National Security and Intelligence Review Agency | Office de surveillance des activités en matière de sécurité nationale et de renseignement

EXAMEN DES CYBEROPÉRATIONS ACTIVES ET DES CYBEROPÉRATIONS DÉFENSIVES DU CST

OSSNR // Examen nº 2021 – 09

TRÈS SECRET // SI // CEO // SECRET PROFES. DE L'AVOCAT

Table des matières

I. SOMMAIRE

1. (U) La *Loi sur le Centre de la sécurité des télécommunications* attribue au CST le pouvoir de mener des cyberopérations actives (COA) et des cyberopérations défensives (COD). En outre, les COA et les COD du CST sont devenus des outils d'application de la politique du gouvernement du Canada en matière d'affaires étrangères et de sécurité. En 2021, l'OSSNR a mené un examen portant sur la gouvernance des COA et des COD, mais aussi sur les processus de planification et d'approbation de ces types de cyberopérations. À la suite de l'examen portant sur la gouvernance des COA et des COD du CST – et d'AMC dans une moindre mesure – bon nombre d'observations ont été formulées. Certaines d'entre elles soulevaient des lacunes, lesquelles ont donné lieu à la formulation de recommandations. S'appuyant sur cet examen de la gouvernance, le présent rapport se penche plutôt sur les COA et les COD du CST en soi. Autrement dit, l'examen vise les opérations suivant une analyse de la mise en œuvre du cadre de gouvernance et du cadre juridique du CST dans le contexte de COA et de COD particulières.

2. (U) L'OSSNR a ajouté AMC, le SCRS, la GRC et le MDN/FAC à la portée du présent examen, dans la mesure où ces organisations pouvaient être, à divers degrés, concernées par les COA et les COD du CST. L'OSSNR a également inspecté quelques éléments techniques d'une COA faisant l'objet d'une étude de cas dans le but de vérifier distinctement certains aspects de l'opération, mais aussi d'approfondir la compréhension de l'OSSNR à l'égard du fonctionnement d'une COA. Certes, l'OSSNR s'est penché sur la totalité des COA et des COD planifiées ou exécutées par le CST jusqu'à la moitié de 2021, mais le présent examen se concentre surtout sur quatre COA ou COD, qui ont été choisies en raison de caractéristiques qui les distinguent les unes des autres.

3. (U) Globalement, l'OSSNR est d'avis que les COA et les COD planifiées et exécutées par le CST pendant la période d'examen étaient conformes aux lois applicables. L'OSSNR a également remarqué certaines améliorations sur le plan des évaluations menées par AMC en matière de risque et en considération du droit international. Par ailleurs, l'OSSNR a noté que le CST avait perfectionné ses processus – quitte à en créer de nouveaux – s'appliquant à la planification et à l'exécution des COA et des COD de sorte à les faire coïncider davantage avec les recommandations formulées à la suite de l'examen de la gouvernance.

4. (U) Du reste, l'OSSNR a tiré des conclusions sur la façon dont le CST pourrait améliorer certains aspects de la planification des COA et des COD, mais aussi sur les communications faites au ministre de la Défense nationale et sur les modalités de coordination avec d'autres entités du gouvernement du Canada. En l'occurrence, l'OSSNR a relevé des risques potentiels pour ce qui a trait aux éléments suivants :

- la capacité d'AMC à évaluer en toute indépendance les risques pouvant résulter des COA et des COD du CST;
- l'exactitude de l'information fournie et les problèmes relatifs à la délégation dans le cas de certaines demandes d'autorisation associées aux COA et aux COD;
- le degré d'engagement du CST envers le SCRS et la GRC relativement aux COA et aux COD, ainsi que les explications fournies par le CST quant à la façon dont il a établi que l'objectif

d'une COA ou d'une COD pouvait, ou non, être raisonnablement atteint d'une autre manière;
- la mesure dans laquelle le CST a décrit la collecte de renseignement pouvant survenir parallèlement ou consécutivement aux COA ou aux COD, dans les demandes d'autorisation des COA et des COD, mais aussi dans les documents opérationnels;
- les dédoublements entre les activités menées au titre des volets COA et COD du mandat du CST et, plus généralement, entre les quatre volets du mandat du CST.

5. (U) Comme ce fut le cas pour les autres examens visant le CST, l'OSSNR a éprouvé d'importantes difficultés lorsqu'il s'est agi d'accéder aux informations du CST devant permettre la poursuite du présent examen. Ainsi, l'OSSNR n'est pas convaincu de la complétude de l'information fournie par le CST et se déclare insatisfait du degré de réactivité du CST.

Liste des sigles et acronymes

AMC – Affaires mondiales Canada

BCP – Bureau du Conseil privé

CCC – Centre canadien pour la cybersécurité ou Centre pour la cybersécurité (au sein du CST)

[redacted]

CNE – Exploitation de réseau informatique [*Computer Network Exploitation*] (voir le glossaire)

COA – Cyberopération active

COD – Cyberopération défensive

COE – Cyberopérations étrangères

[redacted]

CPPC – Cadre de pouvoirs et de planification commun (au CST; voir le glossaire)

[redacted]

CSNR – Conseiller à la sécurité nationale et au renseignement (auprès du premier ministre)

CST – Centre de la sécurité des télécommunications ou le Centre

DI – Demande d'information

DSJ – Direction des services juridiques (au CST)

[redacted]

EM – Expert en la matière

EPM – Ensemble des politiques relatives à la mission (au CST)

ERPE – Évaluation des risques liés à la politique étrangère (à AMC)

[redacted]

GC – Gouvernement du Canada

[redacted]

GOIFC – Groupe des opérations d'information des Forces canadiennes (au sein du MDN/FAC)

GRC – Gendarmerie royale du Canada

GT MSRE – Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (formé de représentants du CST, du SCRS, d'AMC et de la GRC)

[redacted]

IMI – Infrastructure mondiale d'information

JCAD – Document énonçant les pouvoirs liés aux cyberopérations conjointes [*Joint Cyber Authorities Document*] (au CST; voir le glossaire)

Loi sur le CST – *Loi sur le Centre de la sécurité des télécommunications*

MDN/FAC – Ministère de la Défense nationale et Forces armées canadiennes

MinAE – ministre des Affaires étrangères

MinDN – Ministre de la Défense nationale

OCPF – Opérations criminelles de la Police fédérale (à la GRC)

[redacted]

PCCO – Plan conjoint de cyberopérations (au CST; voir le glossaire)

PE – Protocole d'entente

PPO – Police provinciale de l'Ontario

[redacted]

SCRS – Centre canadien du renseignement de sécurité

SDIAC – Section du droit international, administratif et constitutionnel (ministère de la Justice)

SDP – Section des droits de la personne (au ministère de la Justice)

SIGINT – Renseignement électromagnétique [*Signals Intelligence*]

[redacted]

SP – Sécurité publique Canada

[redacted]

Glossaire

Chef. Dans le présent rapport, le terme « chef » désigne le chef ou la chef du CST.

Exploitation de réseau informatique (CNE pour Computer Network Exploitation). Les techniques d'exploitation des réseaux informatiques sont employées pour se donner secrètement accès à des ordinateurs, à des réseaux informatiques, à des réseaux de données, à des dispositifs personnels ou à d'autres dispositifs commandés par ordinateur.

[redacted]

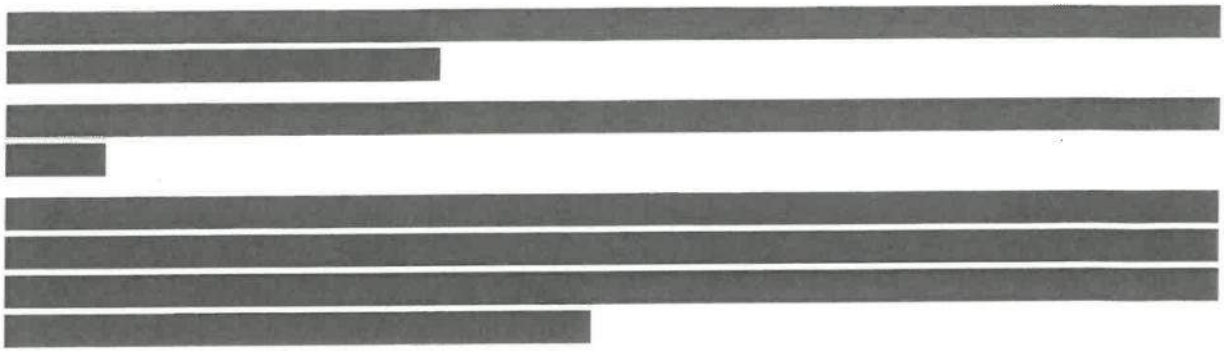
Collectivité des cinq. Partenariat d'échange de renseignement dont font partie le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande.

***Document énonçant les pouvoirs liés aux cyberopérations conjointes* (JCAD pour *Joint Cyber Authorities Document*).** Le JCAD est un document de politique de haut niveau qui classe les autorisations de cyberopérations par thème, [redacted]

Plan conjoint de cyberopérations (PCCO). Le PCCO fait état d'un plan décrivant la conduite des activités de cyberopérations (effets) à l'endroit d'une menace précise ou d'un auteur de menace particulier. [redacted]

Cadre de pouvoirs et de planification commun (CPPC). Désigné dans l'ensemble du présent rapport comme étant le « cadre des cyberopérations », le CPPC est le cadre de gouvernance qui régit l'élaboration et l'exécution des cyberopérations du CST. En l'occurrence, il s'applique à toutes les COA et à toutes les COD.

[redacted]



II. FONDEMENT LÉGISLATIF

6. (U) 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*)[1].

III. INTRODUCTION

Contexte de l'examen

7. (U) La *Loi sur le Centre de la sécurité des télécommunications*[2] a créé un précédent en accordant au CST le pouvoir de mener en toute indépendance des cyberopérations actives et des cyberopérations défensives[3] (ci-après désignées respectivement par les sigles « COA » et « COD », ou collectivement désignées par le terme général « cyberopération »).

8. (U) En 2021, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a examiné la structure de gouvernance ainsi que les processus de planification et d'approbation s'appliquant aux activités menées dans le cadre de COA et de COD jusqu'à la fin d'août 2020 (examen désigné dans la présente par le terme « examen de la gouvernance[4] »). L'examen de la gouvernance fut l'occasion de formuler bon nombre d'observations concernant la gouvernance des COA et des COD du CST – et d'AMC dans une moindre mesure. Certaines de ces observations ont permis de relever des lacunes, mais aussi d'émettre des recommandations. En outre, l'examen de la gouvernance a soulevé plusieurs questions concernant la façon dont les structures de gouvernance du CST et d'AMC étaient mises en place ou concrètement suivies.

9. (U) S'appuyant sur l'examen de la gouvernance, le présent rapport se penche plutôt sur les COA et les COD du CST en soi. Autrement dit, l'examen vise les opérations à proprement parler. Partant des observations faites pendant l'examen de la gouvernance, l'OSSNR examine l'opérationnalisation et la mise en œuvre du cadre de gouvernance et du cadre juridique du CST dans le contexte de COA et de COD particulières. L'OSSNR a demandé qu'on lui donne accès aux informations ayant trait à l'intégralité des COA et des COD envisagées, planifiées et exécutées avant le 30 juillet 2021. À ce titre, les conclusions et les recommandations formulées dans le présent rapport font état de faits se rapportant aux cyberopérations telles qu'elles se présentaient pendant la période d'examen[5].

---

[1] *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, L.C. 2019, ch. 13, art. 2.
[2] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76 [*Loi sur le CST*].
[3] Dans le présent rapport, le terme « cyberopérations » est un hyperonyme des termes COA et COD. Certes, le CST et d'autres ministères du GC emploient le terme « cyberopérations étrangères » (COE) pour désigner les COA et les COD, mais par souci de clarté, l'OSSNR a choisi d'utiliser les termes employés dans le texte de la *Loi sur le CST*.
[4] Examen intitulé « Gouvernance du CST s'appliquant aux cyberopérations actives et défensives » (Examen de l'OSSNR nº 20-02).
[5] Dans certains cas, l'OSSNR a été en mesure de prendre acte sinon d'être avisé des mises à jour apportées depuis le 30 juillet 2021. Lorsque ces mises à jour ont trait ou son consécutives à l'analyse du présent rapport, l'OSSNR en fait mention. Toutefois, l'OSSNR n'a pas pour autant été informé de toutes les mises à jour pertinentes apportées après le 30 juillet 2021.

10. (TS//SI) Les COA et les COD [redacted] ce qui facilite le déroulement des activités liées aux cyberopérations. Ainsi, l'OSSNR a pris en compte ou examiné certains aspects de [redacted]

11. (U) Le présent rapport est structuré de la façon suivante. Il commence par des informations contextuelles sur les COA et les COD. Ensuite, la section IV fait brièvement état de quatre études de cas portant sur des COA et des COD qui servent d'exemples sur lesquels repose l'ensemble de l'analyse. Pour sa part, la section V présente les observations, les conclusions et les recommandations de l'OSSNR relativement aux cyberopérations – ce qui comprend, notamment, les quatre études de cas de l'OSSNR – prises en compte pendant la période d'examen. Divisée en plusieurs thèmes, cette section analyse principalement les éléments suivants :

- les évaluations portant sur les risques juridiques et les risques liés à la politique étrangère;
- les conditions à respecter pour l'autorisation des COA et des COS, particulièrement les exigences stipulées aux paragraphes 34(1) et 34(4) de la *Loi sur le CST*;
- les éléments qui distinguent les COA, les COD et les autres activités du CST.

12. (U) Le rapport se termine par la section VI, qui fait brièvement état de la réactivité globale du CST à l'égard de l'OSSNR durant le présent examen. Enfin, de plus amples détails et des informations complémentaires sont présentés dans les annexes.

Méthodologie

13. (U) L'OSSNR a analysé un large éventail d'informations détenues par le CST, y compris une documentation exhaustive portant sur les processus, les conseils juridiques, les éléments techniques, les consultations auprès des intervenants ou des partenaires, les évaluations post-opérations, etc. Les documents fournis à l'OSSNR comprenaient de la correspondance ayant circulé entre des membres du personnel du CST, mais aussi entre ceux-ci et des partenaires relativement à des opérations spécifiques et à des composantes d'opérations. De plus, l'OSSNR a assisté à trois séances d'information et à deux démonstrations techniques offertes par des spécialistes du CST.

14. (U) Dans le cadre du présent examen, l'OSSNR a reçu de l'information provenant du CST, mais aussi d'AMC, du SCRS, de la GRC et du MDN/FAC, ce qui a permis d'explorer en profondeur les divers secteurs d'intérêt. L'OSSNR a analysé des documents venant des quatre organisations et a assisté à des séances d'informations ciblées présentées par AMC, le SCRS et le MDN/FAC. En tout, l'OSSNR a adressé 30 demandes d'information (ainsi que des demandes de séances d'information) aux organisations visées par l'examen.

15. (U) Conformément à ce qui est énoncé dans le mandat de l'OSSNR, le présent examen avait pour objet de tester divers types d'accès direct aux dépôts d'information du CST. Or, tel qu'il est énoncé à la section VI du présent rapport, le CST n'a pas consenti à ces accès directs aux dépôts d'information du CST, ce qui a entravé le bon fonctionnement de l'examen particulièrement sur le plan de l'accès à l'information détenue par le CST.

Mise en contexte des COA et des COD

Que sont les cyberopérations actives et défensives?

16. (U) Les cyberopérations défensives (COD) sont des activités menées dans l'infrastructure mondiale de l'information (IMI) ou par l'entremise de celle-ci afin d'aider à protéger l'information électronique et les infrastructures d'information des institutions fédérales et celles désignées comme étant d'importance pour le Canada par le ministre de la Défense nationale (MinDN)[6]. Par exemple, les COD pourraient consister en des activités visant à stopper ou à affaiblir les cybermenaces étrangères avant qu'elles [redacted] Canada [redacted] Pour leur part, les cyberopérations actives (COA) sont des activités menées dans l'IMI ou par l'entremise de celle-ci dans le but 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 intentons ou activités[7]. Les COA permettent au gouvernement du Canada (GC) d'utiliser les capacités en ligne du CST en vue d'entreprendre, dans le cyberespace, un éventail d'activités visant à entraver la capacité des adversaires à porter atteinte aux relations internationales, à la défense ou à la sécurité nationale du Canada. Les répercussions des COA et des COD subies par les entités ciblées sont désignées par le terme « effet » (d'une COA ou d'une COD).

17. (S) Pour mener des COA et des COD, le CST s'appuie sur les accès dont il dispose déjà, à savoir à l'IMI, à l'expertise en matière de renseignement étranger ainsi qu'aux partenaires nationaux et internationaux, pour obtenir du renseignement pertinent sur lequel reposera le bon déroulement des cyberopérations.

18. (S) La collecte préliminaire du renseignement, [redacted] représentent l'essentiel du travail à réaliser en amont pour permettre l'exécution des COA ou des COD, alors que les activités réalisées en aval dans le cyberespace [redacted] ne représentent qu'une modeste partie de l'opération.

Fondements juridiques des cyberopérations

19. (U) La *Loi sur le CST* accorde au CST l'autorisation légale de mener des COD et des COA, et ces volets du mandat du CST sont décrits aux articles 18 et 19 de la Loi. Il importe d'indiquer que la *Loi sur le CST* impose des restrictions aux COA et aux COD en ce sens que celles-ci ne peuvent ni viser un Canadien ou une personne se trouvant au Canada, ni contrevenir aux dispositions de la *Charte canadienne des droits et libertés*[8], ni viser une portion de l'IMI qui est

---

[6] *Loi sur le CST*, article 18 : « 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 en vertu du paragraphe 21(1). »

[7] *Loi sur le CST*, article 19 : « 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. »

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

au Canada[9].

20. (U) Les COA et les COD doivent être exécutées en vertu d'une autorisation délivrée par le ministre de la Défense nationale (MinDN) au titre du paragraphe 29(1) (COD) ou du paragraphe 30(1) (COA) de la *Loi sur le CST*[10]. Le régime des autorisations prévu à la *Loi sur le CST* accorde au CST le pouvoir de mener les activités ou les catégories d'activités énumérées à l'article 31 de la *Loi sur le CST* dans la réalisation des volets du mandat touchant les COA et les COD[11]. Les autorisations visant les COA et les COD autorisent le CST à exercer des activités dans le cadre de COA et de COD malgré toute autre loi fédérale ou loi d'un État étranger[12]. Pour délivrer une autorisation, le MinDN doit avoir conclu qu'il y avait des motifs raisonnables de croire que toute activité légitimée par ladite autorisation serait raisonnable et proportionnelle[13]; il doit également avoir conclu que l'objectif de la cyberopération ne pourrait pas être raisonnablement atteint d'une autre manière et qu'aucune information ne serait acquise au titre de l'autorisation[14]. Au reste, le MinDN doit consulter le ministre des Affaires étrangères (MinAE) avant de délivrer une autorisation s'appliquant à une COD et doit obtenir le consentement de ce même MinAE lorsqu'il s'agit de délivrer une autorisation s'appliquant à une COA[15]. Toute activité autorisée aux fins d'une COA ou d'une COD ne peut causer, intentionnellement ou par négligence criminelle, des lésions corporelles à une personne physique ou la mort de celle-ci; elle ne peut non plus tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie[16]. Il importe de noter que contrairement aux autorisations délivrées pour les activités menées dans le cadre des volets renseignement étranger, cybersécurité ou assurance de l'information du mandat du CST, les autorisations s'appliquant aux COA et aux COD ne sont pas assujetties à l'approbation du commissaire au renseignement.

IV. COA ET COD DU CST : ÉTUDES DE CAS

21. (TS//SI) L'OSSNR a reçu des documents, principalement du CST, portant [redacted] **COA ou COD** qui avaient été approuvées ou dont l'étape de la planification s'était terminée au 30 juillet 2021. Toutes les COA et COD planifiées, approuvées ou exécutées pendant la période d'examen ont été respectivement jugées, par le CST et AMC, comme comportant un niveau de risque [redacted][17].

---

[9] *Loi sur le CST*, alinéa 22(2)a).

[10] *Loi sur le CST*, alinéa 22(2)b).

[11] Les activités autorisées à 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 que 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; et 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.

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

[13] *Loi sur le CST*, paragr. 34(1) : « Le ministre ne peut délivrer l'autorisation visée aux paragraphes 26(1), 27(1) ou (2), 29(1) ou 30(1) que s'il conclut qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités. »

[14] *Loi sur le CST*, paragr. 34(4) : « Le ministre ne peut délivrer l'autorisation visée aux paragraphes 29(1) ou 30(1) que s'il conclut, outre ce qui est prévu au paragraphe (1), qu'il y a des motifs raisonnables de croire que l'objectif de la cyberopération ne peut raisonnablement être atteint d'une autre manière et qu'aucune information ne sera acquise au titre de l'autorisation, sauf conformément à une autorisation délivrée en vertu des paragraphes 26(1), ou 27(1) ou (2) ou 40(1). »

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

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

[17] Les COA et les COD comportent deux processus d'évaluation des risques principaux : le processus du [redacted] du CST et le processus de l'ERPE d'AMC. Chaque processus évalue des aspects distincts. Par exemple, AMC se penche sur les risques associés à la politique étrangère, ce qui comprend le droit international et les normes en matière de comportement responsable des États, alors que le CST préconise une approche axée sur le « risque global » qui analyse les facteurs de

22. (S) Pour examiner les COA et les COD du CST de plus près pendant la période d'examen, l'OSSNR a choisi quatre études de cas sur lesquelles se concentrer à l'occasion des demandes d'information ou de séances d'information : [redacted][18]. Les quatre ont été choisies en raison des caractéristiques qui les distinguaient les unes des autres, notamment, la date, les techniques employées et la nature des cibles, mais aussi selon que lesdites opérations devaient être menées en autonomie par le CST ou de concert avec la Collectivité des cinq[19]. Même s'il a choisi de se concentrer sur quatre études de cas aux fins du présent rapport, l'OSSNR a néanmoins examiné d'autre matériel fourni par le CST et par d'autres entités relativement à toutes les COA et COD, de sorte à établir un contexte d'analyse. Dans certains cas, des observations concernant des opérations ne figurant pas au nombre des quatre études de cas ont été formulées dans le présent rapport.

ÉTUDE DE CAS N^{O} 1 : [redacted]

23. (S) Cette opération renvoie à une COD approuvée, mais non exécutée, qui avait pour objet de s'attaquer à des menaces pouvant planer sur les élections fédérales, en mettant en place un mécanisme capable d'affecter, voire de perturber une infrastructure Internet qui aurait pu être utilisée par une entité étrangère résolue de s'attaquer l'infrastructure ou l'information électroniques d'Élections Canada. L'opération devait servir de complément à une série de mesures défensives mises en place par le Centre canadien pour la cybersécurité (CCC) et le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (GT MSRE). En définitive, on a jugé qu'il n'était plus nécessaire d'exécuter l'opération.

24. (S) [redacted] a été planifiée dans le cadre [redacted] lequel permettait de consolider les efforts du CCC lorsqu'il s'est agi de prodiguer des conseils en matière de cybersécurité, de donner des directives ou d'offrir du soutien opérationnel dans le contexte des élections fédérales de 2019.

25. (TS//SI//CEO) [redacted]

26. (S) Une COD très semblable désignée sous le nom [redacted] avait été planifiée par le CST en vue des élections fédérales de 2021, mais n'a pas été exécutée puisque le degré de menace pronostiqué ne s'est pas concrétisé.

---

risque sur le plan des [redacted]

[18] L'OSSNR note ceci : le fait que les COA et les COD ont été choisies ne signifie pas forcément qu'elles ont été ultimement exécutées par le CST.

[19] Pendant son examen des cyberopérations, l'OSSNR a remarqué un certain degré de coordination et de collaboration entre les partenaires de la Collectivité des cinq relativement à certaines COA et COD du CST. En effet, [redacted]

[20] Séance d'information du CST, DI-5, 17 février 2022.

ÉTUDE DE CAS N^{O} 2 : [redacted]

27. (TS) [redacted] L'objectif de [redacted] était de compromettre l'efficacité de [redacted]

28. (TS//SI//[redacted]) [redacted]

29. (S) [redacted]

ÉTUDE DE CAS N^{O} 3 : [redacted]

30. (TS//SI//[redacted]) [redacted] dans le but de perturber [redacted]

31. (TS//SI//[redacted]) [redacted]

[redacted]

32. (TS//SI//[redacted])

[redacted]

33. (TS//SI//[redacted])

[redacted] était considérée comme une réussite

[redacted]

ÉTUDE DE CAS N° 4 : [redacted]

34. (TS//SI//[redacted])

[redacted]

35. (TS//SI//[redacted])

[redacted] pour objet de court-circuiter

[redacted]

[redacted][27].

36. (S//SI//[redacted]) À [redacted]

37. (TS//CEO) [redacted] était la première cyberopération du CST [redacted] en vertu d'une autorisation [redacted] Ce type [redacted] que le CST nomme « autorisation [redacted] » est abordé plus loin dans le présent rapport.

38. (C) [redacted] l'équipe du CST responsable de la conformité en interne a été avisée – par le groupe des « cyberopérations étrangères » (COE) du CST – d'un incident relatif à la protection des renseignements personnels ayant eu lieu [redacted] et ayant coïncidé avec la période d'examen de l'OSSNR[28]. En outre, l'OSSNR a pu établir que cet incident était lié à des difficultés récurrentes sur le plan des évaluations de l'extranéité réalisées par le CST. Des difficultés semblables ont été observées dans le cadre d'autres examens dont les titres sont « Examen des incidents liés à la vie privée et des erreurs de procédures autosignalées par le Centre de la sécurité des télécommunications » et « Examen d'un programme [redacted] spécial relevant du volet renseignement étranger du mandat du CST » (achevé en août 2022). L'OSSNR réalisera un examen qui se penchera exclusivement sur cette difficulté.

V. ANALYSE

Évaluation des risques liés à la politique étrangère et droit international

39. (U) Comme l'indique l'OSSNR dans l'examen de la gouvernance, les cyberopérations du CST peuvent comporter des risques pour la politique étrangère et les relations internationales du Canada[29]. Ainsi, la *Loi sur le CST* exige que le MinAE soit consulté pour ce qui concerne les autorisations de COD. Toutefois, c'est le MinAE qui demande ou consent que l'autorisation de COA soit délivrée[30]. Bien que la *Loi sur le CST* ne l'exige aucunement, AMC et le CST ont choisi de conclure un accord voulant qu'AMC

[redacted]

[28] Document du CST, « *Incident Summary Report (Incident* [redacted] *)* », GCDocs [redacted] et « *Incident_Record_(*[redacted]*)* », GCDocs [redacted]. Le CST a découvert l'incident en mars 2022 puis, en juin 2022, a proactivement avisé l'OSSNR de l'incident en question.

[29] En l'occurrence, les activités de renseignement étranger du CST n'aient pour seul objet de collecter du renseignement, alors que les COA et les COD sont conçues pour produire un effet sur divers types de cibles.

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

tienne un rôle actif sur le plan opérationnel suivant une évaluation des risques liés à la politique étrangère (ERPE), une mesure qui s'harmonise avec l'intention du législateur telle qu'elle est exprimée dans la *Loi sur le CST*[31]. C'est d'ailleurs le Cadre de gouvernance s'appliquant à la collaboration entre AMC et le CST qui est suivi lorsque le CST et AMC collaborent l'un avec l'autre[32]. De plus, comme l'a remarqué l'OSSNR lors de l'examen de la gouvernance, AMC prend part à la rédaction des demandes de COA et de COD.

40. (S//CEO) L'OSSNR a également noté dans l'examen de la gouvernance que les ERPE réalisées par AMC dans le cadre de cyberopérations du CST ne donnaient pas suffisamment de détails et omettaient de donner des renseignements pertinents relativement à certains facteurs importants[33]. Au cours du présent examen, l'OSSNR a remarqué qu

41. (U) Lors de son examen de la gouvernance, l'OSSNR a constaté que le CST et AMC avaient développé un cadre qui n'était pas suffisamment clair et objectif pour permettre, s'agissant des cyberopérations, une évaluation adéquate des obligations du Canada au vu du droit international. L'OSSNR a recommandé que le CST exige qu'AMC mène et documente une évaluation juridique approfondie relativement à la conformité de chacune des opérations aux dispositions du droit international.

42. (TS//SI//SOLICITOR-CLIENT) L'examen de la gouvernance réalisé par l'OSSNR a également pris acte du conseil que le ministère de la Justice a formulé L'OSSNR note, toutefois, que les autorisations accordées pendant la période du présent examen exigeaient que le CST [35].

43. (TS//SOLICITOR-CLIENT) Pour le présent examen, Les évaluations examinées par l'OSSNR Selon l'OSSNR, les évaluations examinées étaient solides. Cette évaluation juridique internationale constitue une mesure positive quant aux obligations découlant du droit international et à la conformité aux autorisations, lorsqu'il s'agit de mener des cyberopérations.

---

[31] Réponse écrite, AMC DI-03, question 1b, 15 février 2022.
[32] Pour de plus amples informations sur le Cadre de gouvernance s'appliquant à la collaboration entre AMC et le CST, consulter l'examen de l'OSSNR 2020-02, p. 26-27.
[33] Consulter l'examen de l'OSSNR 20-02, paragr. 78.
[34] Consulter, à titre d'exemple, les ERPE menées par AMC relativement à .
[35] AM de 2021-2022 visant les , paragr. 9(e); AM de 2019-2020 et de 2020-2021 visant les paragr. 11(d).

Elle permet également d'assurer un certain degré de clarté relativement au cadre juridique international au vu duquel les cyberopérations du CST sont menées.

44. (TS//SI//SOLICTOR-CLIENT) À la suite de son examen de la gouvernance, l'OSSNR a également recommandé que le CST et AMC produisent une évaluation du régime juridique international s'appliquant à la conduite des COA et des COD. En avril 2022, AMC a fait une déclaration publique qui présente le point de vue actuel du gouvernement du Canada sur certains aspects clés du droit international visant le cyberespace et qui explique de quelle façon ces règles s'appliquent au cyberespace[36]. [redacted][38] Bien que la déclaration publique d'AMC ait été diffusée à un moment où le CST avait déjà amorcé l'exécution des COA et des COD, l'OSSNR se dit tout de même convaincu que ladite déclaration est le produit d'une analyse éclairée du droit international et constitue un facteur qui démontre effectivement que « [l]e Canada est déterminé à renforcer l'application du droit international dans le cyberespace »[39].

(U) **Conclusion n° 1 : L'OSSNR estime que le processus appliqué par AMC pour évaluer les risques pour la politique étrangère, tel qu'il s'applique aux évaluations juridiques internationales, s'est amélioré depuis l'examen de la gouvernance régissant les COA et les COD du CST.**

45. (U) À la suite de l'examen de la gouvernance, l'OSSNR a recommandé 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[40] ». Après avoir examiné les opérations, l'OSSNR n'a constaté aucune difficulté sur le plan de la communication. D'ailleurs, les documents produits par AMC et par le CST, notamment les comptes rendus de réunions et les échanges de questions, ont montré que la communication avait été fluide et efficace.

46. (U) AMC a indiqué à l'OSSNR qu'elle ne disposait pas de l'expertise nécessaire pour évaluer en toute indépendance les divers aspects des cyberopérations du CST, par exemple, l'infrastructure et les outils employés par le CST pour mener de telles opérations. D'ailleurs, AMC ne tenait aucun rôle qui lui permette d'évaluer en toute indépendance l'efficacité et le degré de réussite des cyberopérations. Par conséquent, AMC s'en est remise au CST pour fournir l'information et, dans certains cas, les explications. Cela dit, AMC a indiqué à l'OSSNR que le CST avait communiqué plus d'information à AMC, et qu'AMC avait, par exemple, obtenu un accès [redacted] aux rapports de renseignement

---

[36] Le document « Droit international applicable dans le cyberespace » du gouvernement du Canada peut être consulté à l'adresse suivante : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra.

[37] AMC, Commentaire sur l'exactitude des faits, 28 septembre 2022.

[38] [redacted]

[39] « Droit international applicable dans le cyberespace », gouvernement du Canada, paragr. 2.

[40] Examen de l'OSSNR 20-02, recommandation n° 9.

du CST sur lesquels s'appuyaient les cyberopérations[41]. L'OSSNR a constaté que le CST avait fourni des mises à jour périodiques à AMC pendant le déroulement des cyberopérations.

(U) **Conclusion n° 2 : L'OSSNR est d'avis qu'AMC ne dispose pas des capacités lui permettant d'évaluer en toute indépendance les risques pouvant découler des techniques employées par le CST en cours de COA ou de COD.**

(U) **Recommandation n° 1 : L'OSSNR recommande qu'AMC perfectionne ses capacités ou en élabore de nouvelles pour être en mesure d'évaluer en toute indépendance les risques pouvant découler des techniques employées par le CST en cours de COA ou de COD.**

Article 32 – Interdictions

47. (U) Conformément aux dispositions du paragraphe 32(1) de la *Loi sur le CST*, dans le cadre de toute activité menée au titre d'une autorisation de COA ou de COD, le CST ne peut causer, intentionnellement ou par négligence criminelle, des lésions corporelles[42] à une personne physique ou la mort de celle-ci; il ne peut non plus tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice et de la démocratie.

48. (TS//SI//SOLICITOR-CLIENT) Concrètement, la question des conduites répréhensibles est évaluée en considération des documents faisant état du cadre du CST s'appliquant aux cyberopérations, lesquels contiennent les motifs pour lesquels on estime que les activités menées dans le cadre de la cyberopération ne se solderont pas par des agissements illégaux. La DSJ, un intervenant opérationnel pour les cyberopérations, formule [redacted] l'implication de la DSJ [redacted][43]. Comme il est indiqué dans les matrices, l'évaluation appelée à établir si les activités d'une cyberopération risquent d'enfreindre les interdictions doit être menée en s'appuyant [redacted][44]. L'interdiction de causer des lésions corporelles ou la mort du fait d'une négligence criminelle invoque également la norme [redacted] Or, l'OSSNR estime que les opinions juridiques et les matrices témoignent d'une compréhension approfondie des interdictions visées à l'article 32 de la *Loi sur le CST*.

49. (TS//SI//SOLICITOR-CLIENT) Les conclusions tirées dans le cadre des PCCO sont évaluées [redacted] et ce, pour veiller

[41] Séance d'information, AMC DI-2, 10 novembre 2021.
[42] Au paragraphe 32(1), le terme « lésion corporelle » a le même sens que celui qui est entendu à l'article 2 du *Code criminel* (paragraphe 32(2) de la *Loi sur le CST*).
[43] Réponse écrite, CST DI-20, question 3, 26 août 2022. Au CST, ce groupe est désigné par l'appellation de « groupe des COE ».
[44] Document du CST, « *Bodily Harm Risk Matrix* », dans l'EPM – Cyberopérations, novembre 2021 (annexe A, p. 11), GCDocs [redacted]

à ce que les évaluations demeurent raisonnables [redacted][45]. L'ensemble des politiques relatives à la mission du CST comprend des matrices et fournit quelques directives sur la façon d'interpréter les interdictions et d'évaluer les risques. Toutefois, l'obligation d'évaluer repose sur [redacted]. Au reste, l'EMP indique que l'on peut trouver de plus amples directives dans la politique du CST relative à la mission.

50. (TS//SI//SOLICITOR-CLIENT) Toutefois, l'évaluation de la conformité juridique des activités d'une opération donnée n'est pas réalisée par le ministère de la Justice et ne fait pas toujours l'objet de consultations juridiques additionnelles lorsqu'elle est à son tour évaluée à l'occasion de la [redacted] du CST, dans la mesure où la DSJ [redacted][47]. L'OSSNR considère que les directives stratégiques du CST ayant trait aux interdictions demeurent inadéquates tant que le ministère de la Justice n'a pas été consulté, surtout lorsqu'on considère que la conformité d'une opération aux dispositions de l'article 32 de la *Loi sur le CST* s'appuie en bonne partie sur des notions juridiques, alors que la conformité dépend fortement du contexte. L'OSSNR estime qu'il est à propos que le ministère de la Justice soit régulièrement impliqué dans l'évaluation et la validation [redacted] dans la mesure où cette implication servira à réduire les risques juridiques qui pourraient se concrétiser en cours de cyberopération.

(U) **Conclusion n° 3 : L'OSSNR estime que le CST et le ministère de la Justice ont affiché une compréhension approfondie des dispositions de l'article 32 de la *Loi sur le CST*. Toutefois, à l'étape de la [redacted] le CST pourrait consulter le ministère de la Justice de façon plus appropriée, ce qui lui permettait de vérifier si l'évaluation de la conformité aux lois demeure valide.**

(U) **Recommandation n° 2 : L'OSSNR recommande que le ministère de la Justice soit pleinement consulté à toutes les étapes d'une COA ou d'une COD, particulièrement à celles qui sont en amont de l'exécution de l'opération.**

Article 34 de la Loi sur le CST

51. (U) Le présent examen est le premier au cours duquel l'OSSNR a été en mesure d'évaluer le respect des exigences énoncées aux paragraphes 34(1) et 4) de la *Loi sur le CST* dans les autorisations des COA et des COD. Or, il importe de souligner que contrairement à ce qui se fait pour les autorisations pour le renseignement étranger ou la cybersécurité, le commissaire au renseignement n'examine pas les conclusions tirées au titre des paragraphes 34(1) et (4) – conclusions sur lesquelles s'appuient les autorisations de COA et de COD délivrées par le MinDN – pour établir si elles s'avèrent raisonnables.

Description des normes juridiques

52. (U) En vertu du paragraphe 34(1) de la *Loi sur le CST*, le ministre de la Défense nationale peut délivrer une autorisation de COA [paragraphe 30(1)] ou de COD [paragraphe 29(1)] seulement s'il conclut qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et

[45] Réponse écrite, CST DI-20, question 3. Consulter [redacted].

[46] Section 3.4.2., EPM – Cyberopérations, novembre 2021. CST, Commentaires sur l'exactitude des faits, 23 septembre 2022.

[47] Consulter le glossaire du présent rapport.

proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités. Avant qu'une une autorisation de COA ou de COD soit délivrée, le paragraphe 34(4) exige que le MinDN ait conclu qu'il y avait des motifs raisonnables de croire que l'objectif de la cyberopération ne pouvait être atteint d'une autre manière et qu'aucune information ne serait acquise au titre de l'autorisation, sauf conformément à une autorisation délivrée en vertu des paragraphes 26(1) (renseignement étranger), 27(1) ou (2) (cybersécurité) ou 40(1) (situation d'urgence).

53. (U) Il importe de souligner que la demande écrite du chef du CST doit présenter les faits devant permettre au MinDN de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les critères de délivrance sont été respectés[48].

Application des normes juridiques

54. (TS//CEO) Dans le cadre du présent examen, l'OSSNR a pu évaluer les cyberopérations du CST en considération de la structure de gouvernance, mais aussi des autorisations. Plus précisément, il a pu se pencher sur les opérations menées au titre d'autorisations à [redacted] lesquelles [redacted] autorisent un éventail d'activités. À la différence des autorisations à [redacted] visant des COA ou des COD, [redacted] a été menée au titre d'une autorisation [redacted] qui ne visait que les objectifs particuliers à l'opération en question.

55. (TS//CEO) Lors de l'examen de la gouvernance, l'OSSNR a estimé que les demandes d'autorisation visant les cyberopérations à [redacted] ne fournissaient pas suffisamment d'éléments permettant aux ministres de la Défense nationale et des Affaires étrangères de jauger la portée des activités faisant l'objet de la demande. En effet, l'OSSNR était d'avis que les catégories d'activités et les [redacted] des COA et des COD, telles qu'elles étaient décrites dans les deux demandes d'autorisation, [redacted][49]. Cet état de fait pourrait également avoir une incidence sur la capacité du MinDN à évaluer les activités qu'il convient d'autoriser en considération des exigences de la *Loi sur le CST*, une fonction qui exige que la demande destinée au MinDN soit suffisamment précise pour déterminer si elle répond auxdites exigences. Bien qu'il reconnaisse que les autorisations doivent être assez claires pour que, le cas échéant, le CST puisse exécuter les COA et COD à [redacted], l'OSSNR note également qu'il importe que MinDN puisse jauger, avec un certain degré de précision et de certitude, les types d'activités et d'objectifs qui seront mis en application en vertu de l'autorisation.

56. (TS//CEO) En plus de faire état des faits dans la demande devant permettre au MinDN d'établir le degré de raisonnabilité et de proportionnalité avant de délivrer une autorisation de COA ou de COD, le CST évalue et valide lui-même, en application de son cadre des cyberopérations, le degré de raisonnabilité et de proportionnalité de toute opération proposée. Toutefois, à la différence des demandes soumises au MinDN, les documents internes portant sur le cadre des cyberopérations énoncent ceci : [redacted][50]. » La politique du CST propose des directives additionnelles concernant la façon d'évaluer le degré de proportionnalité et de raisonnabilité [redacted]

[48] *Loi sur le CST*, paragr. 33(2).
[49] Consulter l'examen 020-02 de l'OSSNR, conclusion n° 1.
[50] Réponse écrite, CST DI-06, question 4, 4 mars 2022.

[redacted][51]. L'OSSNR note qu'à cette étape plutôt complexe de la planification d'une opération, le MinDN n'est pas encore appelé à tirer des conclusions relativement au degré de raisonnabilité et de proportionnalité des objectifs à atteindre et des activités autorisées dans le contexte particulier à l'opération.

57. (S) Le CST est placé sous la responsabilité du MinDN[52], et l'article 47 de la *Loi sur le CST* exige que celui-ci exerce personnellement les pouvoirs qui lui sont conférés par les paragraphes 29(1) et 30(1)[53]. En outre, les critères énoncés aux paragraphes 34(1) et (4) de la *Loi sur le CST* doivent avoir été respectés avant la délivrance des autorisations. En règle générale, l'approche adoptée par le CST lorsqu'il s'agit de se conformer à ces exigences consiste à confirmer que les activités proposées s'alignent sur les termes de l'autorisation, puis les conclusions du MinDN sont alors confirmées en interne du côté du CST dans [redacted] Même si [redacted] évaluations du degré de raisonnabilité et de proportionnalité, et que l'objectif de la cyberopération ne pourrait pas être atteint par un autre moyen qui [redacted] il fait savoir que les exigences stipulées à l'article 34 constituent les conditions préalables à la délivrance, par le MinDN, d'une autorisation de COA ou de COD sans toutefois constituer des conditions préalables à l'évaluation que le CST [redacted]

58. (TS//CEO) Qui plus est, l'OSSNR a remarqué qu'en pratique, il y avait une différence entre les objectifs dits « stratégiques » et les objectifs dits « opérationnels », lorsqu'il est question des cyberopérations : [redacted] Convient-il de rappeler que la *Loi sur le CST* exige que « la nature de l'objectif à atteindre » et « l'objectif de la cyberopération » soient établis de façon à répondre aux exigences énoncées aux paragraphes 34(1) et (4).

59. (TS//SI//CEO) L'intégralité du contexte factuel suivant lequel le MinDN doit évaluer les autorisations de cyberopérations sur le plan de la conformité aux exigences de la *Loi sur le CST* n'est

---

[51] Document du CST, EPM – Cyberopérations 2019, section 3.6.

[52] *Loi sur le CST*, article 6.

[53] Le libellé de l'article 47 indique clairement que le ministre doit personnellement exercer les pouvoirs qui lui sont conférés au titre des paragraphes 29(1) et 30(1) : « Le ministre exerce personnellement les pouvoirs qui lui sont conférés par les paragraphes 26(1), 27(1) et (2), 29(1), 30(1), 36(2), 39(1) et 40(1). » Voir *Sa Majesté la Reine c. Harrison*, [1977] 1 R.C.S. 238 : « Bien qu'il existe une règle générale d'interprétation de la loi selon laquelle une personne doit exercer personnellement le pouvoir discrétionnaire sont elle est investie (*delegatus non potest delegare*), elle ne peut être modifiée par les termes, la portée ou le but d'un programme administratif donné. »; voir également *Ramawad c. ministre de la Main-d'œuvre et de l'Immigration* [1978] 2 R.C.S. 375.

[54] Réponse écrite, CST DI-6, question 3 : [Traduction] « Au paragraphe 2 ainsi qu'aux paragraphes 2 et 3 des AM relatives aux [redacted] de même qu'au paragraphe 2 de l'AM relative à [redacted], le ministre a défini les objectifs stratégiques à atteindre au titre de ces autorisations et a fourni de l'information étayant ces objectifs [...]. Suivant une lecture globale, on constate que chacune [des autorisations] fournit une définition complète de la nature des activités et des objectifs autorisés. »

[55] Voir également la réponse écrite du CST à la DI-6, questions 3 à 5 : [Traduction] « L'élaboration des objectifs fixés pour les activités opérationnelles comprend la prise en compte d'un certain nombre de facteurs, notamment ceux-ci : [redacted] et les considérations mises de l'avant par d'autres intervenants gouvernementaux, notamment, AMC. Les objectifs stratégiques, opérationnels et tactiques sont définis dans les documents ayant trait au Cadre de pouvoirs et de planification commun [...] ». (DI-6, question 5).

[56] Réponse écrite du CST, DI-6, question 5.

pas intégrée à la demande, puisqu'à vrai dire [redacted] Ainsi, les conclusions sur le plan de la raisonnabilité et de la proportionnalité parmi les autorisations à [redacted] ne s'appuient pas nécessairement sur toutes les informations factuelles pertinentes ayant trait à une cyberopération. Pour ce qui concerne les dossiers examinés pendant la période d'examen, les objectifs identifiés dans les demandes à [redacted] et les autorisations étaient thématiques, sans lien particulier avec une opération. Par exemple, l'un des [redacted] objectifs énoncés dans la demande du chef relativement aux [redacted][57] La demande fait état [redacted][58] Dès lors que l'objectif est formulé en des termes aussi génériques et que cet objectif n'est pas étayé par les éléments contextuels d'une cyberopération donnée, le MinDN n'est pas en mesure d'acquérir une compréhension suffisamment juste des objectifs ou des moyens employés pour atteindre ces objectifs. Ainsi, tel qu'il a déjà été indiqué par l'OSSNR, il se trouve que les demandes à [redacted] ne sont pas suffisamment détaillées pour permettre aux ministres concernés de bien saisir ce qu'ils sont appelés à autoriser.

60. (TS//SI//CEO) Dans le cas de la [redacted], qui a été menée au titre de l'autorisation pour les [redacted][59]. Dans ces documents, le lien entre les activités, l'objectif, les effets et le résultat attendu était clairement établi et défini avec précision. En l'occurrence, des documents expliquaient plus adéquatement la mesure dans laquelle les activités opérationnelles s'avéraient raisonnables et proportionnelles. Or, cette information n'a pourtant pas été inscrite dans la demande du chef.

61. (TS//SI//CEO) De plus, les COA comportent un risque d'infraction aux dispositions de la *Charte*, étant donné que l'un des objectifs pourrait être de [redacted] comme ce fut le cas pour [redacted][60]. Or, l'OSSNR note que la *Charte* peut exiger que le MinDN tienne compte des valeurs consacrées par la Charte, lorsqu'il s'agit d'exercer son pouvoir discrétionnaire et de délivrer une autorisation[61]. Ainsi, la prise en compte de l'incidence possible d'une cyberopération sur les droits

---

[57] Demande de 2020-2021 pour une [redacted], paragr. 18(c).
[58] Demande de 2020-2021 pour une [redacted], paragr. 54.
[59] Voir, à titre d'exemple, le [redacted]
[60] Pour ce qui est de l'opération [redacted] un expert du CST a confirmé que [redacted] n'avait pas soulevé de questions relatives à la protection garantie par la Charte, [redacted] Ainsi, l'OSSNR pourrait éventuellement examiner la façon dont le CST s'assure de respecter les dispositions de la Charte lorsqu'il s'agit de mener des cyberopérations.
[61] *Doré c. Barreau du Québec, 2012 CSC 12, paragr.* 55 à 58 : « Comment un décideur administratif applique-t-il donc les valeurs consacrées par la *Charte* dans l'exercice d'un pouvoir discrétionnaire que lui confère la loi? Il ou elle met en balance

garantis par la Charte peut s'avérer utile pour l'évaluation de la raisonnabilité et de la proportionnalité que le MinDN est appelé à faire avant de délivrer une autorisation.

62. (TS//SI//CEO) Les demandes de [redacted] définissent semblablement l'objectif qu'on envisage d'atteindre en vertu de l'autorisation, en ce qu'elles ne font état que des circonstances qui pourraient engendrer le besoin de renforcer les capacités de cybersécurité, plutôt que de s'appliquer au contexte d'une opération particulière[62]. Cette fois encore, les demandes définissent les objectifs et les activités [redacted] qu'il devient difficile, pour le MinDN, d'établir avec certitude le degré de raisonnabilité et de proportionnalité. Pour ce qui concerne les [redacted] examinées, [redacted] L'OSSNR note que la description du processus – telle qu'elle était énoncée dans les [redacted] de la [redacted] – devant permettre d'établir le degré de raisonnabilité et de proportionnalité manquait nettement de clarté. Cette lacune tenait au fait que l'évaluation du CST [redacted]

63. (TS//SI//CEO) Pour ce qui concerne l'exigence visée au paragraphe 34(4) et énonçant le fait que « l'objectif de la cyberopération ne peut raisonnablement être atteint d'une autre manière », il faut savoir que le CST établit une distinction entre, d'une part [Traduction] « les considérations qui sous-tendent cette détermination [lesquelles] sont présentées par le CST dans la demande au ministre » et, d'autre part, [redacted] en vertu du cadre du CST s'appliquant aux cyberopérations[63]. C'est au titre du cadre s'appliquant aux cyberopérations que le CST [redacted], mais aussi à la suite d'une consultation auprès d'autres intervenants du GC[64]. C'est également au titre du cadre s'appliquant aux cyberopérations, et non en vertu de la demande au ministre, que [Traduction] [redacted]

64. (TS//SI//CEO) Par conséquent, on note un écart entre l'information contenue dans la demande, laquelle est évaluée par le MinDN, et le contenu des documents opérationnels, lesquels sont évalués par le CST [redacted] Il est possible qu'une évaluation fondée sur les activités et objectifs stratégiques diffère de celle qui se fonde sur les activités et objectifs opérationnels et tactiques. En outre, l'évaluation appelée à déterminer si les activités d'une opération risquent de donner lieu aux comportements interdits visés à l'article 32 de la *Loi sur le CST* (tel qu'il a été discuté précédemment) devrait censément faire partie du contexte juridique

---

ces valeurs et les objectifs de la loi. Lorsqu'il procède à cette mise en balance, le décideur doit d'abord se pencher sur les objectifs en question. [...] Ensuite, le décideur doit se demander comment protéger au mieux la valeur en jeu consacrée par la *Charte* compte tenu des objectifs visés par la loi. Cette réflexion constitue l'essence même de l'analyse de la proportionnalité et exige que le décideur mette en balance la gravité de l'atteinte à la valeur protégée par la *Charte*, d'une part, et les objectifs que vise la loi, d'autre part. [...] Si, en exerçant son pouvoir discrétionnaire, le décideur a mis en balance comme il se doit la valeur pertinente consacrée par la *Charte* et les objectifs visés par la loi, sa décision sera jugée raisonnable. »

[62] Voir, à titre d'exemple, la demande de 2020-2021 pour une [redacted], paragr. 10 et 11.

[63] Réponse écrite, CST DI-6, question 5.

[64] Ibid.

[65] Ibid.

et factuel sur lequel le MinDN devrait s'appuyer lorsqu'il décide, en vertu de son pouvoir discrétionnaire, si une autorisation doit être délivrée. En vertu du paragraphe 32(2) de la *Loi sur le CST*, le Centre doit faire état des faits qui permettront au MinDN de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les critères qui en permettraient la délivrance ont été remplis. Pour **ce qui concerne les demandes à [redacted] il semble** que le CST ne produit pas l'intégralité du contexte factuel qui permettrait au MinDN d'établir avec certitude si les conditions visées aux paragraphes 34(1) et (4) ont été respectées.

65. (TS//SI) À titre de décideur responsable, le ministre de la Défense nationale est investi, par le Parlement, du pouvoir de délivrer les autorisations dès lors que les critères énoncés dans la *Loi sur le CST* ont été respectés. À ce titre, il doit prendre en compte toutes les circonstances qui lui permettront d'exercer en connaissance de cause le pouvoir discrétionnaire suivant lequel il pourra délivrer l'autorisation[66]. Ainsi, il pourra imposer, le cas échéant, les conditions et les restrictions qu'il juge à propos au titre de l'alinéa 35d) de la *Loi sur le CST*. Toutes les informations pertinentes dont le MinDN a besoin pour respecter les critères énoncés dans la *Loi sur le CST* avant de délivrer une autorisation **ne lui sont pas fournies dans le cas des demandes à [redacted] Or, tout défaut de fournir l'intégralité des** faits contextuels de l'opération et des activités affecte la capacité du MinDN à approuver en pleine connaissance de cause les autorisations de COA ou à soupeser les autorisations de COD, tel que l'exigent les paragraphes 29(2) et 30(2) de la *Loi sur le CST*.

(U) **Conclusion n° 4 : L'OSSNR estime que les demandes d'autorisation que le CST a soumises au titre des paragraphes 29(1) et 30(1) de la *Loi sur le CST* relativement aux activités [redacted] ne contenaient pas toutes les informations nécessaires pour établir de façon éclairée si les exigences visées aux paragraphes 34(1) et (4) de la *Loi sur le CST* avaient été respectées.**

(S) **Recommandation n° 3 : L'OSSNR recommande que le CST renonce à la pratique donnant lieu à la présentation de demandes de COA et de COD génériques (c.-à-d. lorsqu'il y a un [redacted] au ministre de la Défense nationale, et qu'il soumette plutôt des demandes ponctuelles formulées [redacted]**

Demandes et autorisations formulées récemment

66. (TS//SI//CEO) Dans le cas de [redacted] a été rédigée selon une approche axée sur l'opération et comportait [redacted] plutôt que des éléments [redacted] à ceux qui figurent dans les autorisations [redacted] s'appliquant aux **activités à [redacted]. Le CST a demandé une autorisation sur** mesure pour cette opération puisque les activités **prévues dans le cadre de [redacted] (c.-à-d. [redacted] n'avaient pas été énoncées parmi les** objectifs de l'autorisation à [redacted] et n'étaient donc pas automatiquement autorisées. À ce titre, [Traduction] « le CST devait obtenir [redacted] les pouvoirs lui permettant de mener les activités prévues par [redacted]

[66] *X (Re)*, 2017 C.F. 1048, paragr. 53 et 54; extrait de *Baron c. Canada*, [1993] 1 R.C.S. 416, paragr. 437, 439 et 440.

[redacted][67]

67. (TS//SI//CEO) Contrairement aux autorisations à [redacted] note l'OSSNR, les demandes et autorisations [redacted] à celle s'appliquant à [redacted] se penchent sur certaines des préoccupations énoncées précédemment au sujet des autorisations à [redacted] étant donné qu'elles fournissent au MinDN des justifications précises qui expliquent comment l'opération répond aux exigences de la *Loi sur le CST*. Les demandes et autorisations [redacted] ont fourni beaucoup plus de détails concernant la façon dont les exigences visées au paragraphe 34(1) étaient respectées, ce qui a exposé de façon plus évidente les motifs raisonnables de croire qu'il y avait un lien logique et justifié entre la nature des activités et les objectifs à atteindre (c.-à-d. sur le plan de la proportionnalité et la raisonnabilité) et que le contexte de l'opération avait été pris en compte. Il en va de même pour ce qui a trait au paragraphe 34(4), dans la mesure où il y a de plus amples détails établissant les motifs pour lesquels l'objectif de l'opération ne pourrait pas être atteint d'une autre manière, ce qui comprend les arguments selon lesquels les autres types de mesures du GC, à savoir les options autres que les cyberopérations, ne seraient pas raisonnablement en mesure d'atteindre l'objectif énoncé dans l'autorisation.

Paragraphe 34(4) – Consultation des intervenants

68. (S) Dans son examen de la gouvernance, l'OSSNR a exprimé des réserves quant aux consultations menées par le CST auprès d'autres ministères et organismes du GC, particulièrement sur le plan de la conformité des COA et des COD du CST aux priorités stratégiques du GC en matière de sécurité nationale et de défense[68]. Plus précisément, l'examen de la gouvernance réalisé par l'OSSNR a fait état de la pertinence d'une éventuelle coordination avec le Bureau du Conseil privé (BCP) et Sécurité publique (SP) s'agissant des cyberopérations du CST, particulièrement lorsqu'il est question de garantir l'alignement desdites cyberopérations sur les priorités du GC en matière de sécurité, de politique étrangère et de défense. De plus, dans la recommandation n° 3 du rapport d'examen de la gouvernance, l'OSSNR propose que le conseiller à la sécurité nationale et au renseignement (CSNR) auprès du premier ministre tienne un rôle d'intervenant clé lors des consultations portant sur les cyberopérations du CST.

69. (U) Pour approfondir la question de la collaboration du CST avec des intervenants du GC, hormis AMC, l'OSSNR a inclus le SCRS, la GRC et le MDN/FAC à la portée du présent examen. L'OSSNR a choisi ces entités du GC, car chacune était impliquée dans une, voire plusieurs des COA ou des COD examinées par l'OSSNR. Dans le cadre du présent examen, l'OSSNR a tenu à porter son attention sur le SCRS, la GRC et le MDN/FAC pour tenter de comprendre, le cas échéant, la nature et l'ampleur de l'engagement de ces organismes envers le CST – et vice versa – pendant la planification ou la conduite des cyberopérations du CST.

70. (TS//SI) Tel qu'il a été dit précédemment, l'une des conditions préalables à la délivrance d'une autorisation de COA ou de COD par le MinDN est que celui-ci doit conclure qu'il y a des motifs raisonnables de croire que l'objectif de la cyberopération ne peut raisonnablement être atteint d'une autre manière[69]. Or, la Loi ne précise pas de quelle façon cette conclusion doit être tirée.

---

[67] CST DI-06, question 6.
[68] Consulter l'examen de l'OSSNR n° 2020-02, paragr. 50, conclusion n° 3.
[69] *Loi sur le CST*, paragr. (4). L'exigence libellée ainsi « ne peut raisonnablement être atteint d'une autre manière » est particulière à la *Loi sur le CST*.

71. (S) Selon le CST, [Traduction] « À la suite d'une évaluation, le CST confirme qu'il n'y a aucun autre moyen qui permette raisonnablement d'atteindre l'objectif d'une opération en considération du processus de gouvernance et grâce à la collaboration avec les intervenants internes du CST, les partenaires de la Collectivité des cinq ou d'autres intervenants du GC, nommément, AMC, le SCRS et la GRC », et que [Traduction] « les prises en compte sur le plan des opérations ont été faites en collaboration avec [lesdits intervenants][70]. » Néanmoins, les documents analysés pendant le présent examen indiquaient, s'agissant des COA et des COD, que le CST ne s'engageait dans un processus d'évaluation, de validation et de collaboration avec les intervenants que lorsqu'il le jugeait nécessaire, plutôt que de façon générale.

SCRS

72. (TS//SI//CEO) Au cours de la période d'examen, le SCRS a fait appel au CST dans le cadre [redacted] menées au titre du mandat de réduction de la menace visé à l'article 12.2 de la *Loi sur le Service canadien du renseignement de sécurité*[71] et suivant la possibilité, pour le SCRS, de conclure des ententes ou, d'une façon générale, de coopérer avec les ministères du gouvernement du Canada ou avec le gouvernement d'un État étranger ou l'une de ses institutions, dès lors que sont respectées les exigences sur lesquelles doivent s'appuyer les autorisations ministérielles. Le SCRS a indiqué à l'OSSNR qu'aucune des activités menées avec le CST n'avait eu lieu en vertu d'un mandat délivré au titre de l'article 12.1 de la *Loi sur le SCRS*[72]. Le SCRS a d'ailleurs déclaré à l'OSSNR [redacted] il n'avait reçu aucun avis de la part du CST concernant d'autres cyberopérations[73]. Pour sa part, l'OSSNR n'a relevé aucune consultation du CST auprès du SCRS dans le cas [redacted] en cours pendant la période d'examen, [redacted]

73. (TS//SI) L'une des autres opérations à l'occasion desquelles le SCRS a travaillé avec le CST était la [redacted]. Dans le cas [redacted], le SCRS disposait d'une mesure de réduction de la menace (MRM) permanente qui avait été mise en place [redacted] et ce, au titre de l'article 12.1 de la *Loi sur le SCRS*. Le rôle tenu par le SCRS dans le cadre de la [redacted] du CST consistait à recourir [redacted] dans le but d'appuyer le travail du CST[76].

74. (TS//SI) Concernant l'harmonisation et la communication d'information, le SCRS a indiqué à

---

[70] Réponse écrite du CST à la DI-06, question Q5.

[71] *Loi sur le Service canadien du renseignement de sécurité*, *L.R.C.*, 1985, ch. C-23 [*Loi sur le CST*].

[72] Séance d'information du SCRS, 22 mars 2022. De plus, le SCRS a indiqué que [redacted]

[73] Durant la vérification de l'exactitude des faits (septembre 2022), le CST a contesté la déclaration du SCRS en indiquant que le CST avait informé le SCRS par courriel au sujet [redacted] et avait discuté à la fois [redacted] lors de réunions avec le SCRS. L'OSSNR a pris connaissance des courriels indiquant que le CST avait avisé le SCRS concernant [redacted]. Le 14 octobre 2022, le CST a fait part à l'OSSNR d'un courriel indiquant que le [redacted] e CST a expliqué que [redacted]

[74] [redacted] consistait en [redacted]

[75] [redacted] consistait en [redacted]

[76] Plus précisément, [redacted]

l'OSSNR que son sous-comité se réunissait toutes les deux semaines avec des représentants du CST pour que les deux organismes aient l'occasion de discuter de divers sujets. Toutefois, le SCRS n'était pas informé par le CST concernant des COA ou des COD que le CST devait planifier ou mener à moins que celui-ci estime qu'une COA ou une COD donnée puisse avoir une incidence (chevauchement, utilisation de ressources communes) sur des actifs du SCRS, à savoir [redacted] Le SCRS n'était pas non plus au courant du nombre des cyberopérations que le CST avait exécutées. Le SCRS a déclaré à l'OSSNR que le fait d'exécuter en tandem certains éléments des cyberopérations du CST donnait généralement lieu à un degré d'efficacité plus élevé que si le SCRS devait mener seul ces mêmes activités. D'ailleurs, le SCRS a donné en exemple la [redacted] pour démontrer [redacted]

75. (U) L'OSSNR remarque les différences qu'il y a entre le CST et le SCRS sur le plan des fondements juridiques et des mandats, notamment, lorsqu'il est nécessaire de mener des activités semblables dans le cyberespace. Tel qu'il a été dit plus tôt, le SCRS s'engage dans des activités qui s'avèrent analogues à celles du CST, notamment, en vertu du mandat du SCRS relatif aux MRM [paragraphe 12.1(1) de la *Loi sur le SCRS*] qui consiste à appliquer, au Canada ou à l'étranger, des mesures visant à atténuer une menace pour la sécurité du Canada. Avant d'entreprendre des MRM, le SCRS est tenu de consulter, tel qu'il convient, d'autres ministères ou organismes fédéraux afin d'établir s'ils sont en mesure de réduire la menace[77].

76. (U) En revanche, la *Loi sur le CST* ne contient pas de telles exigences, notamment celle de consulter d'autres ministères ou organismes fédéraux. Elle stipule plutôt qu'il doit y avoir des motifs raisonnables de croire que l'objectif de la cyberopération ne pourrait raisonnablement être atteint d'une autre manière, sans préciser comment il conviendrait d'étayer cette croyance. Or, l'objet du volet COA du mandat du CST diffère de celui du mandat MRM exercé par le SCRS[78], et le CST dispose de compétences techniques et d'une « cyberexpertise » que le SCRS n'a pas.

77. (U) En outre, bien que les mandats et les fondements juridiques ne soient pas les mêmes pour le CST et le SCRS, il existe des situations où c'est le SCRS qui est mieux à même d'atteindre l'objectif de la cyberopération en question. Toutefois, dans les cas où il serait en mesure de réduire la menace, le CST doit tout de même vérifier si l'objectif de la cyberopération ne peut raisonnablement être atteint d'une autre manière. L'OSSNR note que le critère ne porte pas sur le degré d'efficacité, mais plutôt sur le fait que l'objectif « ne peut raisonnablement être atteint d'une autre manière » selon le CST, alors que le SCRS ne doit que consulter au besoin. Cependant, ces exigences pourraient très bien mettre en avant le besoin de se prêter à un exercice comparatif.

(U) **Conclusion n° 5 : L'OSSNR estime qu'un chevauchement est possible entre les activités du SCRS et celles du CST dès lors que celui-ci fait appel à des capacités dans le but d'exécuter ses COA et ses COD. Toutefois, le CST n'a pas systématiquement consulté le SCRS au sujet des cyberopérations menées par le Centre.**

---

[77] *Loi sur le CST*, paragr. 12.1(3).

[78] Tel qu'il a déjà été indiqué, le volet COA a pour objet de mener 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.

GRC

78. (S) Dans le contexte de l'harmonisation et de la communication d'information relative aux cyberopérations du CST, les équipes COA et COD du CST se sont réunies mensuellement avec l'équipe du renseignement sur la cybercriminalité des Opérations criminelles de la Police fédérale (OCPF) – en plus des réunions ponctuelles – pour échanger des informations et s'assurer qu'il n'y avait pas de conflit avec les dossiers de cybercriminalité sur lesquels la GRC faisait toujours enquête[79]. À titre d'exemple, la GRC a indiqué à l'OSSNR que pendant les réunions mensuelles auxquelles prenaient part le CST et la GRC, L'information communiquée peut contenir

79. (TS//SI//CEO) Pour ce qui concerne l'exigence voulant que les objectifs énoncés dans l'autorisation ne puissent raisonnablement être atteints d'une autre manière, la chef du CST a écrit, au sujet des demandes à visées pendant la période d'examen, que [81] La GRC a confirmé à l'OSSNR que pas une seule fois le CST n'avait pris contact avec la GRC pour déterminer si les objectifs d'une cyberopération du CST pouvaient être atteints par les capacités de la GRC[82]. Cela dit, la GRC considère que [Traduction] « les efforts du CST [en date du 13 avril 2022] visant à établir si une cyberopération pouvait par un organe d'application de la loi étaient suffisants[83]. »

80. (TS) La GRC a indiqué à l'OSSNR que dans le cas d'une COA, la collaboration et la coordination de la GRC avec le CST se [85]. Cependant, hormis les types de collaboration qui lui ont été décrits par la GRC, l'OSSNR note également que la GRC avait envisagé – à certaines mesures de perturbation,

---

[79] Réponse écrite de la GRC à la DI-1 : Questions appelant des réponses écrites, 7 mars 2022. Les principes de coopération entre le CST et la GRC sont énoncés dans le protocole d'entente (PE) conclu entre les deux organismes. La GRC a indiqué à l'OSSNR qu'elle reconnaissait que le PE, qui date de 2009, [Traduction] « ne reflète pas fidèlement les COA et les COD du CST ». La GRC a ajouté qu'elle ferait le nécessaire pour veiller à ce que le PE s'adapte au contexte juridique actuel (réponse de la GRC à la DI-2, 13 avril 2022).

[80] Réponse écrite de la GRC à la DI-1 : Questions appelant des réponses écrites, question 1(a), 7 mars 2022.

[81] Demande de 2020-2021 pour une COA à , paragr. 57; Demande de 2020-2021 pour une COA à , paragr. 37.

[82] Réponse écrite de la GRC à la DI-2, question 5(a) (13 avril 2022), et à la DI-1, question 2 (7 mars 2022).

[83] Réponse écrite de la GRC à la DI-2, question 4, fournie le 13 avril 2022.

[84] Réponse écrite de la GRC à la DI-2, 13 avril 2022. La communication d'information entre la GRC et le CST pourrait poser des difficultés relativement au difficile passage du renseignement à la preuve. Ce passage tient au fait que le renseignement peut contenir des éléments de preuve, mais peut également contenir de l'information qui n'a rien à voir avec la preuve. Par conséquent, des problèmes peuvent se poser lorsque du renseignement exploitable est utilisé pour étayer les enquêtes et les poursuites au criminel. L'OSSNR envisage, à l'occasion d'un examen à venir, de se pencher sur cette difficulté dans le contexte du CST et de la GRC.

[85] Réponse écrite de la GRC à la DI-2, question 3, 13 avril 2022.

[86] Selon la réponse écrite de la GRC à la DI-2, question 6, 13 avril 2022,

[redacted][87].

81. (TS//SI) Une enquête de la GRC [redacted] relativement à l'ensemble [redacted] la GRC [redacted][89]. devait être menée sous la direction de la GRC [redacted] mais en coordination avec [redacted] du CST. [redacted] l'OSSNR ne voit pas comment le CST a pu en arriver à estimer que l'objectif de [redacted] ne pouvait raisonnablement être atteint d'une autre manière.

82. (S) L'harmonisation avec le CST relativement à [redacted] s'est avérée nécessaire pour veiller à ce que les activités du CST [redacted][90]. Dans ce contexte, l'OSSNR a vu [redacted] exemples de communication et d'échange d'information entre le CST et la GRC.

MDN/FAC

83. (U) Toute cyberopération que le CST mène en appui aux FAC s'exécute au titre du volet touchant l'assistance technique et opérationnelle du mandat du Centre, un aspect qui est exclu de la portée du présent examen. Pour ce qui concerne les opérations d'assistance dont elles font elles-mêmes la demande, les FAC sont tenues de consulter AMC, s'il y a lieu, par l'intermédiaire de leurs propres mécanismes (p. ex. le mécanisme conjoint de consultation [avec AMC]), qui sont distincts des mécanismes de consultation que le CST a mis sur pied avec AMC[91].

84. (S) [redacted]

[redacted] Plus généralement, la « perturbation » peut aller de [redacted] à tout type d'incidence sur un service donné.

[87] Courriel : "*RE:* [redacted] courriel: « *RE:* [redacted]

[88] Courriel : « *SITREP on RCMP/OPP Coordination* », [redacted] courriel : « *FW:* [redacted]

[89] Pendant la vérification de l'exactitude des faits (28 septembre 2022), la GRC a nié que le CST lui aurait [redacted] et ce, malgré qu'un courriel tende à montrer le contraire. L'OSSNR note que [redacted]

[90] Réponse écrite de la GRC à la DI-2, question 7, 13 avril 2022.

[91] Document du CST, « [redacted] », diapositive 8.

[92] Ibid., diapositive 7.

[redacted]

85. (TS//SI//CEO) Dans le cas de [redacted] du CST qui avait pour objectif de perturber et d'endommager [redacted] – l'approbation officielle du MDN/FAC n'était pas requise, bien que le MDN/FAC eût été mis au courant de [redacted] et qu'il eût l'occasion de soulever de possibles difficultés auprès du CST[93]. Le MDN/FAC a indiqué à l'OSSNR que les militaires responsables de la planification étaient présents [redacted] Au cours de l'opération [redacted] l'harmonisation avait mis l'accent sur les ressources de [redacted] Ainsi, selon le MDN/FAC, l'harmonisation visant [redacted][94].

86. (U) Le MDN/FAC a indiqué à l'OSSNR qu'à ce jour, le travail réalisé conjointement par le CST et le MDN/FAC dans le cadre des cyberopérations avait été très concluant, et que la communication entre les deux organismes avait été efficace. Au moment de la séance d'information, le MDN/FAC a tenu à préciser qu'il y aurait lieu de perfectionner certains aspects, mais jugeait que la relation avec le CST avait été très bonne pour ce qui concerne ce dossier.

Attestation que d'autres moyens ont été pris en compte

87. (TS//SI//CEO) Quelles que soient les occurrences de consultation ou de mobilisation avec d'autres ministères et organismes du GC pendant la planification et l'exécution des COA et des COD du CST, l'OSSNR a remarqué que les documents de planification des cyberopérations du CST mettaient surtout l'accent sur la rapidité et la facilité avec lesquelles l'objectif des cyberopérations pouvait être atteint et, de façon générale, ne faisaient manifestement pas état de la possibilité que d'autres intervenants puissent atteindre le même objectif par d'autres moyens[95].

(U) **Conclusion n° 6 : L'OSSNR estime qu'en dépit de l'étroite collaboration avec Affaires mondiales Canada et avec le ministère de la Défense nationale et les Forces armées canadiennes dans le cadre de COA et de COD, le CST ne s'est pas suffisamment adressé au SCRS ou à la GRC, lorsqu'il s'est agi d'établir si l'objectif d'une COA ou d'une COD ne pouvait raisonnablement être atteint d'une autre manière.**

(U) **Recommandation n° 4 : L'OSSNR recommande que le CST prenne invariablement contact avec le SCRS, la GRC et tout autre ministère ou organisme concerné du gouvernement fédéral pour déterminer si ces ministères et organismes seraient raisonnablement en mesure d'atteindre l'objectif d'une cyberopération.**

[93] MDN/FAC, DI-1, exposé devant l'OSSNR – Examen des COA/COD, diapositive 9, 27 mai 2022.
[94] Ibid.
[95] À titre d'exemple, les paragraphes 56 à 59 de la demande de 2020-2021 pour une [redacted] se concentrent généralement sur la nécessité de recourir [redacted] ce qui ne sert pourtant pas à justifier que les objectifs d'une cyberopération ne peuvent raisonnablement être atteints d'une autre manière.

Acquisition d'information en contrepoint des COA et des COD

Exigences de la Loi sur le CST et autorisations

88. (U) Tel qu'il est indiqué au paragraphe 34(4) de la *Loi sur le CST*, le MinDN peut délivrer une autorisation de COA ou de COD seulement s'il conclut qu'il y a des motifs raisonnables de croire que l'objectif de la cyberopération ne peut raisonnablement être atteint d'une autre manière et qu'aucune information ne sera acquise au titre de l'autorisation, sauf conformément à une autorisation délivrée pour des motifs de renseignement étranger, de cybersécurité ou de situation d'urgence. Selon l'interprétation de l'OSSNR, ce paragraphe permettrait la collecte d'information dans le cadre d'une cyberopération, pour peu qu'il existe déjà une autorisation valide de renseignement étranger, de cybersécurité ou de situation d'urgence qui permette la collecte au titre de l'un ou l'autre de ces trois volets. Ainsi, la collecte d'information peut avoir lieu au titre d'une autre autorisation qui aurait été délivrée en vertu des paragraphes 26(1), 27(1) ou (2), ou 40(1).

89. (TS//SI) Lors de son examen de la gouvernance, l'OSSNR a constaté que « les politiques internes du CST qui portaient sur la collecte d'information dans le cadre de cyberopérations n'étaient pas décrites avec exactitude dans les autorisations ministérielles pour les cyberopérations actives et défensives[96]. » L'OSSNR avait donc recommandé que dans ses demandes, le CST « 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. »

90. (TS//SI) Dans les demandes de COA et de COD correspondantes à la période d'examen, le CST a interprété le paragraphe 34(4) comme interdisant au CST de s'appuyer sur le pouvoir conféré par les autorisations de COA et de COD pour acquérir de l'information[97]. Les autorisations de COA et de COD en vigueur pendant la période d'examen stipulaient que les catégories d'activités autorisées étaient assujetties à la restriction suivante : [Traduction] « Aucune information ne sera acquise consécutivement au déroulement des activités visées par la présente autorisation »[98]. Selon l'interprétation faite par le CST quant à la restriction du MinDN s'appliquant à la collecte d'information « consécutive » aux activités autorisées, celle-ci [Traduction] « avait pour objet de préciser qu'aucune information ne serait acquise « en vertu » des autorisations délivrées au titre de l'article 18 ou de l'article 19[99] ».

91. (TS//SI//CEO) Cependant, l'OSSNR note que les demandes correspondantes n'avisent pas tout à fait le MinDN que des activités de collecte pourraient avoir lieu pendant une cyberopération ou après la production des effets d'une cyberopération exécutée au titre d'une autorisation de renseignement étranger, de cybersécurité ou de situation d'urgence. Bien que la demande énonce [Traduction] « [qu']aucune information ne sera acquise au moyen des activités menées dans le cadre de cyberopérations [actives ou défensives][100] », la chef du CST précise en disant que toute information

---

[96] Examen de l'OSSNR nº 20-02, conclusion nº 5.
[97] Voir les demandes suivantes : 2021-2022, [redacted] paragr. 73; 2020-2021, [redacted], paragr. 60; [redacted], paragr. 56; 2019, [redacted] paragr. 40.
[98] Consulter le paragr. 11(g) des autorisations de COA et de COD délivrées pour 2019-2020 et 2020-2021 ainsi que le paragr. 9(f) de l'autorisation de 2021-2022 visant à [redacted] À partir de juin 2022, les plus récentes autorisations de COA et de COD contenaient les mêmes interdictions. Voir le paragr. 12(h) des autorisations de COA et de COD délivrées pour 2021-2022; le paragr. 8(e) [redacted] délivrée le 18 mars 2022, et le paragr. 9(e) [redacted] renouvelée le 30 juin 2022.
[99] Réponse écrite du CST, DI-12, question 1.
[100] 2020-2021, [redacted], paragr. 27; 2021-2022, [redacted], paragr. 27; 2021-2022, [redacted] paragr. 28.

nécessaire à l'atteinte du résultat attendu d'une COA ou d'une COD serait acquise au titre d'une autorisation de renseignement étranger, de cybersécurité ou de situation d'urgence déjà en vigueur, et non que de l'information serait collectée à des fins de renseignement étranger *consécutivement* aux effets d'une COA ou d'une COD.

Acquisition d'information résultant de la cyberopération

92. (U) L'OSSNR a examiné de près les détails relatifs à la façon, s'il y a lieu, dont l'information était observée et collectée parallèlement aux cyberopérations. En plus de tenir compte de cette question dans le cas de plusieurs COA et COD, l'OSSNR s'est penché de plus près sur l'une des [redacted] pour analyser la journalisation des données et, le cas échéant, pour prendre connaissance de certains détails opérationnels, notamment, les observations formulées ou l'information acquise avant, pendant et après l'opération au titre de l'une ou l'autre des autorisations applicables.

93. (U) Pendant l'étude des COA et des COD visées par le présent examen, l'OSSNR a conclu que l'observation, la collecte et l'analyse du renseignement étranger constituaient des éléments essentiels des cyberopérations (description détaillée plus loin). Sans la capacité d'acquérir de l'information parallèlement aux cyberopérations, le CST s'en trouverait la plupart du temps freiné dans ses efforts de planification, d'exécution et d'évaluation des cyberopérations, sans compter qu'il risquerait de compromettre sa capacité à collecter du renseignement essentiel.

94. (TS//SI//CEO) En conséquence, le CST doit miser, ce qu'il fait déjà, sur ses pouvoirs en matière de renseignement étranger pour exécuter des cyberopérations; la nécessité de tabler sur la collecte de renseignement pour exécuter les cyberopérations [redacted][101].

95. (TS//SI//CEO) L'OSSNR a tenté de savoir si et comment l'information était acquise au titre de pouvoirs autres que ceux conférés aux [redacted] menées parallèlement à [redacted] en examinant certains aspects des opérations et des activités de renseignement étranger qui ont eu lieu en même temps [redacted][102]. Pour ce faire, l'OSSNR a passé en revue les journaux [redacted][103]. L'OSSNR a également assisté à deux démonstrations effectuées par des opérateurs techniques du CST, pour tenter de mieux comprendre la façon dont les systèmes du CST fonctionnent dans le contexte de ce type d'activité.

96. (TS//SI//CEO) L'OSSNR a été en mesure de vérifier que l'information *avait été* acquise par le CST *consécutivement à* [redacted][104].

---

[101] Concernant les AM de 2021-2022, veuillez consulter : [redacted] *subsection 2(c) and 5(d)*; [redacted] *subsection 10(c)*; et [redacted] *subsection 6(c)*. Même si le CST peut théoriquement avoir recours aux pouvoirs qui lui sont conférés en vertu des mandats de cybersécurité et d'assurance de l'information en plus de ceux qui sont conférés au titre des COA et des COD, l'OSSNR n'a relevé aucune occurrence de ce type de recours pendant la période d'examen, [redacted]

[102] Le CST a indiqué à l'OSSNR [redacted]

[103] Documents du CST : [redacted] Tel qu'il a été dit précédemment, dans le cas qui nous concerne ici, l'activité de perturbation est connue sous l'appellation [redacted]

[104] Par exemple, l'OSSNR s'est penché sur le contenu des journaux [redacted]

[redacted]

97. (TS//SI//CEO) Concrètement, il apparaît évident pour l'OSSNR que la collecte d'information doive avoir lieu « consécutivement » à la cyberopération pour que le CST puisse évaluer l'efficacité de ladite opération. Dans le contexte [redacted] l'OSSNR a remarqué que [redacted]

98. (TS//SI) [redacted], l'OSSNR a noté qu'en pratique, l'information acquise au titre d'une autorisation qui en permet la collecte avait bel et bien lieu consécutivement à une cyberopération, [redacted][108]. Par conséquent, toute observation ou collecte effectuée parallèlement ou après la production de l'effet a lieu consécutivement à l'effet produit.

99. (TS//SI//CEO) L'interprétation que le CST avance concernant les activités concomitantes et l'application des restrictions énoncées dans les autorisations est qu'aucune information ne sera acquise consécutivement aux activités de COA ou de COD. Or, le CST déclare plutôt que [Traduction] « toute l'information à l'appui collectée avant, pendant ou après une opération est collectée en vertu de pouvoirs distincts conférés au titre de l'article 16 [renseignement étranger] ou de l'article 17 [cybersécurité ou assurance de l'information], y compris les autorisations ministérielles et les approbations d'activités », et que : [Traduction] « ces volets distincts du mandat ne sont pas mutuellement exclusifs et peuvent avoir lieu simultanément[109]. »

100. (TS//SI//CEO) Par conséquent, l'OSSNR ne considère pas que les activités de collecte concomitantes ou les activités de collecte consécutives aux cyberopérations soient décrites avec précision ou en toute transparence dans les demandes soumises au MinDN. Bien qu'il puisse être exact de dire que toute activité de collecte n'a lieu qu'en vertu des pouvoirs conférés par une autorisation de renseignement étranger ou de cybersécurité, la possibilité que la collecte ait lieu *consécutivement* à

---

[105] Puisqu'un RPF accompagnait cette information, [redacted] (Réponse écrite du CST à la DI-19, question 3, avec pièces justificatives.)

[106] Réponse écrite du CST à la DI-9, question 7, 29 avril 2022.

[107] Réponse écrite du CST à la DI-16, question 1(a), 25 juillet 2022. D'après le CST, un [redacted]

[108] Lorsque, [redacted] du CST [redacted]

[109] Réponse écrite du CST, DI-12, question 1(a), 16 juin 2022.

une cyberopération n'est pas exactement expliquée au MinDN dans les demandes d'autorisation de COA et de COD visées pendant la période d'examen. Les demandes ne décrivent plutôt que le fait de tabler sur l'information acquise en vertu d'une autorisation de renseignement étranger ou de cybersécurité dans le but de produire le résultat attendu de la cyberopération. En outre, les demandes indiquent [Traduction] « [qu']aucune information ne sera acquise par l'intermédiaire des activités des cyberopérations [actives ou défensives][110] ». Selon l'OSSNR, les demandes du chef doivent contenir suffisamment d'information pour informer le MinDN que la collecte en vertu d'une autorisation valide de renseignement étranger, de cybersécurité ou de situation d'urgence se produira parallèlement ou consécutivement aux cyberopérations – puisque dans les faits, de telles activités ont lieu[111].

101. (U) Accompagnant le projet de loi C-59, *Loi concernant des questions de sécurité nationale*, l'énoncé concernant la Charte faisait une distinction entre, d'une part, les activités de renseignement étranger, de cybersécurité et d'assurance de l'information, et d'autre part, les activités des COA et des COD[112]. Les premières étaient considérées comme ayant la possibilité de porter atteinte à des intérêts en matière de vie privée, ce qui ferait intervenir l'article 8 de la Charte, alors qu'il n'y aurait pas lieu de s'attendre à ce que les activités des COA et des COD portent atteinte à des intérêts en matière de vie privée. Aux fins de conformité à l'article 8 de la Charte, le commissaire au renseignement – un juge à la retraite d'une cour supérieure qui agit en toute indépendance – approuve les activités du renseignement étranger, de la cybersécurité et de l'assurance de l'information, lesquelles sont également approuvées par le ministre, afin de prévenir d'éventuelles atteintes à des intérêts en matière de vie privée. Par contre, l'approbation préalable du commissaire au renseignement n'est pas requise dans le cas des autorisations de COA et de COD, puisque ces activités ne prévoient pas l'acquisition de renseignements personnels sur un Canadien ou une personne se trouvant au Canada, ce qui exclut toute intervention des dispositions de l'article 8.

102. (S) Suivant son analyse pratique des opérations, l'OSSNR a confirmé qu'il y avait un lien causal entre l'effet d'une cyberopération et la collecte d'une information qu'il aurait été impossible de recueillir n'eut été dudit effet. Étant donné que les activités des COA et des COD permettent, dans une certaine mesure, la réalisation d'autres activités ayant le potentiel de porter atteinte à des intérêts en matière de vie privée, il y a lieu de conclure que le raisonnement qui sous-tend les contraintes que le projet de loi C-59 impose au commissaire au renseignement pour ce qui a trait aux autorisations de renseignement étranger et de cybersécurité s'oppose aux observations de l'OSSNR quant au lien causal qu'il y aurait entre les cyberopérations et la collecte de renseignement.

103. (U) Les occurrences où, selon les observations de l'OSSNR, la collecte de renseignement dépend de l'effet d'une cyberopération, mais aussi les questions connexes ayant trait à la transparence du CST à l'égard du commissaire au renseignement et du MinDN pourraient être abordées suivant un élargissement du mandat du commissaire au renseignement au titre de la *Loi sur le commissaire au renseignement*. Il convient de préciser qu'un tel élargissement pourrait comprendre des mesures de surveillances visant à établir si les conclusions tirées en vertu de la *Loi sur le CST* et si les autorisations de COA et de COD qui sont délivrées ou modifies s'avèrent raisonnables.

---

[110] 2021-2022, [redacted] paragr. 28; demande de [redacted] paragr. 73 à 75.
[111] L'OSSNR note que les demandes et les autorisations plus récentes qui n'ont pas été visées par le présent examen indiquaient ce qui suit : [redacted] Voir, à titre d'exemple, le paragraphe 46 de la demande [redacted] datant du 18 mars 2022.
[112] Ministère de la Justice, Énoncé concernant la Charte – projet de loi C-59 : *Loi concernant des questions de sécurité nationale*, 20 juin 2017, accessible à : www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/sn-ns.html

(U) **Conclusion n° 7 : L'OSSNR estime que pendant la période d'examen, les demandes présentées par le chef concernant les activités de cyberopération actives et défensives ne décrivaient pas avec suffisamment de précision le lien causal entre une cyberopération et la collecte de renseignement pouvant résulter de ladite cyberopération.**

(S) **Recommandation n° 5 : L'OSSNR recommande que les demandes présentées par le chef concernant les cyberopérations actives et défensives indiquent au ministre de la Défense nationale qu'une acquisition d'information au titre d'une autorisation dûment délivrée pour le renseignement étranger, la cybersécurité ou l'assurance de l'information pourrait avoir lieu en conséquence desdites cyberopérations.**

104. (U) Pour ce qui a trait aux observations formulées dans son rapport d'examen de la gouvernance concernant la collecte d'information en cours de cyberopération, l'OSSNR a noté que les documents de gouvernance ayant trait aux COA devenaient généralement plus clairs quant à l'expression du fait que la collecte de renseignement étranger pourrait avoir avant, pendant et après une COA et que ces documents incluaient des liens avec des missions connexes de renseignement étranger. Toutefois, ces documents ne contenaient pas de détails indiquant clairement de quelle façon cette collecte de renseignement étranger pourrait avoir lieu.

105. (TS//SI//CEO) De fait, les documents clés, notamment le PCCO, ne contenaient pas toujours les liens ou les références aux missions de renseignement étranger qui accompagnent les cyberopérations. Et lorsqu'elles étaient fournies, les références ne contenaient pas suffisamment de détails[113]. Par exemple, dans le cas de la [redacted] dont le nom de code était [redacted][114], le CST a noté dans son matériel d'évaluation après action que l'opération avait manqué de clarté quant aux opérations simultanées de renseignement menées parallèlement à [redacted]

106. (TS) Pendant l'examen, l'OSSNR a relevé des exemples où [redacted] Ainsi, il conviendrait d'indiquer clairement le lien qui existe entre le PCCO d'une COA ou d'une COD et les activités et objectifs du renseignement étranger – [redacted]. Cette mesure permettrait ainsi de mieux répondre aux exigences s'appliquant au CST en matière de renseignement, mais elle fournirait également à l'opérateur des consignes plus claires [redacted]

[113] Par exemple, le [redacted] ne faisait aucune référence au [redacted] en annexe, alors que [redacted] ne prenait qu'une simple phrase pour indiquer que la collecte de renseignement étranger [redacted]

[114] Le terme [redacted] renvoie à [redacted]

[115] Document du CST, courriel : [redacted].

[redacted] mais aussi quant aux autorisations et aux objectifs qui justifieraient la collecte.

107. (TS//SI) Dans le cas de la [redacted] [116]. Autrement dit, le CST a réalisé des évaluations de risques pour les activités [redacted]

(U) **Conclusion n° 8 : L'OSNR estime que, dans ses plans conjoints de cyberopérations, le CST n'a pas toujours été clair s'agissant des missions de renseignement étranger qui étaient ou auraient pu être menées parallèlement à des COA ou des COD.**

(S) **Recommandation n° 6 : L'OSSNR recommande que les documents préparés selon le cadre des cyberopérations du CST (le Cadre de pouvoirs et de planification commun) fournissent en toute clarté les liens avec toutes les missions de renseignement étranger (ou de cybersécurité) concernées – [redacted] – qui pourraient se dérouler en même temps que les COA ou les COD.**

Distinction entre les COA, les COD et les autres volets du mandat

108. (U) En cours d'examen, l'OSSNR a analysé les liens réciproques entre les activités réalisées au titre des divers volets du mandat du CST : renseignement étranger, cybersécurité et assurance de l'information, sans oublier les COD et les COA. En y regardant de plus près, l'OSSNR a remarqué que sur le plan technique, les activités menées dans le cadre des COA et des COD étaient semblables à celles qui ont lieu pour les volets renseignement étranger et cybersécurité.

109. (U) Il importe de souligner que dans le texte de la *Loi sur le CST*, on note d'importants chevauchements entre ces volets du mandat du CST[117]. En effet, les activités et catégories d'activités qui peuvent être autorisées au titre d'une autorisation de renseignement étranger et qui sont visées au paragraphe 26(2), et les activités et catégories d'activités qui peuvent être approuvées en vertu d'une autorisation de COA ou une COD et qui sont visées à l'article 31 sont les mêmes. La seule différence réside dans le fait que l'autorisation de renseignement étranger délivrée au titre du paragraphe 26(1) permet d'acquérir de l'information dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci[118]. De même, il y a des similitudes entre le volet COD et le volet cybersécurité du mandat du CST. Les deux volets ont pour objet de favoriser la protection des informations électroniques ou des infrastructures de l'information des institutions fédérales ou désignées comme étant importantes pour le gouvernement fédéral. À cette fin, le volet COA permet au CST de mener des activités dans l'IMI ou par l'entremise de celle-ci[119], alors que le volet cybersécurité se concentre sur la formulation d'avis, de conseils et de services tout en favorisant l'acquisition d'information[120].

---

[116] Document du CST, [redacted].
[117] Cela n'inclut pas les activités menées en vertu du volet assistance du mandat du CST, article 20 de la *Loi sur le CST*.
[118] *Loi sur le CST*, alinéa 26(2)b).
[119] *Loi sur le CST*, art. 18.
[120] *Loi sur le CST*, art. 17.

110. (TS//SI) Pour marquer la distinction entre une activité de renseignement étranger et une activité réalisée aux fins d'une COA ou d'une COD, dès lors que ces activités ont recours aux mêmes techniques, le CST met l'accent sur l'objectif de l'activité, ce qui lui permet d'établir si ladite activité est menée à des fins de renseignement étranger ou de cyberopération[121]. Cette approche est manifeste, par exemple, lorsque le CST utilise le comme technique à la fois de renseignement étranger et de . Dans les demandes de renseignement étranger nécessitant des autorisées en vertu du paragraphe 26(1) de la *Loi sur le CST*, le chef du CST déclare que les du CST pourraient exercer des activités au titre d'une autorisation de cyberopérations délivrée en vertu des articles 29 et 30 de la *Loi sur le CST*[122]. Dans les autorisations correspondantes, plus précisément dans l'argumentaire du MinDN concernant la raisonnabilité des activités autorisées, celui-ci reconnaît que les pourraient être utilisées dans le but de permettre et de faciliter le déroulement des cyberopérations[123].

111. (TS//SI) Par exemple, (notamment,) peuvent produire un effet qui soit en mesure de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités des entités ciblées. Dans le cas de la laquelle s'appuyait uniquement sur , l'OSSNR a observé que cette utilisation visait à En l'occurrence, ce type a un rapport direct avec l'objectif de la . Par contraste, une opération de renseignement étranger peut aussi avoir recours à la [124]. Dès lors qu'il est en mesure d'établir ce type de distinction entre les divers objectifs à atteindre au moyen de cette technique, l'OSSNR parvient à voir la différence entre, d'une part, les activités de renseignement étranger et de cybersécurité ou d'autre part, celles des COA et des COD.

112. (TS//SI) L'interdépendance entre les volets du mandat du CST est décrite plus avant dans les demandes de de 2021-2022[125]. Dans ces demandes, aux autres techniques employées pour le renseignement étranger, le CST a ajouté l'utilisation de la en tant que moyen raisonnable de faciliter les cyberopérations. Les autorisations correspondantes permettaient au CST de mener toute activité qui puisse s'avérer raisonnable en de telles circonstances, pour peu qu'elle appuie l'une ou l'autre des activités permises par l'autorisation ainsi que les mesures raisonnablement nécessaires à la protection de la nature secrète des activités[126]. En l'occurrence, il est clairement indiqué que les peuvent à la fois produire des effets et viser des objectifs de renseignement étranger.

---

[121] Réponse écrite du CST à la DI-6, question 9, 4 mars 2022.
[122] Demande de paragr. 8.
[123] Autorisation de , paragr. 10(c).
[124] Prenons, à titre d'exemple, la description énoncée au paragraphe 2(d) de l'AM de Cette description indique que le CST peut,
[125] Demande de pour 2020-2021, paragr. 28; demande de pour 2020-2021, paragr. 18. Voir également demande de pour 2021-2022, paragr. 28(d); demande de pour 2021-2022, paragr. 16.
[126] pour 2020-2021, paragr. 7 et 8; pour 2020-2021, paragr. 7 et 8. Dans les autorisations à pour 2021-2022, l'utilisation des a été spécifiquement autorisée. Voir l'autorisation de pour 2021-2022, paragr. 7 et 8; autorisation de pour 2021-2022, paragr. 8 et 9.

COA ou COD?

113. (TS//SI) Bien qu'il soit satisfait de la façon dont le CST distingue les techniques, pourtant semblables, qui sont employées à la fois dans le cadre des volets de renseignement étranger et de cybersécurité ainsi que dans les volets COA et COD, l'OSSNR se demande encore de quelle façon le CST établit une distinction entre le volet COA et le volet COD[127].

114. (U) Dans le texte de la *Loi sur le CST*, on note de nombreuses similitudes entre les COA et les COD. Or, les activités et catégories d'activités citées à l'article 31 qui peuvent être permises au titre d'autorisations de cyberopérations s'avèrent identiques. L'interdiction visée à l'article 32 ainsi que l'exigence interdisant que les activités des cyberopérations visent toute portion de l'IMI se trouvant au Canada[128] s'appliquent à la fois aux COA et aux COD. Néanmoins, la *Loi sur le CST* établit une nette distinction entre le volet COA et le volet COD, comme l'énoncent les articles 18 et 19[129]. En outre, la Loi fait une distinction entre la fin pour laquelle les activités de COA et de COD autorisées sont menées (c.-à-d. assurer le bon fonctionnement des volets COA et COD du mandat du CST) et le processus s'appliquant aux autorisations correspondantes : pour ce qui concerne les autorisations de COD, le MinDN doit consulter le MinAE, alors que dans le cas des COA, le MinDN ne peut délivrer une autorisation que si le MinAE le demande ou y consent[130]. Ainsi, compte tenu de ces distinctions établies dans la *Loi sur le CST*, il est essentiel que le CST définisse clairement ce qui distingue les COA des COD.

115. (S) L'OSSNR note une apparente différence de nature entre les COD. En effet, certaines COD ont été conçues en vue d'une menace potentielle, notamment la COD planifiée [redacted] qui se concentrait sur la sécurité du système électoral. Par contre, d'autres COD ont été conçues pour renforcer les mécanismes de défense contre une menace [redacted] qui a occasionné et continue d'occasionner des dommages à l'information électronique et à l'infrastructure de l'information des institutions fédérales et des systèmes désignés comme étant d'importance pour le GC. À titre d'exemple pour ce dernier élément, rappelons [redacted] qui visait à contrer la cybercriminalité. En effet, cette COD avait pour but de riposter à une menace persistante issue d'un utilisateur de rançongiciels.

116. (TS//SI) Bien que cette opération ait été planifiée en tant que COD, l'OSSNR a remarqué que le CST aurait également pu planifier [redacted] en tant que COA, puisqu'elle correspondait à la

---

[127] Examen 2020-02 de l'OSSNR, conclusion nº 4. À ce sujet, l'une des principales sources de préoccupation exprimée par l'OSSNR dans le rapport d'examen de la gouvernance était le risque que le CST exécute une COD qui ressemble à une COA sans avoir consulté le MinAE ou AMC. Toutefois, la confirmation voulant qu'AMC fournisse une autorisation à FRPE pour les COA *et* les COD atténue le degré de préoccupation de l'OSSNR.

[128] *Loi sur le CST*, alinéa 22(2)a).

[129] 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; et b) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telle en vertu du paragraphe 21(1). » 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. »

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

description du volet COA énoncée dans la *Loi sur le CST*[131]. Par exemple, dans [redacted] Il serait plausible de considérer que cette opération avait pour objet d'interrompre ou de contrecarrer les capacités d'une organisation étrangère dont les activités se rapportaient à la défense ou à la sécurité. Conséquemment, l'opération aurait pu être correspondre à la définition d'une COA.

117. (TS//SI) Même s'il a remarqué que la COD planifiée [redacted] affichait également les caractéristiques d'une COA, l'OSSNR note que le CST exposait clairement, dans la documentation sur le cadre des cyberopérations, les raisons pour lesquelles les objectifs et la nature de [redacted] répondaient aux critères définissant une COD, tel qu'ils étaient énoncés dans la *Loi sur le CST* et dans l'autorisation s'appliquant aux COD à [redacted] Par exemple, le [redacted] faisait état de la menace que la cible [redacted] posait pour l'information électronique et les infrastructures de l'information des institutions canadiennes et pour les systèmes d'importance pour le GC[132]. À ce titre, le [redacted] Compte tenu du chevauchement entre les COD et les COA que l'on peut constater dans la *Loi sur le CST*, l'OSSNR continuera d'évaluer les différences entre les COA et les COD du CST, mais aussi la manière selon laquelle le CST établit qu'une opération doit être menée en tant que COA ou en tant que COD.

(U) **Conclusion n° 9 : L'OSSNR estime que les COA et les COD du CST qui ont été exécutées ou planifiées avant le 30 juillet 2021, y compris les quatre études de cas analysées dans le cadre de la présente, étaient conformes à la loi.**

(U) **Conclusion n° 10 : L'OSSNR estime qu'il y a un important chevauchement entre les activités menées au titre du volet COA et du volet COD du mandat du CST, mais aussi, plus généralement, entre les quatre volets du mandat du CST.**

(U) **Recommandation n° 7 : L'OSSNR recommande que le CST continue de définir et de perfectionner les distinctions qu'il convient d'établir entre les activités menées au titre des divers volets de son mandat, particulièrement entre les activités des COA et des COD, mais aussi entre les activités de renseignement étranger et de cybersécurité.**

---

[131] L'OSSNR note que l'argument selon lequel le CST avait planifié [redacted] en tant que COD était que [redacted] (CST, présentation à l'OSSNR en réponse à la DI-05, 17 février 2022).

[132] Document du CST, [redacted] GCDocs [redacted]

VI. RÉACTIVITÉ DU CST ET COMMUNICATION D'INFORAMTION

Réactivité et rapidité

118. (U) Malgré certaines améliorations apportées vers la fin de la période d'examen, l'OSSNR a été contraint de composer avec des retards importants et déraisonnables après avoir demandé au CST de lui fournir l'information essentielle à la tenue du présent examen, particulièrement dans le cas de la première DI présentée par l'OSSNR, cas qui a d'ailleurs été soulevé par la présidente de l'OSSNR lors d'une rencontre avec la chef du CST. L'OSSNR a communiqué deux avis d'information au CST, lesquels sont joints à la présente.

119. (U) L'OSSNR souhaitait que le présent examen serve à mettre à l'essai diverses formes d'accès direct aux fonds de renseignements du CST dans le cadre d'un mouvement devant permettre la vérification des renseignements[133]. Toutefois, pendant la période du présent examen, le CST n'a jamais consenti à ce que des progrès soient réalisés quant à l'accès à ses fonds de renseignements.

120. (U) En réponse à la première DI de l'OSSNR, le CST a tardivement remis environ 45 000 documents. Les mots clés que le CST a employés pour trouver des documents et les remettre à l'OSSNR comportaient d'importantes omissions – notamment l'omission d'au moins [redacted] COA dont l'étape de la planification était passablement avancée. De plus, l'OSSNR note que le CST a établi ses propres modalités de réponses à la première DI, une approche que l'OSSNR juge inefficace, lourde et lacunaire. Hormis les préoccupations à l'égard de l'efficacité des processus externes du CST, l'OSSNR s'inquiète de l'incidence des argumentaires inexacts et incomplets qui sont véhiculés auprès des employés du CST au sujet, tout d'abord, des examens, mais aussi, plus généralement, au sujet du degré de confiance entre les employés du CST et ceux de l'OSSNR.

121. (U) L'OSSNR estime également que le degré de réactivité de la GRC lui avait posé certaines difficultés dans le contexte du présent examen.

122. (U) En revanche, l'OSSNR était satisfait de la réactivité d'AMC, du SCRS et du MDN/FAC, qui ont fourni l'information et répondu aux questions conformément aux attentes de l'OSSNR.

Solution problématique du CST et communication d'information

123. (U) En septembre 2021, unilatéralement et sans explication ni consignes, le CST a imposé à l'OSSNR un nouveau système de technologie de l'information pour la fourniture des documents du CST, lequel système comportait des paramètres particulièrement restrictifs pour les utilisateurs. En plusieurs occasions, l'OSSNR a indiqué au CST que le système ne convenait pas aux besoins de l'OSSNR pour ce qui concerne la tenue des examens. En outre, l'OSSNR a clairement exigé que des solutions soient apportées, mais en contrepartie, le CST n'a apporté aucune solution à la majorité des

[133] Pour obtenir de plus amples informations concernant les besoins de l'OSSNR en matière de vérification des informations, prière de lire les rapports annuels publics de 2020 et de 2021, que l'on peut consulter depuis le site Web due l'OSSNR : https://nsira-ossnr.gc.ca. Voir également « Les attentes de l'OSSNR en matière de réponse aux examens » : https://nsira-ossnr.gc.ca/fr/expectations-for-responsiveness-in-reviews.

problèmes que l'OSSNR a soulevés pendant l'examen.

VII. CONCLUSION

124. (S) Au 30 janvier 2021, le CST avait approuvé cinq COA et une COD depuis l'entrée en vigueur de la *Loi sur le CST*, le 1er août 2019[134]. En l'occurrence, le CST [redacted] n'a pas réalisé la COD. L'OSSNR est également au fait de [redacted] par le CST au plus tard en avril 2022. Du reste, l'OSSNR remarque que la pandémie de COVID-19 a apporté son lot de difficultés, ce qui a empêché le CST de réaliser les COA et les COD comme prévu pendant les années 2020 et 2021.

125. (U) Pendant la période d'examen, le CST a globalement considéré que l'exécution de ses COA avait été réussie et que la planification de la COD avait comporté certains avantages, bien qu'elle n'ait pas été réalisée. En outre, l'efficacité est l'un des facteurs que l'OSSNR n'a pas été en mesure d'évaluer à l'occasion du présent examen.

126. (U) L'OSSNR a remarqué que le CST avait développé et amélioré ses processus s'appliquant à la planification et à la conduite des COA et des COD, répondant ainsi à certaines observations que l'OSSNR avait formulées dans son rapport d'examen de la gouvernance. Lorsqu'il analyse de près les cyberopérations du CST et les activités connexes, l'OSSNR est mieux à même de comprendre la façon dont les cyberopérations du CST sont menées, notamment, sur le plan des relations que ces cyberopérations peuvent avoir avec d'autres volets du mandat du CST. L'examen de l'OSSNR a permis de soulever quelques questions concernant la façon dont certains aspects des cyberopérations sont décrits dans les documents d'autorisation et concernant les difficultés rencontrées lorsqu'il s'agit de mener les cyberopérations dans la stricte observation des dispositions de la *Loi sur le CST*. Par ailleurs, l'OSSNR continuera d'examiner les cyberopérations du CST, dans la mesure où celles-ci ne cessent d'évoluer et de comporter de nouvelles caractéristiques.

127. (U) Compte tenu des importants changements apportés au mandat du CST depuis l'entrée en vigueur de la *Loi sur le CST*, l'OSSNR s'attendait à un niveau élevé de soutien et de transparence de la part du CST pendant la réalisation du présent examen. Malgré que ces attentes aient été clairement exprimées, l'OSSNR n'a pas été satisfait du degré d'accès à l'information du CST durant la période d'examen. Il a d'ailleurs fait part de ses préoccupations au sujet des retards dans la remise des informations par le CST et au sujet du caractère souvent incomplet de ces informations. Les difficultés relatives à l'accès à l'information du CST ont eu une incidence négative sur la qualité et la profondeur du présent examen, mais aussi sur la satisfaction de l'OSSNR quant à la complétude des informations reçues.

[134] Ces données ne tiennent pas compte des [redacted] au titre du volet assistance technique et opérationnelle du mandat du CST.

ANNEXE A : Séances d'information

128. (U) La présente annexe énumère les séances d'information reçues de la part des intervenants concernés par le présent examen. Cette énumération ne comprend pas les réunions tenues avec les homologues du domaine de la surveillance, mais fait plutôt état des principales séances d'information qui ont été tenues en présence d'experts et qui ont alimenté le présent rapport. Les séances d'information énumérées ci-dessous ont eu lieu selon diverses formules, notamment, des réunions en personne et des vidéoconférences protégées.

(S) Séances d'information :

- **22 septembre 2021** : séance d'information du CST concernant la [redacted]
- **10 novembre 2021** : séance d'information d'AMC concernant le rôle d'AMC dans les COA et les COD.
- **25 novembre 2021** : séance d'information du CST portant sur la structure et le fonctionnement de l'équipe responsable des cyberopérations étrangères (COE) du CST et sur la façon dont cette équipe travaille avec d'autres unités du CST.
- **17 février 2022** : séance d'information du CST concernant les opérations [redacted]
- **22 mars 2022** : séance d'information du SCRS concernant l'étendue de la participation du SCRS à certaines COA et COD du CST.
- **16 mai 2022** : démonstration technique du CST concernant les outils, les systèmes et les techniques employées dans le contexte d[redacted]
- **27 mai 2022** : séance d'information du MDN/FAC concernant la participation du MDN/FAC aux COA et COD du CST, et concernant [redacted]
- **5 août 2022** : démonstration technique du CST concernant l'acquisition et l'analyse de l'information [redacted]

ANNEXE B : Mises à jour apportées à la gouvernance des COA et des COD du CST

Gouvernance

129. (U) Vers le mois d'avril 2021, le CST a actualisé son Cadre de pouvoirs et de planification commun (CPPC) pour les COA et les COD, cadre suivant lequel le CST planifie et mène ses COA et ses COD (le présent rapport désigne le CPPC par l'appellation « cadre des cyberopérations » du CST). Le CPPC actualisé devait apporter des éclaircissements relativement à ceux qui doivent être consultés et ceux qui sont appelés à approuver les cyberopérations. Il devait également établir une distinction entre les trois éléments suivants : ressources et planification, évaluation des risques et conformité aux autorisations[135]. Le principal changement apporté au CPPC consistait en l'ajout d'un nouveau document, à savoir le Document énonçant les pouvoirs liés aux cyberopérations conjointes (JCAD pour *Joint Cyber Authorities Document*).

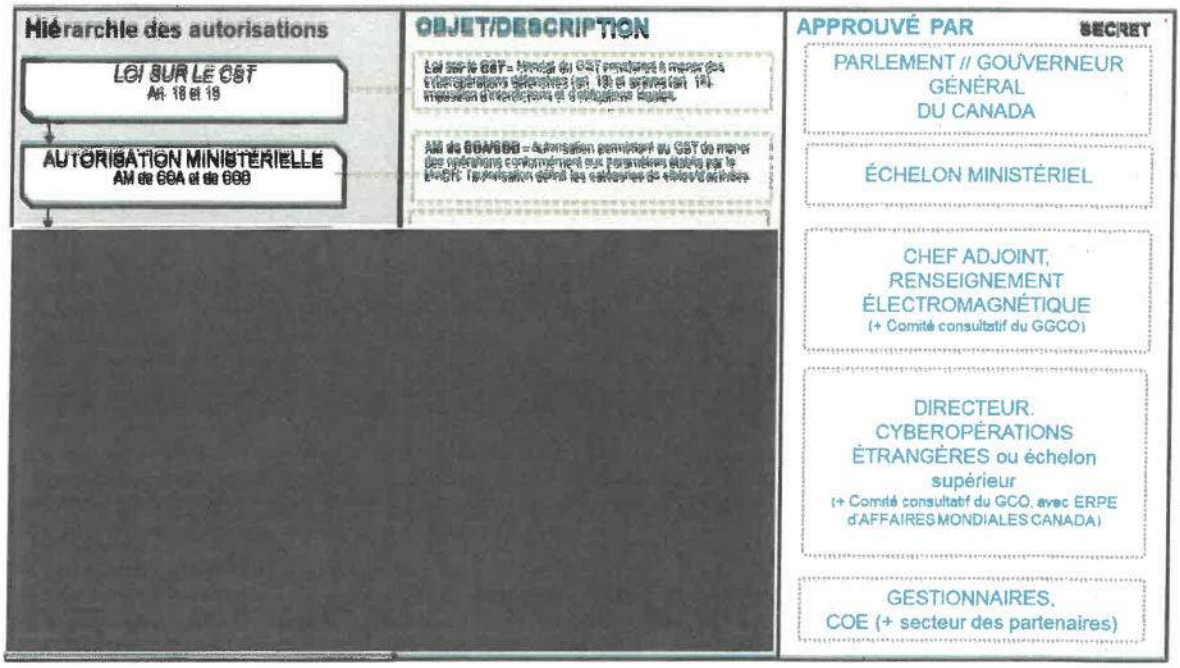
130. (U) Le JCAD est un document stratégique de haut niveau qui classe les autorisations de cyberopérations par thèmes, [redacted] Le JCAD a pour objet de présenter clairement les autorisations du CST en fonction des cibles et des activités, mais aussi d'évaluer les risques au niveau du cadre[137]. [redacted] les JCAD [redacted]

131. (S) Au nombre des exemples de JCAD relevés par l'OSSNR, notons un JCAD [redacted][138]. Parmi les autres JCAD qui ont été soulevés par le CST pendant la période d'examen, [redacted]

132. (S) À titre de nouvelle mise à jour depuis l'examen précédent de l'OSSNR, les JCAD s'accompagnaient également d'un [redacted], lequel existe en plus des [redacted] standards s'appliquant à des opérations particulières. La figure présentée ci-après donne un aperçu du CPPC actualisé en avril 2021 :

[135] Document du CST, « *JPAF evolution – Overview* », diapositive 3.
[136] Terme employé en interne par le CST pour décrire la notion de « thème » (*theme*) est « ligne d'effort » (*line of effort*).
[137] DI-2 présentée au CST, exposé devant l'OSSNR, 22 septembre 2021.
[138] Document du CST, [redacted] Les opérations menées pendant la période d'examen au titre de ce [redacted]

Figure 1 : CPPC actualisé[139]



[139] Créé par le CST en vue de l'exposé devant l'OSSNR présenté le 22 septembre 2021.

ANNEXE C : Recommandations faisant suite à l'examen de l'OSSNR sur la gouvernance du CST s'appliquant aux COA et aux COD

Recommandation n° 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 n° 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 n° 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 n° 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 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.

Recommandation n° 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 n° 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 n° 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 n° 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.

ANNEXE D : Réponses aux demandes d'information présentées par l'OSSNR

Organisme	N° de DI	Type	Demande	Échéance	Réception	Nombre de jours d'avance ou de retard[140]
CST	1	Documents[141]	30 juillet 2021	20 août 2021	25 mars 2022	157
CST	2	Séance d'information	7 juin 2021	16 juillet 2021	22 septembre 2021	50
AMC	1	Documents	24 septembre 2021	13 octobre 2021	21 octobre 2021	6
AMC	2	Séance d'information	24 septembre 2021	10 novembre 2021	10 novembre 2021	0
CST	3	Séance d'information et réponse écrite	15 octobre 2021	5 novembre 2021	25 novembre 2021	14
CST	4	Réponse écrite	22 novembre 2021	10 décembre 2021	15 décembre 2021	3
CST	5	Séance d'information	19 janvier 2022	17 février 2022	17 février 2022	0
GRC	1	Réponse écrite	20 janvier 2022	7 mars 2022	7 mars 2022	0
AMC	3	Réponse écrite	23 janvier 2022	15 février 2022	15 février 2022	0
SCRS	1	Séance d'information	23 janvier 2022	28 mars 2022	22 mars 2022	-4
CST	6	Réponse écrite	24 janvier 2022	4 mars 2022	4 mars 2022	0
CST	7	Réponse écrite	4 mars 2022	28 mars 2022	29 avril 2022	26
CST	8	Réponse écrite	4 mars 2022	8 avril 2022	29 avril 2022	17
CST	9	Réponse écrite	4 mars 2022	28 mars 2022	16 mai 2022	37
CST	10	Démonstration technique	4 mars 2022	16 mai 2022	16 mai 2022	0
GRC	2	Réponse écrite	17 mars 2022	13 avril 2022	13 avril 2022	0
SCRS	2	Réponse écrite	30 mars 2022	25 avril 2022	3 mai 2022	8
MDN/FAC	1	Séance d'information	8 avril 2022	27 mai 2022	27 mai 2022	0
AMC	4	Réponse écrite	4 mai 2022	6 juin 2022	6 juin 2022	0
CST	11	Réponse écrite	5 mai 2022	19 mai 2022	16 mai 2022	-3
CST	12	Réponse écrite	24 mai 2022	15 juin 2022	15 juin 2022	0
CST	13	Documents	26 mai 2022	22 juin 2022	15 juin 2022	-5
MDN/FAC	2	Documents	27 mai 2022	13 juin 2022	6 juin 2022	-5
CST	14	Réponse écrite	17 juin 2022	5 juillet 2022	5 juillet 2022	0
CST/MJ	15	Réponse écrite	27 juin 2022	6 juillet 2022	7 juillet 2022	1
CST	15	Documentation	28 juin 2022	6 juillet 2022	6 juillet 2022	0
CST	16	Réponse écrite	6 juillet 2022	25 juillet 2022	25 juillet 2022	0
AMC	5	Réponse écrite	15 juillet 2022	1er août 2022	29 juillet 2022	-1

[140] Les données de cette colonne ne tiennent pas compte des jours fériés.
[141] Dans le cas de cette DI, par laquelle on demandait une important volume documentaire, le CST a reçu certains documents dès septembre 2021, alors que la majorité des documents n'ont été fournis qu'à la mi-novembre 2021.

CST	17	Documents	15 juillet 2022	28 juillet 2022	28 juillet 2022	0
CST	18	Démonstration technique	21 juillet 2022	12 août 2022	9 août 2022	-3
CST	19	Réponse écrite	5 août 2022	26 août 2022	26 août 2022	0
CST	20	Réponse écrite	16 août 2022	30 août 2022	26 août 2022	-2
CST	21	Réponse écrite	28 septembre 2022	12 octobre 2022	12 octobre 2022	0

ANNEXE E : Conclusions et recommandations

Conclusions

(U) **Conclusion nº 1 :** L'OSSNR estime que le processus appliqué par AMC pour évaluer les risques pour la politique étrangère, tel qu'il s'applique aux évaluations juridiques internationales, s'est amélioré depuis l'examen de la gouvernance régissant les COA et les COD du CST.

(U) **Conclusion nº 2 :** L'OSSNR est d'avis qu'AMC ne dispose pas des capacités lui permettant d'évaluer en toute indépendance les risques pouvant découler des techniques employées par le CST en cours de COA ou de COD

(U) **Conclusion nº 3 :** L'OSSNR estime que le CST et le ministère de la Justice ont affiché une compréhension approfondie des dispositions de l'article 32 de la *Loi sur le CST*. Toutefois, à l'étape de [redacted], le CST pourrait consulter le ministère de la Justice de façon plus appropriée, ce qui lui permettait de vérifier si l'évaluation de la conformité aux lois demeure valide.

(S) **Conclusion nº 4 :** L'OSSNR estime que les demandes d'autorisation que le CST a soumises au titre des paragraphes 29(1) et 30(1) de la *Loi sur le CST* relativement aux activités [redacted] ne contenaient pas toutes les informations nécessaires pour établir de façon éclairée si les exigences visées aux paragraphes 34(1) et (4) de la *Loi sur le CST* avaient été respectées.

(U) **Conclusion nº 5 :** L'OSSNR estime qu'un chevauchement est possible entre les activités du SCRS et celles du CST dès lors que celui-ci fait appel à des capacités dans le but d'exécuter ses COA et ses COD. Toutefois, le CST n'a pas systématiquement consulté le SCRS au sujet des cyberopérations menées par le Centre.

(U) **Conclusion nº 6 :** L'OSSNR estime qu'en dépit de l'étroite collaboration avec Affaires mondiales Canada et avec le ministère de la Défense nationale et les Forces armées canadiennes dans le cadre de COA et de COD, le CST ne s'est pas suffisamment adressé au SCRS ou à la GRC, lorsqu'il s'est agi d'établir si l'objectif d'une COA ou d'une COD ne pouvait raisonnablement être atteint d'une autre manière.

(U) **Conclusion nº 7 :** L'OSSNR estime que pendant la période d'examen, les demandes présentées par le chef concernant les activités de cyberopération actives et défensives ne décrivaient pas avec suffisamment de précision le lien causal entre une cyberopération et la collecte de renseignement pouvant résulter de ladite cyberopération.

(U) **Conclusion nº 8 :** L'OSNR estime que, dans ses plans conjoints de cyberopérations, le CST n'a pas toujours été clair s'agissant des missions de renseignement étranger qui étaient ou auraient pu être menées parallèlement à des COA ou des COD.

(U) **Conclusion nº 9 :** L'OSSNR estime que les COA et les COD du CST qui ont été exécutées ou planifiées avant le 30 juillet 2021, y compris les quatre études de cas analysées dans le cadre de la présente, étaient conformes à la loi.

(U) **Conclusion nº 10 :** L'OSSNR estime qu'il y a un important chevauchement entre les activités menées

au titre du volet COA et du volet COD du mandat du CST, mais aussi, plus généralement, entre les quatre volets du mandat du CST.

Recommandations

(U) **Recommandation n° 1 :** L'OSSNR recommande qu'AMC perfectionne ses capacités ou en élabore de nouvelles pour être en mesure d'évaluer en toute indépendance les risques pouvant découler des techniques employées par le CST en cours de COA ou de COD.

(U) **Recommandation n° 2 :** L'OSSNR recommande que le ministère de la Justice soit pleinement consulté à toutes les étapes d'une COA ou d'une COD, particulièrement à celles qui sont en amont de l'exécution de l'opération.

(S) **Recommandation n° 3 :** L'OSSNR recommande que le CST renonce à la pratique donnant lieu à la présentation de demandes de COA et de COD génériques (c.-à-d. [redacted]) au ministre de la Défense nationale, et qu'il soumette plutôt des demandes ponctuelles [redacted]

(U) **Recommandation n° 4 :** L'OSSNR recommande que le CST prenne invariablement contact avec le SCRS, la GRC et tout autre ministère ou organisme concerné du gouvernement fédéral pour déterminer si ces ministères et organismes seraient raisonnablement en mesure d'atteindre l'objectif d'une cyberopération.

(S) **Recommandation n° 5 :** L'OSSNR recommande que les demandes présentées par le chef concernant les cyberopérations actives et défensives indiquent au ministre de la Défense nationale qu'une acquisition d'information au titre d'une autorisation dûment délivrée pour le renseignement étranger, la cybersécurité ou l'assurance de l'information pourrait avoir lieu en conséquence desdites cyberopérations.

(S) **Recommandation n° 6 :** L'OSSNR recommande que les documents préparés selon le cadre des cyberopérations du CST (le Cadre de pouvoirs et de planification commun) fournissent en toute clarté les liens avec toutes les missions de renseignement étranger (ou de cybersécurité) concernées – [redacted] – qui pourraient se dérouler en même temps que les COA ou les COD.

(U) **Recommandation n° 7 :** L'OSSNR recommande que le CST continue de définir et de perfectionner les distinctions qu'il convient d'établir entre les activités menées au titre des divers volets de son mandat, particulièrement entre les activités des COA et des COD, mais aussi entre les activités de renseignement étranger et de cybersécurité.