Federal Court Cour fédérale

~~**TOP SECRET**~~

Date: 20260226

Docket: C-6-24

Citation: 2026 FC 269

Ottawa, Ontario, February 26, 2026

PRESENT: The Honourable Madam Justice Kane

BETWEEN:

**IN THE MATTER OF an application by [redacted]
for warrants pursuant to sections 12.1 and 21.1 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23**

AND IN THE MATTER OF CYBER ESPIONAGE, CYBER SABOTAGE, CYBER FOREIGN-INFLUENCED ACTIVITIES and MALICIOUS BOTNETS

REASONS

[1] Although the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*] has provided for the issuance of warrants for threat reduction measures [TRM] for several years, this is the first application of its kind. The application was filed on April 24, 2024, pursuant to sections 12.1 and 21.1 of the *CSIS Act* seeking warranted powers to reduce the threat to critical infrastructure posed by foreign adversaries as a result of the infection of certain devices with malicious software, known as malware [the Cyber Threat Reduction Measures Warrant or the TRM warrant]. Given that this is the first application for a TRM warrant of any kind, the Court appointed Mr. Solomon Friedman, a security cleared lawyer, as *amicus curiae* [*amicus*] to assist

the Court, including to probe the evidence of the affiant and the submissions of Counsel for the Attorney General of Canada [AGC].

[2] The Court granted the application and issued the Cyber Threat Reduction Measures Warrant on May 1, 2024, upon finding that the requirements of section 21.1 were met, including that the threat to the security of Canada was clearly established and imminent and that the warranted powers were necessary to reduce the threat. The warrant was first granted for a period of 120 days. On August 29, 2024, the Court renewed the Cyber Threat Reduction Measures Warrant for a further 120 days. The Court undertook to provide brief Reasons for granting the initial application.

[3] These are the Reasons, albeit delayed.

I. Overview

[4] In this application, the Canadian Security Intelligence Service [CSIS or the Service] sought warranted powers to protect critical infrastructure from foreign adversaries that have infected Canada-based servers, small office or home office [SOHO] routers and Internet of Things [IoT] devices (which would include everyday objects that can connect to the Internet, such as “Ring Doorbells”, security cameras, televisions, or other Wi-Fi enabled appliances) with malware. The malware causes these servers, routers, and devices to operate as a network of infected devices, referred to as a “botnet”.

[5] CSIS's strategy is to neutralize the botnets […]. As explained to the Court, the devices are identifiable, but there is no intention or need to identify the owner or user of the device. The strategy is targeted at the devices; neither the users' identity or any content on the devices will be collected.

[6] CSIS seeks the warrant because the necessary TRM to neutralize the botnets […]. These measures likely constitute offences pursuant to the Criminal Code, RSC 1985, c C-46 [*Criminal Code*] and therefore require judicial authorization in accordance with subsection 12.1(3.4) of the *CSIS Act*.

II. The Statutory Provisions

[7] The *CSIS Act* permits CSIS to take measures to reduce threats by non-warranted means; however, depending on the circumstances, warranted powers may be necessary—as in the present case.

[8] "Threats to the security of Canada" is defined in section 2 of the *CSIS Act* and include:

(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,	**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;
(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…	**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; …

[9] Section 12.1 authorizes CSIS to take measures to reduce threats to the security of Canada, where the criteria to do so are established.

[10] Section 12.1 provides:

Measures to reduce threats to the security of Canada	**Mesures pour réduire les menaces envers la sécurité du Canada**
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.	**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.
Limits	**Limites**
(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.	**(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.
Alternatives	**Autres options**
(3) Before taking measures under subsection (1), the Service shall consult, as appropriate, with other federal departments or agencies as to whether they are in a position to reduce the threat.	**(3)** Avant de prendre des mesures en vertu du paragraphe (1), le Service consulte, au besoin, d'autres ministères ou organismes fédéraux afin d'établir s'ils sont en mesure de réduire la menace.
…	[…]
Warrant — *Canadian Charter of Rights and Freedom*	**Mandat — *Charte canadienne des droits et libertés***
(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,	**(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

issues a warrant authorizing the taking of those measures.	l'article 21.1, un juge décerne un mandat autorisant la prise de ces mesures.
…	[…]
Warrant — Canadian law	**Mandat — droit canadien**
(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.	**(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.
Notification of Review Agency	**Avis à l'Office de surveillance**
(3.5) The Service shall, after taking measures under subsection (1), notify the Review Agency of the measures as soon as the circumstances permit.	**(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.
Clarification	**Précision**
(4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.	**(4)** Il est entendu que le paragraphe (1) ne confère au Service aucun pouvoir de contrôle d'application de la loi.

[11] Section 12.2 provides that, in taking measures to reduce a threat, CSIS is prohibited from engaging in certain conduct, including: causing bodily harm or death to anyone; violating the sexual integrity of anyone; and causing serious damage to property if doing so would endanger the safety of anyone.

[12] Section 21.1 sets out the requirements for applications for TRM warrants. Among other things, the application must describe the measures contemplated and address the reasonableness and proportionality of the measures, the reasonable availability of other means, and the foreseeable effects on third parties.

[13] Subsection 21.1(1) provides that an application may be made to this Court for a warrant 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". Subsection 21.1(1.1) describes the measures that may be taken, which include, "(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".

[14] Subsection 21.1(2) sets out the contents of an application for a TRM warrant and the evidentiary requirements.

[15] Subsection 21.1(6) provides that the maximum duration of the TRM warrant is generally 120 days. (The maximum duration is 60 days where the threat relates to the destruction or overthrow by violence of the system of government).

[16] The full text of section 21.1 of the *CSIS Act* is set out in Annex A.

III. The Threat and the Threat Reduction Measures Proposed

[17] Counsel for the AGC and the affiant described the Cyber Threat Reduction Measures Warrant as necessary to protect critical infrastructure from foreign adversaries that have infected certain (identifiable) Canada-based servers, SOHO routers, and IoT devices.

A. *The Threat*

[18] The CSIS affiant attested to the nature, scope, and source of the threat and the proposed measures to reduce the threat.

[19] The affiant explained, in simple terms, that a botnet is a large group of compromised devices. Any kind of Internet accessible device can be compromised, taken over by a cyber actor, and used for malicious purposes.

[20] The affiant noted that all types of devices, SOHO routers, and IoT devices can become vulnerable to cyber attack and can become part of a botnet. Although newer and updated devices are less vulnerable, users who ignore reminders to update the software on their devices and "end of life" devices (no longer able to be updated) are particularly vulnerable.

[21] The affiant noted that security vulnerabilities in susceptible devices are increasingly being leveraged by cyber actors and their affiliates for malicious cyber operations. Once the cyber actor gains access to these devices, they can infect network devices with malware and use the malware to create a botnet—a network of other compromised network devices—individually referred to as "bots". He explained that botnets usually have two layers: a "command and control" layer that provides instructions to infected bots, which are the "client" layer. The devices in both layers are infected with malware, but cyber actors use the command and control layer to maintain communication with, and provide instructions to, the bots in the client layer.

[22] The affiant explained that vulnerable devices are being targeted in order to develop large botnets of co-opted third-party devices, which are primarily vulnerable devices located throughout Canada. The cyber actors seize control of vulnerable devices and use them as covert entry points to access organizations, such as critical infrastructure, military networks, and government systems. The cyber actors exploit the compromised devices in order to appear to be a legitimate connection (such as a client of a service provider, or an employee working from home), which disguises the cyber actor's identity.

[23] The affiant explained that the use of software vulnerabilities to create covert networks victimizes entities by taking unauthorized control of their infrastructure, using that infrastructure for additional hostile cyber activity, and making it appear as if the victimized entity is responsible for cyber attacks against targets such as critical infrastructure, military networks, and government systems.

[24] The affiant explained that the cyber threat actor targets specific models of devices, in particular those that are at the "end of life" and also those that have not been updated by the user. […]. The affiant explained that even […] can disrupt a covert network seeking to gain a foothold in Canada as the cyber actors would be forced to choose new targets or change their exploitation procedures.

[25] The affiant described several examples of botnets used to conduct cyber espionage, cyber attacks and cyber foreign-influenced activities.

[26] In this application, the centralized forms of both botnets are the concern: command and control servers where the computers that are being used by the cyber actors to command and control any compromised devices. The cyber actors submit commands via the command and control servers to all bots and devices that are being controlled. The affiant explained that CSIS is focusing on state-based cyber actors' use of botnets to conduct cyber espionage, sabotage, and foreign-influenced activity against critical infrastructure (for example, the energy sector) and governments.

[27] The affiant described several cyber actors and the threats posed by their cyber sabotage and espionage but emphasized that the TRM warrant sought is with respect to two known botnets.

[28] The affiant described two botnet infrastructures posing imminent risks; […].

[29] […]. The affiant explained that without the Cyber Threat Reduction Measures Warrant, […] could direct their botnets to probe, attack, and potentially disrupt critical infrastructure in Canada.

[30] […].

[31] The affiant noted that if the warrant were issued, CSIS […].

[32] […]. At the time of the application, time was of the essence with respect to the […] botnet. […].

[33] […].

[34] […].

[35] […]. This application identified […] devices—SOHO routers and IoT devices located at various places in Canada (with Canadian Internet Protocol [IP] addresses […].

[36] […].

[37] […].

[38] […]. The affiant explained that, […] CSIS proposed to remove the compromised devices from Canada as soon as possible.

[39] The affiant expressed his belief that without the Cyber Threat Reduction Measures Warrant, threat actors will conduct malicious activities in Canada, including to direct the botnets to attack and potentially disable Canadian infrastructure, with increasing frequency and without resistance in order to advance their financial, political, ideological, and economic interests—to the detriment of Canada and Canadians. In particular, without the TRM, […] would regard Canada as an easy target to exploit.

B. *The Powers Sought*

[40] The affiant described the specific powers sought to enable CSIS to reduce the threat posed by the botnets with respect to the infrastructure and IP addresses identified (and also with respect to any IP addresses subsequently identified in a supplemental application pursuant to Condition 3 to the Cyber Threat Reduction Measures Warrant).

[41] […].

[42] […].

[43] […].

[44] […]. The affiant reiterated that CSIS strategy targets devices, not users of devices, and assured the Court that the identity of the user will not be known or sought and that CSIS will not conduct any intercept of content. The goal is only to disrupt the botnet.

[45] […]. The TRM does not allow CSIS to search, view, or collect the device owner's content or data. However, if the configuration settings in the botnet infrastructure contained other information, any incidentally collected personal information would be destroyed in accordance with the Conditions of the warrant.

IV. The Submissions

[46] The AGC submits that the TRM necessary to combat the threat as described by the affiant requires judicial authorization pursuant to sections 12.1 and 21.1 of the *CSIS Act* because these measures likely constitute a criminal offence or offences. The AGC pointed to paragraphs 342.1(1)(b) and (c) of the *Criminal Code*, which provide that everyone commits an offence who "fraudulently and without colour of right": (b) "by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system," or (c) "uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system". Section 430 provides that everyone commits mischief who, *inter alia*, destroys or alters computer data, obstructs, interrupts, or interferes with the lawful use of computer data.

[47] The AGC emphasized that the various means by which the TRM would be executed, as described by the affiant, would fall squarely within paragraph 21.1(1.1)(b) of the *CSIS Act*; the measures required would constitute "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".

[48] The AGC submits that the evidence supports finding that there are reasonable grounds to believe that the warrant is required to take the measures described to reduce the threat to the security of Canada posed by the botnets.

[49] The AGC further submits that all the applicable requirements of subsection 21.1(2) have been satisfied. In particular, the affiant's evidence established that the measures are reasonable and proportional. The affiant noted the impact of a botnet controlled by foreign adversaries with the potential to cause catastrophic disruptions to critical infrastructure, compared to the proposed measures […] on devices that are part of or vulnerable to malicious botnets. The AGC noted that, as the affiant explained, there is no other means to reduce the threat. The AGC added that no other government department or agency has a mandate to address the cyber threat. The AGC emphasized that the warrant was directed against the identified devices, not their users; CSIS has no interest in the identity of the user. The AGC submits that the TRM described and contemplated did not limit any *Charter* right.

[50] The AGC noted that the proposed Cyber Threat Reduction Measures Warrant relied on the IP addresses […].

[51] The AGC acknowledged that in *R v Bykovets*, 2024 SCC 6 [*Bykovets*], the Supreme Court of Canada held that there is a reasonable expectation of privacy in an IP address and that a request by the police for an IP address requires prior judicial authorization. The AGC submits that the IP addresses at issue in this application were lawfully collected without a warrant pursuant to section 12 of the *CSIS Act* and are admissible in support of the Cyber Threat Reduction Measures Warrant.

[52] […]. The AGC submits that section 8 of the *Charter* is not engaged […].

[53] The AGC relied on section 12 of the *CSIS Act* as sufficient authority for CSIS to collect the IP addresses […] for the common national security purpose.

[54] The AGC further noted that Condition 3 of the Cyber Threat Reduction Measures Warrant would permit CSIS to bring a supplemental application where new botnet infrastructure is identified. The AGC submits that if the Court finds a *nexus* between the cyber actor and the malicious botnet infrastructure in this application for the Cyber Threat Reduction Measures Warrant, that same *nexus* would exist in subsequent supplemental applications.

[55] The *amicus* was in general agreement with the AGC, but also probed the evidence of the AGC's affiant and proposed several clarifications to the definitions and authority set out in the warrant, as noted below.

V. The Cyber Threat Reduction Measures Warrant is Necessary and is a Reasonable and Proportional Response to the Threat

[56] The Court considered the detailed affidavit evidence and oral evidence of the affiant and the submissions of Counsel for the AGC and the *amicus*.

[57] As the AGC noted, the TRM would not be possible without the IP addresses […]. The AGC acknowledged that the implications of *Bykovets* on CSIS's collection of IP addresses would be addressed by this Court in other proceedings. The AGC advanced similar arguments in support of their position that the […] collection of the IP addresses do not engage any

reasonable expectation of privacy. The AGC also emphasized that in this application, the IP addresses lead only to things and not to individuals.

[58] The Court notes that it subsequently released (classified) Reasons in *In the Matter of an Application by* […] *for Warrants Pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c. C-23 AND in the Matter of Cyber Espionage, Cyber Sabotage and Cyber Foreign-Influenced Activities* (2025 FC 1978), which was a Condition 3, Supplemental Application to the Cyber Warrant to execute powers with respect to newly identified infrastructure. The Court was called upon to consider the impact of *Bykovets* on CSIS's ability to collect specified IP addresses.

[59] Among other things, the Court found that the specified IP addresses at issue in that Supplemental Application were lawfully collected pursuant to section 12 as non-intrusive collection; the IP addresses did not attract a reasonable expectation of privacy and did not engage section 8.

[60] […].

[61] The Court was satisfied that all the requirements of section 21.1 (noted above at paragraphs 12-15 and as set out in Annex A) were established and, therefore, issued the Cyber Threat Reduction Measures Warrant. The facts attested to by the affiant demonstrated that the actions of the two foreign adversaries constituted a threat to the security of Canada. The facts attested to by the affiant justified the reasonable grounds to believe that the warrant was required

to reduce this threat and that the specific measures as described were necessary, reasonable, and proportional in the circumstances. These measures were directed against devices, not persons. As noted above, there is no need or intention on the part of CSIS to identify the owners of the devices. No personal information or other content is collected. […]. The affiant provided helpful advice to device users to guard against becoming the unwitting medium for a cyber threat, which is to install the updates on personal devices when prompted to do so. The "end of life" and non-updated devices are vulnerable and are exploited by malicious cyber actors, with the potential to cause serious harm to infrastructure and government systems in Canada and beyond.

[62] The Cyber Threat Reduction Measures Warrant was refined in response to issues raised by the *amicus* to clarify certain aspects. […].

[63] The AGC also agreed with the *amicus*' proposal that CSIS's authority […] should be constrained by the requirement to "use the least intrusive means in the circumstances". This clarification is consistent with the evidence of the affiant, who described how CSIS would go about the TRM beginning with the least intrusive measures.

[64] As noted above, the Court issued the Cyber Threat Reduction Measures Warrant for a duration of 120 days and subsequently renewed the warrant for an additional 120 days.

[65] The AGC and *amicus* shared the view that the threats posed by the botnets and CSIS's efforts to reduce these threats should be made known to the public. The affiant had noted that the

United States issued a press release regarding their successful efforts to disrupt cyber threats and that other Five Eyes countries had been more open about disrupting similar cyber threats, including botnets. The Court speaks through its decisions. The AGC and *amicus* agree that the public version of the Court's Reasons could provide some transparency regarding the nature and scope of the threat and CSIS's efforts to combat the threat.

[66] The Court will endeavour to provide the public version of the Reasons as soon as feasible following the Court's consideration of the submissions of the AGC and *amicus* with respect to any necessary redactions to the Reasons.

"Catherine M. Kane"
Judge

Annex "A"

Section 21. 1 of the CSIS Act

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;

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;

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

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

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

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

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

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).

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:

Contenu de la demande

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

(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;

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) the measures proposed to be taken;

b) les mesures envisagées;

(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;

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

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

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

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

(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;

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

(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

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;

(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.

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.

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,

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 :

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

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

(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;

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;

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

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

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

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

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.

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).

Matters to be specified in warrant

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

Contenu du mandat

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

(a) the measures authorized to be taken;

a) les mesures autorisées;

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

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

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

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

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

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

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

e) la durée de validité du mandat;

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

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

Maximum duration of warrant

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

Durée maximale

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

(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

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

threats to the security of Canada in section 2; or

(b) 120 days in any other case.

sens de l’alinéa d) de la définition de telles menaces à l’article 2;

b) de cent vingt jours, dans tout autre cas.

FEDERAL COURT

SOLICITORS OF RECORD

DOCKETS:	C-6-24
STYLE OF CAUSE:	IN THE MATTER OF an application by [redacted] for warrants pursuant to sections 12.1 and 21.1 of the *Canadian Security Intelligence Service Act*, RSC 1985, c. C-23 AND IN THE MATTER OF CYBER ESPIONAGE, CYBER SABOTAGE, and CYBER FOREIGN-INFLUENCED ACTIVITIES and MALICIOUS BOTNETS
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	MAY 1, 2024
CLASSIFIED REASONS:	KANE J.
DATED:	FEBRUARY 26, 2026

APPEARANCES:

Andrew Cameron	FOR THE ATTORNEY GENERAL OF CANADA
Solomon Friedman	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Attorney General of Canada	FOR THE APPLICANT
Friedman Mansour LLP Ottawa (ON)	*AMICUS CURIAE*