Cour fédérale Federal Court

~~**TRÈS SECRET**~~

Date : 20260226

Dossier : C-6-24

Référence : 2026 CF 269

Ottawa (Ontario), le 26 février 2026

En présence de : madame la juge Kane

ENTRE :

DANS L'AFFAIRE concernant la demande de mandats présentée par […] au titre des articles 12.1 et 21.1 de la *Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, c C-23

ET DANS L'AFFAIRE VISANT DES CYBERACTIVITÉS D'ESPIONNAGE, DE SABOTAGE ET D'INGÉRENCE ÉTRANGÈRE ET DES RÉSEAUX DE ZOMBIES

MOTIFS

[1] Malgré le fait que la *Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, c C-23 [*Loi sur le SCRS*] prévoit la délivrance de mandats autorisant des mesures pour réduire les menaces envers la sécurité [les mesures] depuis plusieurs années, la présente demande est la toute première présentée à l'égard de telles mesures. Déposée le 24 avril 2024 au titre des articles 12.1 et 21.1 de la *Loi sur le SCRS*, la demande visait l'obtention de pouvoirs par mandat en vue de réduire la menace que représentent les adversaires étrangers à l'égard des infrastructures essentielles en raison de l'infection de certains appareils par des logiciels malveillants [le mandat autorisant des mesures de réduction de la cybermenace ou le mandat autorisant des mesures]. Il s'agit de la toute première demande de mandat autorisant des mesures,

et la Cour a nommé un *amicus curiae* [*amicus*], M. Solomon Friedman, qui est avocat et détient la cote de sécurité nécessaire, afin qu'il puisse aider la Cour, notamment en passant en revue le témoignage du déposant et les observations de l'avocat du Procureur général du Canada [PGC].

[2] Ayant conclu que les exigences prévues à l'article 21.1 ont été remplies, notamment, que la menace à la sécurité du Canada est clairement identifiée et imminente et que les pouvoirs conférés par le mandat sont nécessaires pour la contrer, la Cour a accueilli la demande et a décerné le mandat autorisant des mesures de réduction de la cybermenace le 1er mai 2024. La durée initiale du mandat était de 120 jours. Le 29 août 2024, la Cour a renouvelé le mandat autorisant des mesures de réduction de la cybermenace pour une période supplémentaire de 120 jours. La Cour a décidé de donner de brefs motifs étayant sa décision d'accueillir la demande initiale.

[3] Bien qu'ils soient tardifs, voici ces motifs.

I. Aperçu

[4] Par la présente demande, le Service canadien du renseignement de sécurité [le SCRS ou le Service] a demandé que des pouvoirs lui soient conférés par mandat afin de protéger des infrastructures essentielles contre des adversaires étrangers qui, au moyen d'un logiciel malveillant, ont infecté des serveurs, des routeurs de l'informatique individuelle et des petites entreprises ainsi que des appareils de l'Internet des objets (notamment, des objets de la vie de tous les jours qui peuvent se connecter à l'Internet, tels que des sonnettes électroniques « Ring »,

des caméras de sécurité, des télévisions ou d'autres appareils connectés à un réseau Wi-Fi) basés au Canada. Le logiciel malveillant entraîne ces serveurs, routeurs et appareils à se comporter comme un réseau d'appareils infectés, qu'on appelle « réseau de zombies ».

[5] La stratégie du SCRS consiste à neutraliser les réseaux de zombies […]. Comme on l'a expliqué à la Cour, les appareils sont identifiables, mais il n'est pas nécessaire que le SCRS en identifie les propriétaires ou les utilisateurs. La stratégie ne vise que les appareils; ni l'identité des utilisateurs ni le contenu des appareils ne sont recueillis.

[6] Le SCRS demande un mandat parce que les mesures nécessaires pour neutraliser les réseaux de zombies […]. Il est fort probable que ces mesures constituent des infractions prévues au *Code criminel*, LRC 1985, c C-46 [*Code criminel*]. En conséquence, ces mesures nécessitent une autorisation judiciaire préalable en application du paragraphe 12.1(3.4) de la *Loi sur le SCRS*.

II. Les dispositions législatives

[7] La *Loi sur le SCRS* autorise le SCRS à prendre des mesures, sans mandat, en vue de contrer des menaces par divers moyens. Toutefois, dans certaines circonstances, des pouvoirs conférés par mandat peuvent s'avérer nécessaires; c'est le cas en l'espèce.

[8] La définition du terme « menaces envers la sécurité du Canada » figure à l'article 2 de la *Loi sur le SCRS*. Certaines activités constituent des menaces, notamment :

a) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage;	**(a)** espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
b) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque; …	**(b)** foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person…

[9] L'article 12.1 autorise le SCRS à prendre des mesures pour réduire les menaces à la sécurité du Canada et prévoit les critères entourant leur autorisation.

[10] L'article 12.1 prévoit ce qui suit :

Mesures pour réduire les menaces envers la sécurité du Canada	**Measures to reduce threats to the security of Canada**
12.1 (1) S'il existe des motifs raisonnables de croire qu'une activité donnée constitue une menace envers la sécurité du Canada, le Service peut prendre des mesures, même à l'extérieur du Canada, pour réduire la menace.	**12.1 (1)** If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.
Limites	**Limits**
(2) Les mesures doivent être justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, des solutions de rechange acceptables pour réduire la menace et des conséquences raisonnablement prévisibles sur les tierces parties, notamment sur leur droit à la vie privée.	**(2)** The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat and the reasonably foreseeable effects on third parties, including on their right to privacy.
Autres options	**Alternatives**
(3) Avant de prendre des mesures en vertu du paragraphe (1), le Service consulte, au	**(3)** Before taking measures under subsection (1), the Service shall consult, as appropriate,

besoin, d'autres ministères ou organismes fédéraux afin d'établir s'ils sont en mesure de réduire la menace.

[…]

Mandat — Charte canadienne des droits et libertés

(3.2) Le Service ne peut, en vertu du paragraphe (1), prendre des mesures qui limiteraient un droit ou une liberté garanti par la Charte canadienne des droits et libertés que si, sur demande présentée au titre de l'article 21.1, un juge décerne un mandat autorisant la prise de ces mesures.

[…]

Mandat — droit canadien

(3.4) Le Service ne peut, en vertu du paragraphe (1), prendre des mesures qui seraient par ailleurs contraires au droit canadien que si ces mesures ont été autorisées par un mandat décerné au titre de l'article 21.1.

Avis à l'Office de surveillance

(3.5) Dans les plus brefs délais possible après la prise de mesures en vertu du paragraphe (1), le Service avise l'Office de surveillance de ces mesures.

Précision

(4) Il est entendu que le paragraphe (1) ne confère au Service aucun pouvoir de contrôle d'application de la loi.

with other federal departments or agencies as to whether they are in a position to reduce the threat.

…

Warrant — *Canadian Charter of Rights and Freedom*

(3.2) The Service may take measures under subsection (1) that would limit a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* only if a judge, on an application made under section 21.1, issues a warrant authorizing the taking of those measures.

…

Warrant — Canadian law

(3.4) The Service may take measures under subsection (1) that would otherwise be contrary to Canadian law only if the measures have been authorized by a warrant issued under section 21.1.

Notification of Review Agency

(3.5) The Service shall, after taking measures under subsection (1), notify the Review Agency of the measures as soon as the circumstances permit.

Clarification

(4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

[11] L'article 12.2 prévoit que, lorsqu'il prend des mesures pour contrer une menace, le SCRS ne peut ni causer des lésions corporelles à un individu ou la mort de celui-ci; ni porter atteinte à

l'intégrité sexuelle d'un individu; ni causer des dommages importants à des biens si cela porterait atteinte à la sécurité d'un individu.

[12] L'article 21.1 prévoit des exigences liées aux demandes de mandats autorisant des mesures. Entre autres, la demande doit décrire les mesures envisagées et mentionner comment les mesures sont justes et adaptées aux circonstances; les solutions de rechange acceptables pour réduire la menace et les conséquences raisonnablement prévisibles sur les tierces parties.

[13] Le paragraphe 21.1(1) prévoit qu'une demande de mandat peut être présentée à la Cour « pour permettre au Service de prendre, au Canada ou à l'extérieur du Canada, les mesures prévues au paragraphe (1.1) pour réduire une menace envers la sécurité du Canada ». Le paragraphe 21.1(1.1) décrit les mesures qui peuvent être prises, notamment : « (b) modifier, enlever, remplacer, détruire, détériorer ou fournir tout ou partie d'un objet, notamment des registres, des documents, des biens, des composants et du matériel, ou en entraver la livraison ou l'utilisation ».

[14] Le paragraphe 21.1(2) prévoit le contenu d'une demande de mandat autorisant des mesures et les exigences en matière de preuve.

[15] Le paragraphe 21.1(6) prévoit que la durée maximale d'un mandat autorisant de telles mesures est généralement de cent vingt jours. (La durée maximale est de soixante jours pour les activités qui visent à saper le régime de gouvernement ou dont le but est sa destruction ou son renversement, par la violence.).

[16] Le libellé entier de l'article 21.1 de la *Loi sur le SCRS* figure à l'Annexe A.

III. La cybermenace et les mesures de réduction proposées

[17] Selon l'avocat du PGC et le déposant, le mandat autorisant des mesures de réduction de la cybermenace était nécessaire afin de protéger des infrastructures essentielles contre des adversaires étrangers qui ont infecté certains serveurs, routeurs de l'informatique individuelle et des petites entreprises et appareils de l'Internet des objets (identifiables) basés au Canada.

A. *La cybermenace*

[18] Le déposant du SCRS a confirmé la nature, la portée et la source de la cybermenace ainsi que les mesures proposées pour la contrer.

[19] Le déposant a expliqué que, en termes simples, un réseau de zombies est un vaste groupe d'appareils compromis. Tout type d'appareil connecté à l'Internet peut être compromis pour ensuite être contrôlé par un cyberacteur et utilisé à des fins malveillantes.

[20] Le déposant a remarqué que tous les types d'appareils, de routeurs de l'informatique individuelle et des petites entreprises et d'appareils de l'Internet des objets sont potentiellement vulnérables aux cyberattaques et peuvent éventuellement devenir la proie d'un réseau de zombies. Bien que les appareils plus récents et à jour soient plus sûrs, les appareils dont les utilisateurs ignorent les rappels de mise à jour des logiciels ainsi que les appareils en « fin de vie » (qui ne peuvent plus recevoir de mise à jour) demeurent particulièrement vulnérables.

[21] Le déposant a signalé que les cyberacteurs et leurs associés exploitent de plus en plus les vulnérabilités de certains appareils à risque en vue de mener des cyberopérations malveillantes. Lorsqu'il obtient l'accès à un appareil à risque, un cyberacteur peut l'infecter avec des logiciels malveillants et créer un réseau de zombies, soit un réseau constitué d'autres appareils compromis, que l'on appelle zombies. Le déposant a expliqué que les réseaux de zombies comportent habituellement deux couches : une couche [TRADUCTION] « de commande et de contrôle », qui donne des instructions aux zombies infectés, lesquels forment la couche [TRADUCTION] « clients ». Les appareils des deux couches sont infectés par des logiciels malveillants, mais les cyberacteurs passent par la couche de commande et de contrôle pour maintenir la communication avec les zombies de la couche clients et leurs donner des instructions.

[22] Le déposant a expliqué que les appareils vulnérables sont ciblés afin de créer de larges réseaux de zombies formés d'appareils cooptés appartenant à des tiers; il s'agit d'appareils vulnérables se trouvant aux quatre coins du pays. Les cyberacteurs prennent alors le contrôle des appareils vulnérables et les utilisent comme points d'entrée cachés pour infiltrer des organismes, tels que des infrastructures essentielles, des réseaux militaires et des systèmes de gouvernement. Les cyberacteurs exploitent les appareils compromis et se font passer pour des relations légitimes (p. ex. : le client d'un prestataire de service ou un télétravailleur), ce qui voile la véritable identité du cyberacteur.

[23] Le déposant a expliqué que l'exploitation de vulnérabilités logicielles permet l'établissement de réseaux cachés et, par la suite, la victimisation des entités. En effet,

l'exploitation de vulnérabilités logicielles permet la prise de contrôle sans autorisation d'une infrastructure; l'infrastructure est ensuite utilisée pour perpétrer d'autres cyberactivités hostiles, alors qu'en apparence, l'entité victimisée semble responsable des cyberattaques perpétrées contre des cibles, telles que des infrastructures essentielles, des réseaux militaires et des systèmes de gouvernement.

[24] Le déposant a ajouté que les cyberacteurs ciblent des modèles précis d'appareils, en particulier ceux en « fin de vie » et ceux qui n'ont pas été mis à jour par l'utilisateur. […]. Le déposant a expliqué que même […] peut perturber un réseau caché qui tente d'établir un point d'ancrage au Canada. En effet, le correctif force les cyberacteurs à choisir de nouvelles cibles ou à changer leurs méthodes d'exploitation.

[25] Le déposant a décrit plusieurs exemples de réseaux de zombies utilisés pour mener des cyberactivités d'espionnage, des cyberattaques et des cyberactivités d'ingérence étrangère.

[26] Dans la présente demande, la forme centralisée des deux réseaux de zombies est une source de préoccupation : il s'agit d'un serveur de commande et de contrôle au moyen duquel le cyberacteur utilise les ordinateurs pour contrôler les appareils compromis. Le cyberacteur transmet, au moyen du serveur de commande et de contrôle, une commande à tous les zombies et appareils contrôlés. Le déposant a expliqué que le SCRS se concentre sur le recours par des cyberacteurs étatiques à des réseaux de zombies au moyen desquels des cyberactivités d'espionnage, de sabotage et d'ingérence étrangère sont menées contre des infrastructures essentielles (par exemple, le secteur de l'énergie) et des gouvernements.

[27] Le déposant a décrit plusieurs cyberacteurs et les menaces que constituent leurs cyberactivités de sabotage et d'espionnage, mais a toutefois insisté sur le fait que le mandat demandé porte sur deux réseaux de zombies connus.

[28] Le déposant a décrit deux infrastructures de réseaux de zombies qui posaient des risques imminents; […].

[29] […]. Le déposant a expliqué que, sans le mandat visant des mesures de réduction de la cybermenace, […] pourraient ordonner à leurs réseaux de zombies d'éprouver, d'attaquer et éventuellement de perturber les infrastructures essentielles du Canada.

[30] […].

[31] Le déposant a fait remarquer que, si le mandat était décerné, le SCRS […].

[32] […]. Au moment de la présente demande, il était urgent d'agir à l'encontre du réseau de zombies […]. […].

[33] […].

[34] […].

[35] […]. La présente demande a identifié […] appareils, soit des routeurs de l'informatique individuelle et des petites entreprises et des appareils de l'Internet des objets situés à divers endroits au Canada (dont les adresses canadiennes de protocole Internet [IP] […].

[36] […].

[37] […].

[38] […]. Le déposant a expliqué que […] le SCRS se propose de retirer les appareils compromis du Canada dès que possible.

[39] Le déposant croit que, sans le mandat visant des mesures de réduction de la cybermenace, les cyberacteurs mèneront des activités malveillantes au Canada, par exemple, ordonner aux réseaux de zombies d'attaquer et éventuellement de désactiver les infrastructures canadiennes, de plus en plus fréquemment et sans résistance afin de faire valoir leurs intérêts financiers, politiques, idéologiques et économiques, et ce, au détriment du Canada et des Canadiens. En particulier, sans la prise de ces mesures, le Canada serait une cible facile à exploiter […].

B. *Les pouvoirs demandés*

[40] Le déposant a décrit les pouvoirs précis demandés pour permettre au SCRS de réduire la menace que constituent les réseaux de zombies en ce qui a trait à l'infrastructure et les

adresses IP identifiées (et aussi en ce qui a trait à toute adresse IP identifiée ultérieurement dans une demande supplémentaire conformément à la troisième condition du mandat visant des mesures de réduction de la cybermenace).

[41] […].

[42] […].

[43] […].

[44] […]. Le déposant a réitéré que la stratégie du SCRS cible les appareils et non leurs utilisateurs et a assuré la Cour que le SCRS ne chercherait pas à obtenir l'identité des utilisateurs et qu'il n'intercepterait aucun contenu. L'unique objectif consiste à perturber le réseau de zombies.

[45] […]. Les mesures ne permettent pas au SCRS de faire des recherches sur l'appareil ni de consulter ou de recueillir le contenu ou les données du propriétaire de l'appareil. Toutefois, dans l'éventualité où les réglages de configuration de l'infrastructure du réseau de zombies contiennent d'autres renseignements, tout renseignement personnel recueilli par inadvertance sera détruit conformément aux conditions du mandat.

IV. Les observations

[46] Le PGC fait valoir que les mesures sont essentielles pour lutter contre la cybermenace, telle qu'elle a été décrite par le déposant, et nécessitent une autorisation judiciaire conformément aux articles 12.1 et 21.1 de la Loi sur le SCRS parce qu'elles constituent probablement des infractions criminelles. Le PGC mentionne les alinéas 342.1(1)b) et c) du Code criminel, qui prévoient certaines infractions, notamment « frauduleusement et sans apparence de droit » b) « au moyen d'un appareil électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte[r] ou fai[re] intercepter toute fonction d'un ordinateur »; ou c) « directement ou indirectement, utilise[r] ou fai[re] utiliser un ordinateur dans l'intention de commettre une infraction prévue aux alinéas a) ou b) ou à l'article 430 concernant des données informatiques ou un ordinateur ». L'article 430 prévoit entre autres qu'une personne commet un méfait lorsque, volontairement, elle détruit ou détériore les données d'un ordinateur ou empêche, interrompt ou gêne l'emploi, la jouissance ou l'exploitation légitime des données d'un ordinateur.

[47] Le PGC insiste sur le fait que les divers moyens employés pour exécuter les mesures, comme l'a décrit le déposant, relèvent entièrement de l'application de l'alinéa 21.1(1.1)b) de la *Loi sur le SCRS*; en effet, les mesures nécessaires auraient pour effet de « modifier, enlever, remplacer, détruire, détériorer ou fournir tout ou partie d'un objet, notamment des registres, des documents, des biens, des composants et du matériel, ou en entraver la livraison ou l'utilisation ».

[48] Le PGC fait valoir que la preuve appuie la conclusion selon laquelle il existe des motifs raisonnables de croire qu'un mandat est nécessaire pour autoriser les mesures décrites afin de réduire la menace à la sécurité du Canada que constituent les réseaux de zombies.

[49] Le PGC fait en outre valoir que les exigences applicables du paragraphe 21.1(2) ont été remplies. Notamment, d'après le témoignage du déposant, les mesures sont raisonnables et proportionnelles. Le déposant a signalé que le contrôle d'un réseau de zombies par des adversaires étrangers peut entraîner des répercussions catastrophiques sur des infrastructures essentielles, comparativement aux mesures proposées, qui, elles, […] appartenant aux réseaux de zombies malveillants ou d'appareils vulnérables. Le PGC a également signalé, tout comme le déposant l'a expliqué, qu'il n'y a pas d'autre moyen de réduire la menace. Le PGC a ajouté qu'aucun autre ministère ou organisme gouvernemental ne détient un mandat pour répondre aux cybermenaces. Le PGC a insisté sur le fait que le mandat allait servir contre les appareils identifiés, et non leurs utilisateurs; le SCRS ne s'intéresse aucunement à l'identité des utilisateurs. Le PGC fait valoir que les mesures décrites et envisagées ne violent aucun droit protégé par la *Charte*.

[50] Le PGC a signalé que le mandat proposé visant des mesures de réduction de la cybermenace cible les adresses IP […].

[51] Le PGC a reconnu que dans l'arrêt *R c Bykovets,* 2024 CSC 6 [*Bykovets*], la Cour suprême du Canada a conclu qu'il existe une attente raisonnable au respect de la vie privée à l'égard d'une adresse IP et qu'une demande faite par la police visant l'obtention d'une adresse IP

nécessite une autorisation judiciaire préalable. Le PGC avance que les adresses IP en cause dans la présente demande ont été recueillies légalement sans mandat conformément à l'article 12 de la *Loi sur le SCRS* et peuvent faire l'objet du mandat visant des mesures de réduction de la cybermenace.

[52] […]. Le PGC avance que […] ne fait pas intervenir l'article 8 de la *Charte*.

[53] Se fondant sur l'article 12 de la *Loi sur le SCRS*, le SCRS a recueilli les adresses IP […] visent […] la sécurité nationale.

[54] Le PGC a fait en outre valoir que la troisième condition du mandat visant des mesures de réduction de la cybermenace permet au SCRS de présenter une demande supplémentaire dans l'éventualité où de nouveaux réseaux de zombies seraient identifiés. Le PGC fait valoir que, si la Cour conclut, dans la présente demande de mandat visant des mesures de réduction de la cybermenace, à l'existence d'un lien entre le cyberacteur et l'infrastructure du réseau de zombies malveillante, ce même lien continuerait d'exister en cas de demandes supplémentaires.

[55] Bien que l'*amicus* ait été essentiellement d'accord avec le PGC, il a tout de même passé en revue le témoignage du déposant du PGC et a proposé plusieurs précisions à apporter aux définitions et au pouvoir prévu par le mandat, dont il est question ci-dessous.

V. Le mandat visant des mesures de réduction de la cybermenace est nécessaire et ces mesures sont une réponse raisonnable et proportionnelle à la menace

[56] La Cour a tenu compte de l'affidavit détaillé et du témoignage du déposant ainsi que des observations de l'avocat du PGC et de l'*amicus*.

[57] Comme l'a mentionné le PGC, la prise des mesures ne serait pas possible sans les adresses IP […]. Le PGC a reconnu qu'il est question des répercussions de l'arrêt *Bykovets* sur la collecte d'adresses IP par le SCRS dans d'autres affaires qui seront entendues par la Cour. Le PGC a fait valoir des arguments semblables à l'appui de sa position selon laquelle […] la collecte d'adresses IP ne font pas intervenir d'attente raisonnable au respect de la vie privée. Le PGC a également insisté sur le fait que les adresses IP ne visent que des choses et non des personnes.

[58] La Cour signale qu'elle a publié ultérieurement des motifs (classifiés) dans la décision intitulée *Dans l'affaire concernant la demande de mandats présentée par* […] *au titre des articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité, LRC 1985, c C-23* (2025 CF 1978), qui portaient sur la troisième condition du cybermandat, dans le cadre d'une demande supplémentaire pour exécuter des pouvoirs à l'égard d'une infrastructure nouvellement identifiée. On a demandé à la Cour de prendre en compte les répercussions de l'arrêt *Bykovets* sur la capacité du SCRS de recueillir des adresses IP précises.

[59] La Cour a conclu, entre autres, que les adresses IP en cause dans cette demande supplémentaire avaient été recueillies légalement conformément à l'article 12 dans le cadre d'une collecte non intrusive; les adresses IP ne suscitent donc pas d'attente raisonnable au respect de la vie privée et leur collecte ne fait pas fait intervenir l'article 8.

[60] […].

[61] Ayant été convaincue que toutes les exigences de l'article 21.1 (notées ci-dessus aux paragraphes 12 à 15 et figurant à l'annexe A) ont été remplies, la Cour a, en conséquence, décerné le mandat visant des mesures de réduction de la cybermenace. Les faits confirmés par le déposant démontrent que les actions des deux adversaires étrangers constituent effectivement une menace à la sécurité du Canada. Selon les faits confirmés par le déposant, il y a des motifs raisonnables de croire à la nécessité du mandat pour réduire la menace, et les mesures précises qui y sont décrites étaient nécessaires, raisonnables et proportionnelles dans les circonstances. Ces mesures ont été prises à l'encontre d'appareils, et non de personnes. Comme mentionné ci-dessus, le SCRS n'a pas à identifier les propriétaires des appareils et n'a pas l'intention de le faire. Aucun renseignement personnel ou autre contenu n'a été recueilli. […]. Le déposant a prodigué des conseils utiles aux utilisateurs pour éviter que leur appareil ne devienne à leur insu un moyen de perpétrer une cybermenace, en l'occurrence, installer les mises à jour lorsque l'appareil le propose. Les appareils en « fin de vie » et non à jour sont vulnérables et peuvent être facilement exploités par les cyberacteurs malveillants, qui sont alors en mesure de causer un préjudice grave à l'infrastructure et aux systèmes du gouvernement au Canada et à l'étranger.

[62] Le mandat visant des mesures de réduction de la cybermenace a été peaufiné en réponse aux questions soulevées par l'*amicus*, qui souhaitait clarifier certains aspects. […].

[63] Le PGC était également d'accord avec la proposition de l'*amicus* selon laquelle le pouvoir du SCRS de […] devrait être conforme à l'exigence de [TRADUCTION] « utiliser les moyens les moins intrusifs dans les circonstances ». Cette précision est cohérente avec le témoignage du déposant, qui décrit comment le SCRS allait exécuter les mesures en commençant par les mesures les moins intrusives.

[64] Comme je l'ai mentionné précédemment, la Cour a décerné le mandat visant des mesures de réduction de la cybermenace pour une durée de 120 jours et l'a ensuite renouvelé pour une période additionnelle de 120 jours.

[65] Le PGC et l'*amicus* s'entendent pour dire que les menaces que constituent les réseaux de zombies et les efforts déployés par le SCRS pour réduire ces menaces doivent être connus du public. Le déposant a mentionné que les États-Unis ont publié un communiqué de presse annonçant leur interruption réussie de cybermenaces et que les autres pays du Groupe des cinq se sont montrés plus ouverts quant à l'interruption de telles cybermenaces, notamment des réseaux de zombies. La Cour s'exprime à travers ses jugements. Le PGC et l'*amicus* estiment que la version publique des motifs de la Cour favoriserait la transparence quant à la nature et la portée de la cybermenace et les efforts déployés par le SCRS pour la contrer.

[66] La Cour s’efforcera de fournir la version caviardée des motifs dès que possible une fois que la Cour pris connaissance des observations du PGC et de l’*amicus* en ce qui a trait aux passages des motifs qui doivent être caviardés.

"Catherine M. Kane"
Juge

Annexe « A »

L'article 21.1 de la *Loi sur le SCRS*

Demande de mandat — mesures pour réduire les menaces envers la sécurité du Canada

21.1 (1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de prendre, au Canada ou à l'extérieur du Canada, les mesures prévues au paragraphe (1.1) pour réduire une menace envers la sécurité du Canada.

Mesures

(1.1) Pour l'application du paragraphe (1), les mesures sont les suivantes :

a) modifier, enlever, remplacer, détruire, interrompre ou détériorer des communications ou des moyens de communication;

b) modifier, enlever, remplacer, détruire, détériorer ou fournir tout ou partie d'un objet, notamment des registres, des documents, des biens, des composants et du matériel, ou en entraver la livraison ou l'utilisation;

c) fabriquer ou diffuser de l'information, des registres ou des documents;

d) effectuer ou tenter d'effectuer, directement ou indirectement, des opérations financières qui font intervenir ou qui paraissent faire intervenir des espèces ou des effets;

Application for warrant — measures to reduce threats to security of Canada

21.1 (1) If the Director or any employee who is designated by the Minister for the purpose believes on reasonable grounds that a warrant under this section is required to enable the Service to take measures referred to in subsection (1.1), within or outside Canada, to reduce a threat to the security of Canada, the Director or employee may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

Measures

(1.1) For the purpose of subsection (1), the measures are the following:

(a) altering, removing, replacing, destroying, disrupting or degrading a communication or means of communication;

(b) altering, removing, replacing, destroying, degrading or providing — or interfering with the use or delivery of — any thing or part of a thing, including records, documents, goods, components and equipment;

(c) fabricating or disseminating any information, record or document;

(d) making or attempting to make, directly or indirectly, any financial transaction that involves or purports to involve currency or a monetary instrument;

e) interrompre ou détourner, directement ou indirectement, des opérations financières qui font intervenir des espèces ou des effets;

f) entraver les déplacements de toute personne, à l'exception de la détention d'un individu;

g) se faire passer pour une autre personne, à l'exception d'un policier, dans le but de prendre l'une des mesures prévues aux alinéas a) à f).

Contenu de la demande

(2) La demande est présentée par écrit et accompagnée de l'affidavit du demandeur portant sur les points suivants :

a) les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada;

b) les mesures envisagées;

c) le fait que les mesures envisagées sont justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, des solutions de rechange acceptables pour réduire la menace et des conséquences raisonnablement prévisibles sur les tierces parties, notamment sur leur droit à la vie privée;

d) l'identité des personnes qui sont touchées directement par les mesures envisagées, si elle est connue;

e) les personnes ou catégories de personnes destinataires du mandat demandé;

(e) interrupting or redirecting, directly or indirectly, any financial transaction that involves currency or a monetary instrument;

(f) interfering with the movement of any person, excluding the detention of an individual; and

(g) personating a person, other than a police officer, in order to take a measure referred to in any of paragraphs (a) to (f).

Matters to be specified in application

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by the applicant's affidavit deposing to the following matters:

(a) the facts relied on to justify the belief on reasonable grounds that a warrant under this section is required to enable the Service to take measures to reduce a threat to the security of Canada;

(b) the measures proposed to be taken;

(c) the reasonableness and proportionality, in the circumstances, of the proposed measures, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat and the reasonably foreseeable effects on third parties, including on their right to privacy;

(d) the identity of the persons, if known, who are directly affected by the proposed measures;

(e) the persons or classes of persons to whom the warrant is proposed to be directed;

f) si possible, une description générale du lieu où le mandat demandé est à exécuter;

(f) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

g) la durée de validité applicable en vertu du paragraphe (6), de soixante jours ou de cent vingt jours au maximum, selon le cas, demandée pour le mandat;

(g) the period, not exceeding 60 days or 120 days, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (6); and

h) la mention des demandes antérieures présentées au titre du paragraphe (1) touchant des personnes visées à l'alinéa d), la date de chacune de ces demandes, le nom du juge à qui elles ont été présentées et la décision de celui-ci dans chaque cas.

(h) any previous application made under subsection (1) in relation to a person who is identified in the affidavit in accordance with paragraph (d), the date on which each such application was made, the name of the judge to whom it was made and the judge's decision on it.

Délivrance du mandat

(3) Par dérogation à toute autre règle de droit mais sous réserve de la *Loi sur la statistique*, le juge à qui est présentée la demande visée au paragraphe (1) le mandat s'il est convaincu de l'existence des faits qui sont mentionnés aux alinéas (2)a) et c) et énoncés dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à prendre les mesures qui y sont indiquées. À cette fin, il peut autoriser aussi, de leur part :

Issuance of warrant

(3) Despite any other law but subject to the *Statistics Act*, if the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (c) that are set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to take the measures specified in it and, for that purpose,

a) l'accès à un lieu ou un objet ou l'ouverture d'un objet;

(a) to enter any place or open or obtain access to any thing;

b) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé;

(b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing;

c) l'installation, l'entretien et l'enlèvement d'objets;

(c) to install, maintain or remove any thing; or

d) les autres actes nécessaires dans les circonstances à la prise des mesures.

(d) to do any other thing that is reasonably necessary to take those measures.

Mesures à l'extérieur du Canada

(4) Sans égard à toute autre règle de droit, notamment le droit de tout État étranger, le juge peut autoriser la prise à l'extérieur du Canada des mesures indiquées dans le mandat décerné en vertu du paragraphe (3).

Measures taken outside Canada

(4) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize the measures specified in it to be taken outside Canada.

Contenu du mandat

(5) Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes :

Matters to be specified in warrant

(5) There shall be specified in a warrant issued under subsection (3)

a) les mesures autorisées;

(a) the measures authorized to be taken;

b) l'identité des personnes qui sont touchées directement par les mesures, si elle est connue;

(b) the identity of the persons, if known, who are directly affected by the measures;

c) les personnes ou catégories de personnes destinataires du mandat;

(c) the persons or classes of persons to whom the warrant is directed;

d) si possible, une description générale du lieu où le mandat peut être exécuté;

(d) a general description of the place where the warrant may be executed, if a general description of that place can be given;

e) la durée de validité du mandat;

(e) the period for which the warrant is in force; and

f) les conditions que le juge estime indiquées dans l'intérêt public.

(f) any terms and conditions that the judge considers advisable in the public interest.

Durée maximale

(6) Il ne peut être décerné de mandat en vertu du paragraphe (3) que pour une période maximale :

Maximum duration of warrant

(6) A warrant shall not be issued under subsection (3) for a period exceeding

a) de soixante jours, lorsque le mandat est décerné pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada au

(a) 60 days if the warrant is issued to enable the Service to take measures to reduce a threat to the security of Canada within the meaning of paragraph (d) of the definition

sens de l’alinéa d) de la définition de telles menaces à l’article 2;	***threats to the security of Canada*** in section 2; or
b) de cent vingt jours, dans tout autre cas.	**(b)** 120 days in any other case.

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIERS :	C-6-24
INTITULÉ :	DANS L'AFFAIRE concernant la demande de mandats présentée par […] au titre des articles 12.1 et 21.1 de la *Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, ch C-23 ET DANS L'AFFAIRE VISANT DES CYBERACTIVITÉS D'ESPIONNAGE, DE SABOTAGE ET D'INGÉRENCE ÉTRANGÈRE ET DES RÉSEAUX DE ZOMBIES
LIEU DE L'AUDIENCE :	OTTAWA (ONTARIO)
DATE DE L'AUDIENCE :	1er MAI 2024
MOTIFS CLASSIFIÉS :	LA JUGE KANE
DATE :	26 FÉVRIER 2026

COMPARUTIONS :

Andrew Cameron	POUR LE PROCUREUR GÉNÉRAL DU CANADA
Solomon Friedman	*AMICUS CURIAE*

AVOCATS INSCRITS AU DOSSIER :

Le Procureur général du Canada	POUR LE DEMANDEUR
Friedman Mansour LLP Ottawa (ON)	*AMICUS CURIAE*