse à une cybermenace et les COD préventives visant à empêcher la concrétisation d'une cybermenace[77]. De plus, le CST et AMC ont discuté de la nature de ces opérations, notamment qu'elles se trouvaient dans le spectre des opérations en aval et en amont. Notamment, dans le cas des COD, **concerne des opérations du CST** [redacted][78].

53. ~~(TS)~~ Le CST a expliqué que le lancement d'une COD [traduction] « exige une preuve que la menace représente une source potentielle de dommage à une institution fédérale ou à une infrastructure de l'information ou de l'information électronique précise[79] ». Selon le CST, il n'est pas nécessaire qu'une infrastructure soit compromise avant que soit lancée une COD. Il faut simplement pouvoir établir la preuve d'un lien entre une menace de compromission et l'infrastructure[80].

54. ~~(TS)~~ En même temps, le CST ne dispose pas encore des moyens de faire la distinction entre ce type de COD et une COA[81], étant donné que des discussions entre AMC et le CST indiquaient qu'une COD pouvait ressembler à une COA si la première est menée en amont[82]. Contrairement aux COA, qui demandent le consentement du MAE et la participation exhaustive d'AMC tout au long du processus de planification, les COD ne requièrent qu'une consultation auprès du MAE. Sans l'établissement d'un seuil clair pour une COD menée en amont, il est possible que la participation d'AMC à une opération qui s'apparente (ou corresponde) à une COA soit insuffisante, [redacted]

[77] CST, « CSE's Evolving Approach to Cyber Operations », présentation, mars 2020, p. 5.
[78] Toutefois, il est quand même interdit de mener une COD contre un Canadien, une personne au Canada ou sur l'infrastructure mondiale de l'information au Canada.
[79] CST, commentaires sur l'exactitude des faits, 13 août 2021.
[80] *Ibid.*
[81] CST, « GAC-CSE Meeting, April 30, 2019 », dossier de réunion.
[82] CST, « GAC-CSE Meeting, May 7, 2019 », dossier de réunion.

55. (NC) Dans notre examen ultérieur, nous porterons une attention particulière à la nature des COD préventives planifiées ou exécutées afin de déterminer si elles constituent ou non des COA.

(NC) Conclusion nº 4 : Le CST et AMC n'ont pas mis en place de seuil permettant de définir et de distinguer les cyberopérations actives et les cyberopérations défensives, une lacune qui pourrait mener à une participation insuffisante de la part d'AMC advenant qu'une opération soit considérée à tort comme étant défensive.

(NC) Recommandation nº 4 : L'OSSNR recommande que le CST et AMC instaurent un seuil qui permette de distinguer une cyberopération active d'une cyberopération défensive préventive, et que ce seuil soit fourni au ministre de la Défense nationale dans les autorisations ministérielles applicables.

Collecte de renseignement dans le cadre d'une cyberopération

56. (NC) Aux termes du paragraphe 34(4) de la *Loi sur le CST*, le MinDN ne peut délivrer l'autorisation que s'il conclut qu'aucune information ne sera acquise au titre de l'autorisation, sauf conformément à une autorisation délivrée en vertu des paragraphes 26(1), 27(1) ou (2), ou 40(1). Les AM pour les COA/COD délivrées pendant la période à l'examen témoignent de cette restriction[83]. Ces AM et leurs demandes correspondantes mentionnent seulement que les AM entourant les renseignements étrangers serviront à acquérir de l'information en *appui* des activités de COA/COD. Elles énoncent aussi clairement qu'aucune information ne sera acquise dans le cadre des activités de COA/COD autorisées par l'AM de COA[84].

57. ~~(TS)~~ Cependant, les AM et les demandes à l'appui ne décrivent pas l'intégralité des activités de collecte d'information découlant des COA/COD. D'après les politiques du CST, le Centre peut encore recueillir de l'information [redacted] tant que l'activité est menée au titre d'une autre AM. Le CST a expliqué que les AM pour les COA/COD ne peuvent servir de fondement à la collecte de renseignements, mais que [redacted] **concerne des opérations du CST** [redacted][85]. [redacted] Par exemple, [redacted] tout en s'appuyant sur l'autorisation liée aux renseignements étrangers pour [redacted] conformément aux priorités en matière de renseignement du gouvernement du Canada[86].

58. ~~(TS)~~ Même si la *Loi sur le CST* autorise le CST à acquérir de l'information au titre d'AM de collecte, l'OSSNR est d'avis que la politique du CST permettant la tenue d'activités de collecte au titre d'AM distinctes pendant la tenue de cyberopérations n'est pas énoncée clairement dans les AM pour les COA/COD. Plutôt, la collecte d'information fait partie des interdictions dans l'AM de COA, donnant l'impression que la collecte ne peut avoir lieu peu importe les circonstances. Par conséquent, l'OSSNR

[83] Autorisations ministérielles pour les COA et les COD, 2019-2020, paragraphe 2(c).
[84] Autorisations ministérielles pour les COA et les COD, 2019-2020, paragraphe 11(g).
[85] CST, « Information Sharing and Use Across Aspects of CSE's Mandate », réponse à la DI-6, 16 octobre 2020.
[86] SP, « Cyber Operations Chapter », section 3.5.

souligne que le libellé de l'AM de COA ne traduit pas en toute transparence les politiques internes du CST.

59. ~~(TS//SI)~~ Le CST a expliqué que [redacted] durant une COA/COD[87]. En outre, l'OSSNR a appris d'un expert du CST qu'un [redacted] précis qui énonce en détail les activités à réaliser dans le cadre de l'opération oriente chaque COA/COD. [redacted]

60. ~~(TS)~~ Étant donné la politique du CST permettant la tenue simultanée de la collecte et de cyberopérations [redacted] l'OSSNR examinera minutieusement les rôles et responsabilités [redacted] participant aux COA/COD, ainsi que les aspects techniques de l'utilisation des systèmes du CST à l'appui des COA/COD lors de son examen ultérieur des opérations qu'a menées le CST jusqu'à présent.

(NC) Conclusion n° 5 : Les politiques internes du CST qui portent sur la collecte d'information dans le cadre de cyberopérations ne sont pas décrites avec exactitude dans les autorisations ministérielles pour les cyberopérations actives et défensives.

(NC) Recommandation n° 5 : L'OSSNR recommande que le CST, dans ses demandes présentées au ministre de la Défense nationale, décrive avec exactitude la possibilité que, dans le cadre de cyberopérations actives et défensives, des activités de collecte se déroulent au titre d'autorisations distinctes.

Gouvernance interne du CST

61. (NC) L'OSSNR a décidé d'évaluer dans quelle mesure les processus de gouvernance interne prenaient suffisamment en compte les éléments essentiels à la planification et à l'exécution des opérations, et de savoir si les intervenants appelés à prendre part aux COA/COD (c.-à-d. AMC et [redacted]) étaient précisément au fait des paramètres et des contraintes s'appliquant aux cyberopérations.

62. ~~(TS)~~ Pendant le déroulement de l'examen, le CST donné suite aux exigences applicables en vertu de la *Loi sur le CST* et des AM en mettant en place divers mécanismes internes de planification et de gouvernance. Ces mécanismes visaient les documents et les mesures stratégiques de haut

[87] [redacted] CST, réponse à la DI-05, 26 janvier 2021, Q2.

[88] Entrevue avec un expert du CST, 14 janvier 2021.

niveau, mais aussi chacune des [redacted] opérationnelles, [documents/méchanismes] de chacune des COA/COD.

Gouvernance des opérations

63. ~~(TS)~~ Comme il a été décrit plus tôt[89], lorsqu'il s'agit d'approuver chacune des COA/COD, le CST s'appuie sur divers documents de planification et de gouvernance, notamment, les [redacted] Dans un premier temps, le CST élabore le [redacted] une COA/COD donnée. Par la suite, le CST crée un [redacted] dans lequel on fait état des risques dont il faut tenir compte pendant le déroulement de la COA/COD. De plus, le [redacted] et le [redacted] comprennent des champs portant sur les interdictions énoncées dans la *Loi sur le CST*[90]. Dès lors qu'une cible a été choisie, la [redacted] tient lieu de document de gouvernance définitif, jusqu'à l'établissement des [redacted] des COA/COD.

64. ~~(TS)~~ Semblablement aux AM pour les COA/COD et en guise de plan initial, le [redacted] consiste généralement en une approbation préalable de l'ensemble des activités et de [redacted] Il est ensuite perfectionné et développé dans le cadre du processus de [redacted] Du point de vue de l'OSSNR, [redacted] **concerne des opérations du CST** [redacted]

65. ~~(TS)~~ De fait, le [redacted] **concerne des opérations du CST** [redacted] mais aussi les éléments opérationnels qui, selon l'OSSNR, représentent bien plus que la simple [redacted] dans la mesure où celle-ci énonce aussi les aspects essentiels de la planification opérationnelle. [redacted] Enfin, la [redacted] décrit en détail les modalités de [redacted][92]. Or, même si [redacted] la [redacted] pourrait jouir d'un seuil d'approbation moins élevé que celui du [redacted][93].

66. ~~(TS)~~ Dans l'ensemble, l'OSSNR accueille favorablement le fait que le CST a élaboré des

[89] Consulter les paragraphes 17 à 20.
[90] La Loi circonscrit les activités des COA/COD : elles ne doivent jamais être dirigées contre des Canadiens ou contre des personnes se trouvant au Canada; elles ne doivent jamais porter atteinte aux dispositions de la Charte canadienne des droits et libertés; et elles ne doivent jamais viser un segment de l'infrastructure mondiale d'information (IMI) se trouvant en territoire canadien. *Loi sur le CST*, alinéa 22(2)a).
[91] Par exemple, le [redacted] indique simplement [redacted] Consulter [redacted] du CST [redacted] p. 1.
[92] [redacted] CST [redacted] En outre, le [redacted] énonce en termes généraux les principes sur lesquels s'appuient [redacted] mais la [redacted] contient tout de même des éléments particuliers qui en disent davantage sur les directives opérationnelles.
[93] Présentation du CST, « Séance d'information sur les cyberopérations actives et défensives à l'intention de l'OSSNR », mars 2020, diapositive 3. « Présentation du CST, Séance d'information à l'intention de la chef du CST [redacted] p. 9.

procédures et documenté la planification opérationnelle visant les activités des COA/COD, conformément aux exigences énoncées dans l'EPM. Toutefois, les nombreux documents portant sur la gouvernance s'appliquant aux COA/COD visent divers auditoires et ont diverses fonctions. En l'occurrence, les informations essentielles sont réparties dans plusieurs de ces documents au lieu d'être réunies dans une structure centrale, que les intervenants et les décideurs concernés seraient appelés à consulter, voire à évaluer. L'OSSNR estime que la pluralité des documents faisant état de la gouvernance entraînerait des chevauchements et des dédoublements donnant lieu à une ambiguïté désavantageuse au sein même d'un plan opérationnel devant guider les COA/COD. Ainsi, à l'occasion de son prochain examen, l'OSSNR procédera à l'évaluation de la structure de gouvernance telle qu'elle aura été appliquée, d'ici là, aux opérations.

(NC) Conclusion nº 6 : Le processus de [redacted] lequel a lieu une fois que les documents de planification ont été approuvés, contient des informations pertinentes pour les plans opérationnels généraux du CST. Or, il est arrivé que la [redacted] contienne des informations essentielles qui n'apparaissaient pas dans ces autres documents, bien que cette présentation soit approuvée à un niveau de gestion inférieur.

(NC) Recommandation nº 6 : L'OSSNR recommande que le CST inscrive toutes les informations pertinentes – y compris les informations sur le ciblage et le contexte – dans tous les plans opérationnels qui sont produits dans le cas d'une cyberopération ainsi que dans tout document soumis à l'attention d'AMC.

Formation sur le nouveau cadre pour les cyberopérations

67. ~~(TS)~~ Les autorisations ministérielles visant les COA et les COD permettent aux catégories de personnes suivantes de mener des activités COA/COD : **concerne la politique opérationnelle du CST** [redacted] Les AM exigent également que ces [traduction] « personnes ou catégories de personnes appuient les opérations du CST et favorisent les intérêts du Canada en matière de renseignement; elles exigent également que ces personnes ou catégories de personnes aient démontré une compréhension approfondie des exigences juridiques et stratégiques applicables[94]. »

68. ~~(TS)~~ Soucieux de la formation et de l'orientation de son personnel opérationnel au sujet des nouvelles exigences juridiques et stratégiques, le CST a déclaré – relativement à une opération particulière – que :

> [TRADUCTION] « Les activités opérationnelles entreprises [redacted] lesquels sont tenus de suivre des formations complètes et continues sur les fonctions et les tâches qu'ils sont appelés à exercer, mais aussi sur les politiques et les exigences en matière de conformité qui s'appliquent à leurs rôles respectifs. De plus, [redacted] ont été formés, sont tenus responsables des activités qu'ils réalisent et respectent les exigences en matière de production de rapports sur la conformité. En outre, [redacted] qui participent aux activités [redacted] ont

[94] Autorisations ministérielles COA et autorisations ministérielles COD, 2019-2020, paragr. 9. Guillemets ajoutés par l'OSSNR.

préalablement reçu le matériel opérationnel permettant de veiller à ce que les conditions d'opération énoncées dans la présente soient comprises et strictement observées[95]. »

69. ~~(TS)~~ Enfin, le CST a indiqué à l'OSSNR [traduction] « qu'avant l'adoption de la nouvelle loi, le CST fournissait, virtuellement et en présentiel, des séances d'information sur les nouveaux pouvoirs du CST à tous les membres de l'effectif du Centre. Des séances d'information personnalisées étaient également fournies aux équipes opérationnelles ». Au nombre de ces séances, on a pu compter des conférences, des séances de question avec le chef-adjoint, Politiques et Communication, ainsi que d'autres types de présentations préparées par les équipes des politiques du CST[96]. Toutefois, l'OSSNR note que ces séances de formation, qui comportent nombre d'informations générales, ne sont pas axées sur les opérations et ne mettent pas à l'épreuve les connaissances que les employés ont nouvellement acquises concernant le nouveau cadre juridique régissant les opérations.

70. ~~(TS)~~ Compte tenu des exigences et des assurances énoncées plus haut, l'OSSNR s'attendait à constater que les employés du CST qui fournissent du soutien aux COA/COD disposent d'une formation effective qui soit suffisante pour acquérir une compréhension approfondie des responsabilités qui leur incombent en considération des nouveaux pouvoirs, mais aussi des nouvelles contraintes que la loi leur impose; et pour mettre cette compréhension en pratique pendant le déroulement des COA/COD.

71. ~~(S//SI)~~ Dans ce contexte, le CST a mené des exercices pratiques ayant pour objet, entre autres, de présenter [certains employés] les premières étapes du processus de préparation des AM, de leur donner l'occasion de rédiger des AM et de tester la viabilité fonctionnelle du cadre des AM. Durant les exercices, [l'employé susmentionné] n'avaient pas le droit de demander conseil auprès des responsables des affaires juridiques ou stratégiques, permettant ainsi aux gestionnaires d'observer les résultats appelés à se manifester naturellement. Or, l'OSSNR remarque un point essentiel au sujet de cet exercice :

> [TRADUCTION] « [redacted] se sont montrés réticents à l'égard du besoin de recourir à plusieurs AM pour soutenir les objectifs de mission. Des directives et de la formation en matière de politiques seront nécessaires pour rendre [redacted] aptes à connaître les autorisations qui régissent leurs interventions dès lors qu'ils prennent part aux opérations réalisées dans le cadre de diverses missions et selon les termes des AM connexes. Ces directives et cette formation doivent également tenir compte du fait que les informations collectées en vertu de diverses AM pourraient être assujetties à certaines exigences en matière de gestion des données[97]. »

72. ~~(TS)~~ Le CST a indiqué que [certains employés] recevaient les éléments de connaissance concernant les autorités juridiques, les exigences et les interdictions s'appliquant aux COA et aux COD pendant des réunions de planification et à la lecture de documents opérationnels[98]. Or, à l'occasion d'une entrevue avec un expert du CST [redacted] l'OSSNR a appris que la formation offerte sur les autorités juridiques, les exigences et les interdictions [redacted] L'expert en question a également dit que les intervenants qui auraient des questions concernant la gouvernance devraient [redacted] **concerne des opérations du CST** [redacted][99].

[95] [redacted] CST, [redacted] Soulignements ajoutés par l'OSSNR.
[96] Réponse du CST à la DI-7, 26 février 2021.
[97] Document du CST, « MA Modeling Exercise – report to ExCom [initials] Comments Nov 21 2018 ([initials] comments) », p. 1. Soulignements ajoutés par l'OSSNR.
[98] Réponse du CST à la DI-7, 5 février 2021.
[99] Entrevue avec un expert du CST, 14 janvier 2021.

73. ~~(TS)~~ À l'OSSNR, on ne sait trop s'il existe des exigences suivant lesquelles [redacted] sont tenus de posséder une profonde compréhension des paramètres définis pour une COA/COD dans un [redacted] De fait, [redacted] Par exemple, lorsqu'on l'a questionné au sujet de son degré d'aisance à exécuter ses fonctions en vertu de diverses AM, [redacted] énoncés dans le [redacted] Le CST ajoute que [redacted] sont élaborés à partir du [redacted][100]. Or, comme l'indique [redacted] Par conséquent, l'OSSNR estime que s'ils ne se concentrent que sur le contenu du [certain document/méchanisme] risquent de ne pas avoir une compréhension suffisante des paramètres et des restrictions s'appliquant à l'ensemble de l'opération[101].

74. ~~(TS)~~ Les AM qui autorisent l'exécution des COA/COD imposent une condition aux employés du CST impliqués dans l'exécution desdites COA/COD : celle de posséder une compréhension approfondie des exigences juridiques et stratégiques régissant leurs interventions. Les AM et les documents de planification opérationnelle contiennent des informations essentielles concernant les paramètres qui déterminent les pouvoirs s'appliquant, de façon générale, à la conduite des COA/COD, mais aussi des opérations particulières. Ainsi, l'OSSNR affirme qu'il est de prime importance que les employés travaillant sur un aspect de l'exécution des COA/COD reçoivent des séances de formation leur permettant de bien connaître les exigences et les limites s'appliquant à leurs interventions respectives, lesquelles sont énoncées dans le [redacted] et la [redacted] Enfin, [certains employés] pourraient subir des tests visant à mesurer leur degré de compréhension des AM et des contraintes imposées à certaines opérations.

(NC) Conclusion no 7 : Le CST a prodigué à ses employés des formations générales leur permettant d'acquérir une connaissance des nouveaux pouvoirs autorisant la conduite de cyberopérations actives et défensives (COA/COD). Toutefois, il y a lieu de croire que les employés directement impliqués dans les COA/COD n'auraient une compréhension suffisante ni des éléments ayant trait aux pouvoirs légaux nouvellement acquis par le CST ni des paramètres régissant l'application de ces pouvoirs.

(NC) Recommandation nº 7 : L'OSSNR recommande que le CST offre un programme de formation structuré aux employés prenant part à l'exécution des cyberopérations actives et défensives (COA/COD). Ce faisant, le CST s'assurerait que lesdits employés possèdent une connaissance adéquate des pouvoirs légaux, des exigences et des interdictions stipulées dans les autorisations ministérielles.

Cadre de mobilisation entre le CST et AMC

75. (NC) Étant donné l'exigence législative selon laquelle le MAE doit donner son approbation ou être consulté en ce qui a trait aux COA/COD, l'OSSNR a cherché à déterminer si le CST avait élaboré un cadre propice à la mobilisation et à la consultation des représentants d'AMC pour les aspects communs de leurs mandats respectifs.

[100] Réponse du CST, « NSIRA FCO governance review : Response to RFI-7 », 5 février 2021, Q3.
[101] Entrevue avec un expert du CST, 14 janvier 2021.

Évaluation des risques liés à la politique étrangère par AMC

76. ~~(TS)~~ Lors de l'élaboration du cadre de consultation, AMC et le CST ont mis au point un mécanisme selon lequel AMC est appelé à donner son avis, voire son approbation avant le lancement d'une opération, et à évaluer les risques que celle-ci peut comporter en matière de politique étrangère. En réponse à une demande de consultation présentée par le CST, AMC est tenu de fournir, dans un délai de cinq jours ouvrables, une évaluation des risques liés à la politique étrangère (ERPE) visant à établir si [redacted] Il convient de souligner que l'ERPE ne constitue pas une approbation de l'opération; il ne s'agit que d'un mécanisme de consultation[102]. Pour orienter l'ERPE, le CST prépare un [document/méchanisme] à l'intention d'AMC résumant les divers aspects de l'opération[103]. Par ailleurs, c'est dans le cadre d'un examen subséquent que l'OSSNR vérifiera si l'échéancier fourni par le CST relativement à certaines opérations aura permis à AMD de mener des ERPE adéquates.

77. ~~(S)~~ Pour déterminer si une COA/COD [redacted] AMC doit considérer bon nombre de facteurs. Il faut notamment vérifier si la COA/COD est conforme à la position d'AMC par rapport aux normes internationales régissant le cyberespace et si elle contribue aux intérêts du Canada. AMC doit aussi tenir compte de [redacted]**concerne des sujets du GC liés à la sécurité nationale**[redacted][104]. Ces considérations sont présentées dans les mandats du Groupe de travail du CST-AMC, lesquels requièrent qu'AMC évalue :

- [redacted]
- la conformité au droit international et aux cybernormes;
- la cohérence sur le plan de la politique étrangère, notamment la conformité de l'opération aux priorités en matière de politique étrangère, de sécurité nationale et de défense (au-delà des [besoins permanents en matière de renseignement]);
- [redacted][105].

78. ~~(TS//SI)~~ Dans le contexte des exigences d'évaluation susmentionnées, AMC a expliqué à l'OSSNR que ses évaluations des risques posés par les opérations sur le plan de la politique étrangère n'étaient pas forcément exhaustives, étant donné qu'il évaluait déjà en détail les catégories d'activités autorisées par l'AM[106]. Cette approche en matière d'évaluation est perceptible dans [redacted] ERPE reçues par l'OSSNR, lesquelles concluaient que [redacted] ces opérations [redacted] sans toutefois fournir de précisions sur les facteurs susmentionnés[107]. Étant donné qu'elles fournissent l'assurance qu'une opération [redacted] et qu'elles sont requises aux termes de l'AM relative aux COA, les ERPE feront l'objet d'un examen détaillé dans le cadre du prochain

[102] CST et AMC, « Terms of Reference Governance Framework », document du Groupe de travail sur les COA/COD, p. 9.
[103] Toutefois, dans le cas de certaines opérations examinées par l'OSSNR, le CST a employé d'autres mécanismes pour consulter AMC, le [redacted] n'ayant été mis au point qu'à la fin de la période d'examen. Par exemple, dans le cadre de [redacted] le CST a fourni un document de synthèse de l'opération à AMC, aux fins de consultation. Voir le document du CST [redacted] Overview ».
[104] AMC, « Active Cyber Operations – Scenario Vignettes », 4 avril 2019, p. 1.
[105] CST-AMC, « CSE-GAC ACO/DCO Working Group Terms of Reference », septembre 2020, annexe 1, p. 7.
[106] AMC, réunion du 16 février 2021.
[107] Par exemple, dans l'ERPE pour [redacted] AMC note les [redacted] participant à la COD. [redacted] Voir AMC, « FPRA [redacted]

examen de l'OSSNR, lequel portera sur les opérations.

Conformité au droit international et aux cybernormes

79. (TS [redacted][108]. [redacted][109].

80. (NC [redacted] Le Parlement peut autoriser des violations du droit international, s'il le fait expressément[110]. Par exemple, à la suite de la décision dans X (Re) 2014 CAF 249, le Parlement a modifié la *Loi sur le SCRS* en adoptant le projet de loi C-44 en 2015[111]. Les nouvelles dispositions énonçaient clairement que le SCRS pouvait s'acquitter de ses fonctions au pays et à l'étranger, et qu'en vertu de nouvelles dispositions de la *Loi sur le CST,* un juge pouvait autoriser des activités à l'étranger afin de permettre au Service d'enquêter sur une menace pour la sécurité du Canada « sans égard à toute autre règle de droit »[112]. Conformément au libellé de la *Loi sur le CST,* les AM relatives aux COA/COD peuvent uniquement autoriser le CST à mener des activités « malgré toute autre loi fédérale ou loi d'un État étranger »[113]. Tel qu'énoncé dans la jurisprudence[114], ce libellé pourrait ne pas être suffisamment clair pour permettre au ministre d'autoriser la violation de règles coutumières du droit international.

81. (TS [redacted] les AM examinées par l'OSSNR énonçaient que les activités devaient être [traduction] « conformes aux obligations du Canada en matière de droit international »[115], et chaque AM exigeait que les activités du CST ne contreviennent pas aux obligations du Canada en la matière[116]. Ainsi, cela porte à croire que toutes les activités menées aux termes de l'AM sont conformes au droit international. Or, les documents de gouvernance rédigés par le CST et AMC, notamment le cadre de consultation, n'établissent pas les paramètres permettant d'évaluer la conformité des COA/COD avec les obligations du Canada en matière de droit international. Qui plus est, on ne précise pas les obligations légales internationales en fonction desquelles la conformité des COA/COD doit être évaluée. Dans son prochain examen, l'OSSNR évaluera dans quelle mesure les COA/COD menées par le CST et AMC se conforment au droit international.

82. (TS [redacted]) Dans le cadre de ses échanges avec l'OSSNR, AMC a

---

[108] [redacted] AMC note ce qui suit : [traduction] [redacted] AMC, commentaires sur l'exactitude des faits, 18 août 2021.

[109] Le CST a mentionné que dans son avis, [redacted] CST, commentaires sur l'exactitude des faits, 13 août 2021.

[110] *R. c. Hape*, 2007 CSC 26, à l'alinéa 39 [*Hape*]; *Nevsun,* aux alinéas 90 à 94. Par exemple, la *Loi sur le SCRS* autorise sans équivoque les infractions de lois internationales pour ce qui est des activités visées par l'article 16 et des mesures d'atténuation des menaces prises en vertu de mandats judiciaires par l'inclusion de libellés tels que « malgré toute autre loi » [paragr. 21(3) et 24)] et « sans égard à toute autre règle de droit » [paragr. 21(3.1) et 21.1(4)].

[111] Loi modifiant la *Loi sur le Service canadien du renseignement de sécurité et d'autres lois*, LC 2015, ch. 9.

[112] *Loi sur le SCRS*, paragr. 21(3.1) et 21.1(4).

[113] Paragr. 29(1) et 30(1), *Loi sur le CST.*

[114] *Hape*, à l'alinéa 39; *Nevsun,* aux alinéas 90 à 94.

[115] Demande au ministre de la Défense nationale relative aux cyberopérations actives, p. 1.

[116] Autorisation ministérielle concernant une COA, 2019-2020, alinéa 11(d).

fait mention de ses consultations interministérielles et internationales remontant à 2016 concernant le *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0)*[117], lequel a contribué à orienter les AM [redacted][118]. À la suite de ces consultations, AMC a créé un manuel qui traite de l'évaluation préliminaire du Canada visant des règles clés du droit international relatif au cyberespace, selon le *Tallinn Manual 2.0*. Bien qu'il ne s'agisse que d'une ébauche ne représentant pas la position définitive du Canada[119], l'analyse [traduction] « sert de fondement à des considérations juridiques approfondies[120] ». L'OSSNR n'a reçu aucun autre document décrivant la manière dont le Canada interprète le droit international relativement aux COA/COD.

83. (~~TS~~ [redacted] Par ailleurs, dans des documents fournis par AMC et le CST, on fait état de la nécessité d'examiner la légalité de chaque COA/COD envisagée. AMC a notamment relevé qu'il faudrait analyser les termes [traduction] « reconnus comme étant nuisibles » et « posant un risque pour la paix internationale et à la sécurité », et ce, dans le contexte de chaque COA/COD. [redacted][121]

84. ~~(TS)~~ AMC a expliqué avoir examiné chaque activité s'inscrivant dans les catégories autorisées afin de vérifier la conformité au droit international au stade d'élaboration de l'AM. Ainsi, il n'a mené qu'un examen sommaire de la conformité au droit international au stade de l'ERPE pour chaque opération[122]. AMC a mentionné que le manuel qu'il a créé ainsi que le *Tallinn Manual 2.0* ont été consultés à cet effet. D'après la teneur [redacted] ERPE examinées par l'OSSNR jusqu'à présent, on ne saurait dire dans quelle mesure le manuel ou l'analyse des normes volontaires de 2015 du Groupe d'experts gouvernementaux des Nations Unies (GEG de l'ONU) a orienté l'examen du niveau de risque de chaque opération[123], ou encore, si les conclusions d'AMC étaient conformes au droit international. Or, AMC conclut que les activités sont conformes au droit international sans toutefois fournir de justification.

85. (NC) L'OSSNR constate qu'en matière de cyberespace, le droit international en est à ses balbutiements, mais il reconnaît que le Canada et d'autres États continuent de développer et de peaufiner leur analyse juridique dans le domaine. Mener des COA/COD sans qu'elles aient d'abord fait l'objet d'analyses exhaustives et documentées comporte des risques considérables pour le Canada sur le plan juridique advenant qu'une opération viole le droit international. En fin de compte, pour être en mesure d'évaluer la conformité d'une opération au droit international, le CST et AMC devront approfondir leurs analyses des obligations légales du Canada[124]. L'OSSNR se penchera sur la légalité

---

[117] Le *Tallinn Manual 2.0* examine l'applicabilité de 154 règles coutumières du droit international relatif aux cyberopérations. Toutefois, il ne s'agit pas d'une source de droit. Le *Tallinn Manual 2.0* renferme les opinions d'un groupe d'experts internationaux réunis par le Centre d'excellence en cyberdéfense coopérative de l'OTAN, mais il ne représente pas les opinions de l'OTAN ou de ses États membres.

[118] AMC, « Annex to explanatory note for NSIRA », 5 mars 2020.

[119] AMC, document « Draft Deskbook – International Law Applicable to Cyber Operations », août 2019.

[120] AMC, « Annex to explanatory note for NSIRA », réponse à RFI-02, 5 mars 2020.

[121] [redacted]

[122] AMC, réunion du 16 février 2021.

[123] [redacted] L'OSSNR note qu'il s'agit de normes volontaires non contraignantes qui ne sont pas représentatives des obligations légales internationales du Canada.

[124] [redacted]

des COA/COD dans le cadre de son prochain examen.

(NC) Conclusion nº 8 : En ce qui concerne les cyberopérations actives et défensives, le cadre élaboré par le CST et AMC pour évaluer les obligations du Canada en matière de droit international manque de clarté et d'objectivité.

(NC) Recommandation nº 8 : L'OSSNR recommande que le CST et AMC fournissent une évaluation du régime légal international applicable à l'exécution des cyberopérations actives et défensives, et que le CST exige d'AMC qu'il procède à une évaluation juridique exhaustive de la conformité de chaque opération au droit international.

Communication bilatérale de l'information pertinente

86. ~~(TS)~~ AMC et le CST ont tous deux adopté des méthodes qui leur permettent d'évaluer les risques en fonction de certains facteurs. Cependant, ces types de risques ne sont pas absolus; ils dépendent d'une vaste gamme de facteurs qui évoluent au fil du temps et à mesure qu'émergent des renseignements nouveaux. Pour sa part, AMC compose avec des facteurs comme [redacted] **concerne des sujets du GC liés à la sécurité nationale** [redacted][125].

87. ~~(TS)~~ À l'heure actuelle, le CST et AMC ont adopté une méthode selon laquelle le CST compte sur l'information que lui transmet AMC pour demeurer au courant de tout changement lié aux risques sur le plan de la politique étrangère du Canada[126]. Toutefois, selon la méthode d'AMC susmentionnée, les risques d'une opération peuvent s'accroître à mesure qu'on obtient des renseignements sur [redacted] ou sur les répercussions possibles de l'opération au-delà d'un [redacted][127]. Pour sa part, le CST semble surtout se concentrer sur les changements touchant les risques opérationnels, [qui sont découverts à un certain moment et d'une certaine manière] [redacted][128]. Il s'agit d'un mécanisme à sens unique qui ne tient pas compte d'autres facteurs [redacted]

88. ~~(TS//SI)~~ Dans ce contexte, le CST a expliqué qu'une COA/COD consistait en [redacted] **concerne des opérations du CST** [redacted][129], et que par conséquent, [redacted][130]. Le CST a également mentionné que [redacted], et que les activités

---

[redacted] AMC a aussi mentionné qu'il consoliderait son analyse juridique qui remonte à une déclaration publique communiquée plusieurs années auparavant. La publication de l'analyse juridique est prévue pour la fin de 2021. AMC, commentaires sur l'exactitude des faits, 18 août 2021.

[125] CST-AMC, « ACO/DCO Working Group Terms of Reference », document, septembre 2020, annexe 1, p. 7.

[126] CST, « RFI-07 Q7 », 5 février 2021. Voir aussi : AMC, « NSIRA Deck », février 2021, p. 7 et CST-AMC, « CSE-GAC ACO/DCO Working Group Terms of Reference », septembre 2020, p. 5.

[127] L'OSSNR constate qu'AMC a maintes fois soulevé que les répercussions [redacted] pouvaient représenter [redacted] Voir AMC, « Risks and MINA basis of consent », courriel, 19 juin 2019; et AMC, « ACO FP considerations thoughts », courriel, 30 avril 2019.

[128] CST, « RFI-07 Q7 », 5 février 2021.

[129] CST, « RFI-07 Q7 », 5 février 2021.

[130] Un expert en la matière du CST a aussi soutenu que [redacted] Consulter « Interview with CSE subject-matter expert », 14 janvier 2021.

subséquentes peuvent être modifiées au besoin, en fonction de l'information obtenue pendant l'opération en cours[131]. [redacted]

89. ~~(TS//SI)~~ Dans ce contexte, l'OSSNR a examiné des opérations devant se dérouler sur une période donnée, dont une COD où le CST devait entreprendre des **concerne des opérations du CST** [redacted][132]. Dans le cadre d'une autre COA, le CST [redacted][133]. Dans sa description de l'opération à AMC, le CST a mentionné que de telles activités s'étendraient sur un certain laps de temps [redacted][134].

90. ~~(TS)~~ **concerne des opérations du CST** [redacted] tire parti de [redacted] des COA/COD [redacted] l'OSSNR estime qu'il faudrait mettre en place un mécanisme de notification bidirectionnel permettant de réévaluer les risques liés à une COA/COD, que ces risques soient découverts avant la mise en œuvre de l'opération ou pendant son exécution.

91. ~~(TS)~~ Enfin, en ce qui a trait au processus de gouvernance interne du CST, AMC a un rôle à jouer dans [document/méchanisme] D'ailleurs, AMC a indiqué que les objectifs, [redacted] associés aux opérations constituaient des renseignements qu'il incombe au CST de fournir aux fins de l'évaluation des risques pour la politique étrangère[135]. L'OSSNR a constaté que le [redacted][136]. L'OSSNR note qu'AMC devrait avoir accès à ces détails, car ils servent de contexte important à son examen, d'autant plus qu'AMC indique dans ses conclusions que les activités étaient conformes à [redacted]

(NC) Conclusion nº 9 : Le CST s'attend à ce qu'AMC l'avise de tout changement à la politique étrangère, mais n'accorde pas assez d'importance à la nécessité de faire part à AMC des autres risques pouvant survenir au cours d'une opération. En outre, des informations essentielles à l'évaluation d'AMC visant les risques pour la politique étrangère ne figurent pas dans la documentation que le CST utilise pour mobiliser AMC aux fins d'une opération. Ainsi, il se peut que le cadre de consultation actuel n'incite pas le CST à communiquer suffisamment d'information pour permettre à AMC d'évaluer les risques pour la politique étrangère et de gérer

---

[131] CST, commentaires sur l'exactitude des faits, 13 août 2021.
[132] CST, [redacted] p. 4.
[133] [redacted] CST, [redacted] p. 2 et 3.
[134] CST, « RE: URGENT: Heads up [redacted] courriel, [redacted]
[135] « CSE-GAC Senior Management Team (SMT) », compte rendu des discussions, 22 novembre 2019. Voir aussi « GAC-CSE Meeting », compte rendu de réunion, 30 avril 2019.
[136] CST, [redacted] Par exemple, la [redacted] explique [redacted] ce que le MAE a souligné à titre de limitation qui confirme [redacted] Or, dans la documentation utilisée pour informer AMC, on ne fait que répéter la formulation de l'AM concernant cette condition. Dans un autre cas, [redacted] Voir CST, [redacted] p. 1.

les risques qui se présentent au cours d'une cyberopération.

(NC) Recommandation nº 9 : L'OSSNR recommande que le CST et AMC s'échangent toute l'information pertinente et se tiennent au courant de tous les nouveaux développements ayant une incidence sur l'évaluation des risques associés aux cyberopérations, et ce, tant au stade de la planification qu'à celui de l'exécution.

V CONCLUSION

92. (NC) Le présent rapport fait suite au premier examen de l'OSSNR portant sur les nouveaux pouvoirs conférés au CST pour la conduite de COA/COD et illustre l'évolution de la structure de gouvernance du CST et d'AMC s'appliquant auxdites COA/COD. Le CST est autorisé à mener ce type d'opération depuis 2019, bien que l'examen ait permis de constater que les deux organismes avaient commencé à conceptualiser le régime de gouvernance avant l'entrée en vigueur de la *Loi sur le CST*. L'OSSNR reconnaît qu'à ce jour, le CST a élaboré une structure de gouvernance complète et salue son implication dans l'élaboration d'un cadre de consultation avec AMC, cadre dans lequel sont définis les rôles et les responsabilités de chacune des organisations.

93. (NC) Toutefois, le CST pourrait apporter des améliorations dans l'ensemble de la structure de gouvernance sur le plan de la transparence et de la clarté, pour ce qui a trait à la planification des COA/COD – particulièrement lors des premières étapes – en établissant, dans les AM concernées, des paramètres clairs s'appliquant aux catégories d'activités et aux groupes de cibles qui pourraient être concernés par des COA/COD. De plus, l'OSSNR estime que la préparation des cyberopérations pourrait tirer parti de consultations auprès d'autres ministères responsables des priorités et objectifs stratégiques du Canada en matière de sécurité nationale et de défense. Enfin, le CST et AMC devraient définir en quoi consiste une COD et établir un seuil applicable à la conduite des COD préventives, ce qui garantirait une participation appropriée d'AMC dans le cadre des opérations.

94. (NC) Sur le plan opérationnel, le CST et AMC devraient veiller à ce que le degré de conformité au droit international de chacune des opérations soit évalué et documenté. Pour ce qui concerne le CST, celui-ci devrait s'assurer que l'information essentielle à l'évaluation des risques posés par la conduite d'une opération soit normalisée et incluse dans tous les documents sur la gouvernance, et qu'elle soit mise à la disposition des intervenants appelés à prendre part à l'élaboration et à l'approbation des COA/COD – y compris AMC. En dernière analyse, le CST devrait s'assurer que son personnel opérationnel ait une excellente connaissance du nouveau cadre légal et de ses modalités d'application aux diverses opérations.

95. (NC) Certes, le présent examen s'est concentré sur les structures de gouvernance en vigueur pour ce qui concerne les COA/COD, mais il faut savoir qu'il sera encore plus important de voir comment ces structures sont appliquées et observées dans la pratique. Nous avons déjà formulé plusieurs commentaires concernant l'information contenue dans les documents qui ont été produits à ce jour en matière de gouvernance mais, à l'occasion d'un prochain examen portant sur les COA/COD, nous nous pencherons plutôt sur la façon dont les dispositions énoncées dans ces documents sont concrètement mises en œuvre.

ANNEXE A : Types de COA/COD


[redacted]

Figure 1 : Divers type de cyberopérations. Source : documents d'information du CST

	CYBEROPÉRATIONS DÉFENSIVES	CYBEROPÉRATIONS ACTIVES
Activités autorisées	▪ Obtenir l'accès à une part de l'infrastructure mondiale d'information. ▪ Installer, maintenir, copier, distribuer, rechercher, modifier, interrompre, supprimer ou intercepter quoi de ce soit dans l'infrastructure mondiale de l'information ou par son entremise pour atteindre un objectif qui ne pourrait pas être raisonnablement atteint par d'autres moyens. ▪ Prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète de l'activité. ▪ Mener toute autre activité qui est raisonnable dans les circonstances et est raisonnablement nécessaire pour faciliter l'exécution des activités ou des catégories d'activités visées par l'autorisation ministérielle.	
Approbation ministérielle	▪ Approbation du MinDN et **consultation** auprès du MAE.	▪ Approbation du MinDN et **consentement** ou demande du MAE.
Finalité	▪ Appliquer des mesures en ligne contribuant à la protection de l'information électronique et des infrastructures de l'information d'importance pour le gouvernement du Canada.	▪ Endommager, perturber, influencer ou contrer les capacités de tout personne, organisation ou État étrangers.
Auteur de menace/ Ensemble de cibles	▪ Dirigées contre des menaces pour les systèmes du gouvernement ou les systèmes d'importance, quelque soit l'auteur de menace. **Une fois qu'il est certain que l'entité visée n'est pas un Canadien, une personne se trouvant au Canada ou l'IMI sur le territoire canadien.	▪ Dirigées contre des cibles particulières conformément aux termes d'une autorisation ministérielle. **Une fois qu'il est certain que l'entité visée n'est pas un Canadien, une personne se trouvant au Canada ou l'IMI sur le territoire canadien.
Résultat	▪ Conçues dans le but de stopper ou de prévenir les menaces dirigées contre les infrastructures fédérales ou désignées comme étant d'importance, suivant des moyens jugés justes et adaptés en fonction desdites menaces.	▪ Réalisées dans le but d'atteindre un objectif en matière d'affaires internationales, de défense ou de sécurité suivant des moyens jugés justes et adaptés aux circonstances

Figure 2 : Distinctions entre les COA et les COD. Source : documents d'information du CST

ANNEXE B : COA et COD (2019-2020)

ANNEXE C : Cadre de travail pour le CST et AMC

Groupe interministériel	Équipe de la haute direction (EHD) du CST-AMC	Groupe de travail des DG du CST-AMC sur les COA/COD[137]	Niveau des SMA[138]
Coprésidents	Coprésidents de l'EHD : CST, DG, [redacted] AMC, DG, Direction générale du Renseignement	Coprésidents : CST, DG [redacted] AMC, DG Direction générale du Renseignement Composé, notamment, de membres (niveau des DG) de l'EHD et de membres de leurs équipes de soutien respectives.	Coprésidents : CST, chef adjoint, SIGINT AMC, SMA (directeur politique) Sécurité internationale
Rôles et responsabilités	Échange de renseignements sur les priorités et plans de chacun des ministères ainsi que sur les sphères de collaboration.	Relevant de l'EHD, cette entité a été établie pour exercer un mandat de collaboration visant les questions relatives aux COA/COD. Mise en œuvre du cadre de gouvernance associé aux AM visant les opérations – en cours ou planifiées [redacted] Coordination du partage de renseignement ayant trait à la planification opérationnelle et à l'exécution des COA/COD, mais aussi aux risques connexes et à la prise en compte de la politique étrangère du Canada. Collaboration relative au renouvellement, à l'évolution et au développement des AM en vigueur ou à venir.	Résoudre les problèmes relevant de la compétence du GT, mais non résolu au niveau des DG.

[137] Document du CST-AMC, « CSE-GAC ACO/DCO Working Group Terms of Reference », septembre 2020, p. 1 et 2. Les membres du groupe de travail se sont entendus sur un processus normalisé par l'intermédiaire duquel AMC sera mobilisé aux fins des COA/COD. De plus, le CST et AMC collaborent au niveau opérationnel requis (niveau allant jusqu'à celui des directeurs) dans le cadre des activités du Groupe des fonctionnaires (GF).
[138] Document du CST-AMC, « CSE-GAC ACO/DCO Working Group Terms of Reference », septembre 2020, p. 1 et 2.

ANNEXE D : Conclusions et recommandations

Conclusions

Conclusion nº 1 : Les demandes d'autorisation ministérielle pour les cyberopérations actives et défensives n'offrent pas suffisamment de détails pour que les ministres concernés comprennent l'étendue des catégories d'activités demandées dans l'autorisation. De même, l'autorisation ministérielle ne définit pas suffisamment les catégories d'activités, les techniques connexes et les ensembles de cibles à utiliser dans l'exécution des opérations.

Conclusion nº 2 : L'évaluation des risques pour la politique étrangère exigée suivant deux conditions des autorisations ministérielles pour les cyberopérations actives et défensives repose trop sur la détermination technique des risques au détriment des éléments qui caractérisent la politique étrangère du gouvernement du Canada.

Conclusion nº 3 : Le cadre de gouvernance actuel ne comprend pas de mécanisme permettant de confirmer la conformité d'une cyberopération active (COA) aux grandes priorités stratégiques du gouvernement du Canada, comme le demandent la *Loi sur le CST* et l'autorisation ministérielle. Bien que les objectifs et priorités ne relèvent pas uniquement du CST et d'AMC, ceux-ci dictent les COA sans l'apport de la communauté globale du gouvernement du Canada prenant part à la gestion des objectifs généraux du Canada.

Conclusion nº 4 : Le CST et AMC n'ont pas mis en place de seuil permettant de définir et de distinguer les cyberopérations actives et les cyberopérations défensives, une lacune qui pourrait mener à une participation insuffisante de la part d'AMC advenant qu'une opération soit considérée à tort comme étant défensive.

Conclusion nº 5 : Les politiques internes du CST qui portent sur la collecte d'information dans le cadre de cyberopérations ne sont pas décrites avec exactitude dans les autorisations ministérielles pour les cyberopérations actives et défensives.

Conclusion nº 6 : Le processus [redacted] lequel a lieu une fois que les documents de planification ont été approuvés, contient des informations pertinentes pour les plans opérationnels généraux du CST. Or, il est arrivé que [redacted] contienne des informations essentielles qui n'apparaissaient pas dans ces autres documents, bien que cette présentation soit approuvée à un niveau de gestion inférieur.

Conclusion nº 7 : Le CST a prodigué à ses employés des formations générales leur permettant d'acquérir une connaissance des nouveaux pouvoirs autorisant la conduite de cyberopérations actives et défensives (COA/COD). Toutefois, il y a lieu de croire que les employés directement impliqués dans les COA/COD n'auraient une compréhension suffisante ni des éléments ayant trait aux pouvoirs légaux nouvellement acquis par le CST ni des paramètres régissant l'application de ces pouvoirs.

Conclusion nº 8 : En ce qui concerne les cyberopérations actives et défensives, le cadre élaboré par le CST et AMC pour évaluer les obligations du Canada en matière de droit international manque de clarté et d'objectivité.

Conclusion nº 9 : Le CST s'attend à ce qu'AMC l'avise de tout changement à la politique étrangère, mais n'accorde pas assez d'importance à la nécessité de faire part à AMC des autres risques pouvant survenir au cours d'une opération. En outre, des informations essentielles à l'évaluation d'AMC visant les risques pour la politique étrangère ne figurent pas dans la documentation que le CST utilise pour

mobiliser AMC aux fins d'une opération. Ainsi, il se peut que le cadre de consultation actuel n'incite pas le CST à communiquer suffisamment d'information pour permettre à AMC d'évaluer les risques pour la politique étrangère et de gérer les risques qui se présentent au cours d'une cyberopération.

Recommandations

Recommandation nº 1 : L'OSSNR recommande que le CST définisse plus précisément les catégories d'activités, les techniques connexes et les ensembles de cibles employés dans le cadre des cyberopérations actives et défensives, ainsi que les motifs et objectifs sous-jacents, tant dans les demandes que dans les autorisations ministérielles pour ces activités.

Recommandation nº 2 : L'OSSNR recommande qu'AMC inclue, dans les autorisations ministérielles, un mécanisme d'évaluation de tous les paramètres des risques pour la politique étrangère découlant des cyberopérations actives et défensives.

Recommandation nº 3 : L'OSSNR recommande que le CST et AMC établissent un cadre de consultation des intervenants clés, notamment, le conseiller à la sécurité nationale et au renseignement auprès du premier ministre et les autres ministères concernés, dont les mandats touchent les cyberopérations actives proposées afin que celles-ci s'harmonisent aux grandes priorités stratégiques du gouvernement du Canada et que les exigences énoncées dans la *Loi sur le CST* soient respectées.

Recommandation nº 4 : L'OSSNR recommande que le CST et AMC instaurent un seuil qui permette de distinguer une cyberopération active d'une cyberopération défensive préventive, et que ce seuil soit fourni au ministre de la Défense nationale dans les autorisations ministérielles applicables.

Recommandation nº 5 : L'OSSNR recommande que le CST, dans ses demandes présentées au ministre de la Défense nationale, décrive avec exactitude la possibilité que, dans le cadre de cyberopérations actives et défensives, des activités de collecte se déroulent au titre d'autorisations distinctes.

Recommandation nº 6 : L'OSSNR recommande que le CST inscrive toutes les informations pertinentes – y compris les informations sur le ciblage et le contexte – dans tous les plans opérationnels qui sont produits dans le cas d'une cyberopération ainsi que dans tout document soumis à l'attention d'AMC.

Recommandation nº 7 : L'OSSNR recommande que le CST offre un programme de formation structuré aux employés prenant part à l'exécution des cyberopérations actives et défensives (COA/COD). Ce faisant, le CST s'assurerait que lesdits employés possèdent une connaissance adéquate des pouvoirs légaux, des exigences et des interdictions stipulées dans les autorisations ministérielles.

Recommandation nº 8 : L'OSSNR recommande que le CST et AMC fournissent une évaluation du régime légal international applicable à l'exécution des cyberopérations actives et défensives, et que le CST exige d'AMC qu'il procède à une évaluation juridique exhaustive de la conformité de chaque opération au droit international.

Recommandation nº 9 : L'OSSNR recommande que le CST et AMC s'échangent toute l'information pertinente et se tiennent au courant de tous les nouveaux développements ayant une incidence sur

l'évaluation des risques associés aux cyberopérations, et ce, tant au stade de la planification qu'à celui de l'exécution.