

## **McGill Academic**

**Issue:** A June 7, 2019 *La Presse* article claims that a McGill academic identified by the FBI as being associated with the Chinese intelligence services and involved in the transfer of sensitive research and technology to China received over half a million dollars of Government of Canada research funding between 2009 and 2014.

### **Proposed Response:**

- **One of Canada's strengths is our advanced research and technological capabilities, combined with expertise in a number of industrial sectors.**
- **This makes our country an attractive target for foreign actors and intelligence services seeking to gather intellectual property and proprietary information to further their own economic, political or military interests.**
- **Our national security agencies monitor all potential threats and have robust measures in place to address them, in collaboration with Canadian and international partners.**
- **I would like to emphasize that the Canadian Security Intelligence Service has a mandate to investigate threats to the security of Canada, which may include espionage. Any individual engaged in this kind of threat-related activity may be subject to lawful investigation.**
- **Beyond this, I cannot comment on the contents of the article or speak to specific threats or operational activity in a public forum.**
- **However, I would reassure the Members of this House that our national security agencies are constantly working to identify threats to national security and take the necessary steps to keep Canadians safe.**

## McGill Academic

### Background:


A June 7, 2019 La Presse article claims that a McGill academic identified by the FBI as being associated with the Chinese intelligence services and involved in the transfer of sensitive research and technology to China received over half a million dollars of Government of Canada research funding between 2009 and 2014. This funding was allocated individually or as part of group projects from the Natural Sciences and Engineering Research Council and the National Research Council.

La Presse originally reported the FBI accusations against Professor Ishiang Shih in January 2018. Shih has denied these accusations as based on a misunderstanding. La Presse claims that Shih and his brother are accused by American authorities of having conspired since 2006 to steal American and Canadian intellectual property and technology to help develop a civil-military semiconductor enterprise in China, with support from Chinese authorities.

American authorities formally requested Ishiang Shih's extradition from Canada on October 10, 2018. The article claims the request is still under study by Canada's Department of Justice. Shih retired from McGill shortly after La Presse broke the original story. Shih's brother was arrested by the FBI in January 2018 and faces charges of illegally obtaining and transferring technologies to a Chinese company without the required export license.

### Contacts:

Prepared by: N/A

Approved by: Tricia Geddes, Assistant Director Policy and Strategic Partnerships, 

## **Chercheur de l'Université McGill**

**Objet :** D'après un article de La Presse publié le 7 juin 2019, un professeur agrégé de l'université McGill accusé par le FBI d'être lié aux services de renseignement chinois et impliqué dans le transfert de matériel de recherche et de technologies sensibles vers la Chine aurait reçu plus d'un demi-milliard de dollars entre 2009 et 2014 de la part du gouvernement canadien pour subventionner ses recherches.

### **Réponses suggérées :**

- **La recherche de pointe et les moyens technologiques, combinés à une expertise dans de nombreux secteurs industriels, constituent l'une des forces du Canada.**
- **Ces ressources représentent une cible attrayante pour certaines parties étrangères, notamment des services de renseignement, qui cherchent à acquérir des informations exclusives et des propriétés intellectuelles pour appuyer l'atteinte des visées économiques, politiques et militaires de leur pays.**
- **Les organismes qui assurent la sécurité nationale du Canada surveillent toutes les menaces. Pour y faire face, ils disposent de moyens robustes et collaborent avec des partenaires canadiens et étrangers.**
- **J'aimerais rappeler que le Service canadien du renseignement de sécurité a pour mandat de faire enquête sur les menaces pour la sécurité du Canada, ce qui peut comprendre l'espionnage. Ainsi, aux termes de la *Loi*, toute personne qui participe à une activité liée à une menace peut faire l'objet d'une enquête.**
- **Cela dit, je tiens à souligner que je ne peux pas me prononcer sur le contenu de l'article ni discuter de menaces particulières ou d'activités opérationnelles dans un cadre public.**

- **Toutefois, je tiens à rassurer mes collègues; nos organismes de sécurité surveillent sans relâche les menaces pour la sécurité nationale et prennent les mesures qui s'imposent pour protéger les Canadiens.**

## Chercheur de l'Université McGill

### Contexte :

D'après un article de La Presse publié le 7 juin 2019, un professeur agrégé de l'université McGill accusé par le FBI d'être lié aux services de renseignement chinois et impliqué dans le transfert de matériel de recherche et de technologies sensibles vers la Chine aurait reçu plus d'un demi-milliard de dollars entre 2009 et 2014 de la part du gouvernement canadien pour subventionner ses recherches. Les fonds ont été alloués parfois de manière individuelle, parfois, pour des ensembles de projets relevant du Conseil de recherches en sciences naturelles et en génie du Canada et du Conseil national de recherche du Canada.

D'après un article publié par La Presse en janvier 2018, le FBI a déposé des accusations contre le professeur Ishiang Shih. M. Shih a affirmé que les accusations n'étaient pas fondées et découlaient d'un malentendu. Selon La Presse, les autorités américaines accusent M. Shih et son frère de comploter, depuis 2006, pour voler des technologies et des propriétés intellectuelles canadiennes et américaines en vue d'appuyer, avec le concours des autorités chinoises, l'essor d'une entreprise en Chine qui fabrique des semi-conducteurs destinés à des applications civiles et militaires.

Les autorités américaines ont officiellement demandé l'extradition de M. Ishiang Shih le 10 octobre 2018. Selon l'article, le ministère de la Justice du Canada étudie toujours la demande. M. Shih a pris sa retraite de l'Université McGill peu après la publication de l'article dans La presse. En janvier 2018, le FBI a appréhendé le frère de M. Shih, qui a été accusé de possession illégale de technologies et de les avoir transférées sans permis à une entreprise chinoise

### Contacts :

Préparée par : Non-applicable

Approuvé par : Tricia Geddes, Directrice adjointe, Politiques et Partenariats stratégiques, 

## **5G NETWORK REVIEW**

- The Government of Canada takes the security of our country's critical infrastructure very seriously.
- Canadians can be assured that the Communications Security Establishment (CSE) works to address cyber security concerns to protect Canada's critical infrastructure from threats.
- Since 2013, CSE's Security Review Program has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei. To date, this program has led to the exclusion of designated equipment in sensitive areas of Canadian networks.
- The Government is continuing to review its approach to emerging 5G technology to protect Canada's national security.
- Our Government takes security matters extremely seriously and goes to great lengths to ensure the integrity and protection of our facilities and information.

## **EXAMEN DU RESEAU 5G**

- Le gouvernement prend la sécurité de ses infrastructures essentielles très au sérieux.
- Les Canadiens peuvent être certains que le Centre de la sécurité des télécommunications (CST) travaille en vue d'éliminer les préoccupations en matière de cybersécurité afin de protéger les infrastructures essentielles du Canada contre toute menace.
- Depuis 2013, le Programme d'examen de la sécurité du CST est en place afin de tester et d'évaluer l'équipement et les services qu'on envisage utiliser sur les réseaux canadiens 3G et 4G/LTE, y compris Huawei.
- À ce jour, ce programme a mené à l'exclusion de certaines pièces d'équipement dans des parties sensibles des réseaux canadiens.
- Le gouvernement est à revoir son approche à l'égard de la technologie 5G afin de protéger la sécurité nationale du Canada.
- Notre gouvernement prend les questions liées à la sécurité très au sérieux et ne ménage aucun effort pour assurer l'intégrité et la protection de nos installations et de l'information.

## BACKGROUND

- On June 18, 2018, Senators on the United States (U.S.) Senate intelligence committee warned the federal government and other Five Eyes countries of the risks posed by Chinese smartphone and telecom equipment maker, Huawei. They indicated a desire to see a concerted response among allies and made reference to the integrated nature of the U.S. and Canadian economies and infrastructures as a concern.
- Previously, former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warned the federal government to cut Canadian ties with Huawei. The warning followed comments made by the heads of the CIA, FBI, National Security Agency and the Defence Intelligence Agency that Huawei poses a cybersecurity threat to American customers.
- Media has reported that security officials are particularly concerned that Huawei products in the context of emerging 5G network technologies could provide China with the capacity to conduct remote espionage, modify or steal information, or even shut down systems. John Adams, the former head of the Communications Security Establishment (CSE), was quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. security and intelligence services.
- On May 4, 2018, media reported that the Pentagon banned the sale of Huawei and ZTE phones on military bases. These devices are not currently on sale on Canadian Armed Forces bases.
- On September 7, 2018, media reported that CSE has been testing Huawei's equipment for security vulnerabilities for the last five years. As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services (including Huawei) considered for use on Canadian 3G and 4G/LTE networks. CSE accredits third-party labs to conduct assurance testing in accordance with requirements outlined by CSE. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. While non-disclosure agreements limit the degree to which CSE can comment on specific details, Canadians can be assured that the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadian rely on.
- On September 19, 2018, media reported that the Minister of Public Safety, in response to questions about Huawei, stated that Canada is "examining the issue of security in relation to supply chains right across the government very carefully," but has not made any decisions yet.
- On October 26, 2018, media reported that executives at Huawei Canada have been lobbying members of Parliament from all parties since late August in an effort to convince them that Huawei does not pose a national security threat to Canada.
- On November 2, 2018, media reported that the Government had indicated that it was "not ruling out barring Huawei from supplying equipment for Canada's next generation 5G mobile networks" and that it was "backing away from previous assurances that Canadian security agencies were capable of containing any cyberespionage threat from the Chinese telecommunications giant."
- On December 1, 2018, Wanzhou Meng, the daughter of the founder of Huawei telecommunications and a senior executive at Huawei, was arrested at the Vancouver airport by Canadian officials. The arrest was made pursuant to the U.S.-Canada extradition treaty, under which the U.S. had requested the provisional arrest of Ms. Meng on November 30, 2018. There has been significant press attention in relation to this case, in light of the high-profile nature of Huawei and Ms. Weng, and the significant criticism of Canada by China respecting Ms. Weng's arrest under the *Extradition Act*.
- On December 19, 2018, media reported on comments made by the Prime Minister, who stated that the decision on whether to ban Huawei technology from 5G networks should not be political but one based on experts from its intelligence and security agencies.



- On January 11, 2019, media reported on comments made by Huawei Canada, who stated that it “cannot and would not allow the Chinese government to access the wireless networks its technology supports.”
- On January 11, 2019, media reported that senior Huawei Canada executive Scott Bradley had stepped down.
- On January 18, 2019, media reported that China’s ambassador in Ottawa, Lu Shaye, warned Canadian officials that there would be repercussions if the Canadian government banned Huawei from participating in the 5G networks.
- The week of April 22, 2019, a reported leak from Britain’s National Security Council indicated that the government of Prime Minister Theresa May had decided to allow Huawei – China’s biggest private firm – to play a limited role in non-core parts of Britain’s 5G network.
- On April 29, 2019, Robert Strayer, the U.S. State Department’s deputy assistant secretary for cyberpolicy, called the reported decision “an unacceptable risk” and warned that Washington might rethink intelligence sharing with any country that allowed “unsecure and untrusted vendors” into its 5G networks.
- On April 30, 2019, the Minister of Public Safety said a national-security review of Huawei is still under way. The Minister stated further: “We understand the importance and the urgency of the question,” he told reporters on Tuesday. “We want to make sure Canadians have access to the best and most beneficial 5G technology and, at the same time, we want to make sure they are safe and that their systems are not compromised.”
- On May 1, 2019, a Globe and Mail article misquoted the Minister of Public Safety as saying that he expects a cabinet decision well before Canadians go to the polls in October. A correction has been sent indicating that “it is the Government’s hope to have more to say in the coming months.”

Department / Ministère : Public Safety Canada

Name of PCO Policy Analyst / Nom de l’analyste du BCP :

Secretariat / Secrétariat :

Telephone number / Numéro de téléphone :

## **Huawei**

### **Proposed Response:**

- **Our Government takes the security of our country's critical infrastructure very seriously.**
- **Canadians can be assured that the Communications Security Establishment (CSE) works to address cyber security concerns to protect Canada's critical infrastructure from threats.**
- **Since 2013, CSE's Security Review Program has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.**
- **Our Government is currently reviewing its approach to emerging 5G technology to protect Canada's national security.**
- **Our Government takes security matters extremely seriously and goes to great lengths to ensure the integrity and protection of our facilities and information.**

## Huawei

### Background:

- On June 18, 2018, Senators on the United States (U.S.) Senate intelligence committee warned the federal government and other Five Eyes countries of the risks posed by Chinese smartphone and telecom equipment maker, Huawei. They indicated a desire to see a concerted response among allies and made reference to the integrated nature of the U.S. and Canadian economies and infrastructures as a concern.
- Previously, former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warned the federal government to cut Canadian ties with Huawei. The warning followed comments made by the heads of the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA) and the Defence Intelligence Agency (DIA) that Huawei poses a cybersecurity threat to American customers.
- Media has reported that security officials are particularly concerned that Huawei products in the context of emerging 5G network technologies could provide China with the capacity to conduct remote espionage, modify or steal information, or even shut down systems. John Adams, the former head of the Communications Security Establishment (CSE), was quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. security and intelligence services.
- On May 4, 2018, media reported that the Pentagon banned the sale of Huawei and ZTE phones on military bases. These devices are not currently on sale on Canadian Armed Forces bases.
- On September 7, 2018, media reported that CSE has been testing Huawei's equipment for security vulnerabilities for the last five years. As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services (including Huawei) considered for use on Canadian 3G and 4G/LTE networks. CSE accredits third-party labs to conduct assurance testing in accordance with requirements outlined by CSE. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. While non-disclosure agreements limit the degree to which CSE can comment on specific details, Canadians can be assured that the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadian rely on.
- On September 19, 2018, media reported that the Minister of Public Safety, in response to questions about Huawei, stated that Canada is "examining the issue of security in relation to supply chains right across the government very carefully" but has not made any decisions yet.
- On October 26, 2018, media reported that executives at Huawei Canada have been lobbying members of Parliament from all parties since late August in an effort to convince them that Huawei does not pose a national security threat to Canada.
- On November 2, 2018, media reported that the Government had indicated that it was "not ruling out barring Huawei from supplying equipment for Canada's next generation 5G mobile networks" and that it was "backing away from previous assurances that Canadian security agencies were capable of containing any cyberespionage threat from the Chinese telecommunications giant."
- On December 1, 2018, Wanzhou Meng, the daughter of the founder of Huawei telecommunications and a senior executive at Huawei, was arrested at the Vancouver airport by Canadian officials. The arrest was made pursuant to the U.S.-Canada extradition treaty, under which the U.S. had requested the provisional arrest of Ms. Meng on November 30, 2018. There has been significant press attention in relation to this case, in light of the high-profile nature of Huawei and Ms. Weng, and the significant criticism of Canada by China respecting Ms. Weng's arrest under the *Extradition Act*.
- On December 19, 2018, media reported on comments made by the Prime Minister, who stated that the decision on whether to ban Huawei technology from 5G networks should not be political but one based on experts from its intelligence and security agencies.
- On January 11, 2019, media reported on comments made by Huawei Canada, who stated that it "cannot and would not allow the Chinese government to access the wireless networks its technology supports."
- On 11 January 2019, media reported that senior Huawei Canada executive Scott Bradley had stepped down.

### Contacts:

Prepared by: Gregory Bunghardt, Acting Senior Policy Advisor, National Cyber Security Directorate, 613-991-2811  
Approved by: Monik Beaugard, Senior Assistant Deputy Minister, 613-990-4976

## **Huawei**

### **Proposed Response:**

- **Our Government takes the security of our country's critical infrastructure very seriously.**
- **Canadians can be assured that the Communications Security Establishment (CSE) works to address cyber security concerns to protect Canada's critical infrastructure from threats.**
- **Since 2013, CSE's Security Review Program has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.**
- **Our Government is currently reviewing its approach to emerging 5G technology to protect Canada's national security.**
- **Our Government takes security matters extremely seriously and goes to great lengths to ensure the integrity and protection of our facilities and information.**

## Huawei

### Background:

- On June 18, 2018, Senators on the United States (U.S.) Senate intelligence committee warned the federal government and other Five Eyes countries of the risks posed by Chinese smartphone and telecom equipment maker, Huawei. They indicated a desire to see a concerted response among allies and made reference to the integrated nature of the U.S. and Canadian economies and infrastructures as a concern.
- Previously, former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warned the federal government to cut Canadian ties with Huawei. The warning followed comments made by the heads of the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA) and the Defence Intelligence Agency (DIA) that Huawei poses a cybersecurity threat to American customers.
- Media has reported that security officials are particularly concerned that Huawei products in the context of emerging 5G network technologies could provide China with the capacity to conduct remote espionage, modify or steal information, or even shut down systems. John Adams, the former head of the Communications Security Establishment (CSE), was quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. security and intelligence services.
- On May 4, 2018, media reported that the Pentagon banned the sale of Huawei and ZTE phones on military bases. These devices are not currently on sale on Canadian Armed Forces bases.
- On September 7, 2018, media reported that CSE has been testing Huawei's equipment for security vulnerabilities for the last five years. As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services (including Huawei) considered for use on Canadian 3G and 4G/LTE networks. CSE accredits third-party labs to conduct assurance testing in accordance with requirements outlined by CSE. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. While non-disclosure agreements limit the degree to which CSE can comment on specific details, Canadians can be assured that the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadian rely on.
- On September 19, 2018, media reported that the Minister of Public Safety, in response to questions about Huawei, stated that Canada is "examining the issue of security in relation to supply chains right across the government very carefully" but has not made any decisions yet.
- On October 26, 2018, media reported that executives at Huawei Canada have been lobbying members of Parliament from all parties since late August in an effort to convince them that Huawei does not pose a national security threat to Canada.
- On November 2, 2018, media reported that the Government had indicated that it was "not ruling out barring Huawei from supplying equipment for Canada's next generation 5G mobile networks" and that it was "backing away from previous assurances that Canadian security agencies were capable of containing any cyberespionage threat from the Chinese telecommunications giant."
- On December 1, 2018, Wanzhou Meng, the daughter of the founder of Huawei telecommunications and a senior executive at Huawei, was arrested at the Vancouver airport by Canadian officials. The arrest was made pursuant to the U.S.-Canada extradition treaty, under which the U.S. had requested the provisional arrest of Ms. Meng on November 30, 2018. There has been significant press attention in relation to this case, in light of the high-profile nature of Huawei and Ms. Weng, and the significant criticism of Canada by China respecting Ms. Weng's arrest under the *Extradition Act*.
- On December 19, 2018, media reported on comments made by the Prime Minister, who stated that the decision on whether to ban Huawei technology from 5G networks should not be political but one based on experts from its intelligence and security agencies.
- On January 11, 2019, media reported on comments made by Huawei Canada, who stated that it "cannot and would not allow the Chinese government to access the wireless networks its technology supports."
- On 11 January 2019, media reported that senior Huawei Canada executive Scott Bradley had stepped down.

### Contacts:

Prepared by: Gregory Bunghardt, Acting Senior Policy Advisor, National Cyber Security Directorate, 613-991-2811  
Approved by: Monik Beaugard, Senior Assistant Deputy Minister, 613-990-4976

## **CSIS Engagement with Canadian Universities**

**Issue:** A December 10, 2018 *Globe and Mail* article reports that the Canadian Security Intelligence Service (CSIS) met with researchers at Canadian universities recently to share concerns about research partnerships with Chinese electronics firm Huawei.

### **Proposed Response:**

- **CSIS has a duty, mandated by Parliament, to investigate threats to the security of Canada, including long-term threats to Canada's national interests and prosperity.**
- **To this end, CSIS regularly engages with Canadians from all walks of life, including from universities, to advise them of potential threats to the security and interests of Canada and to provide information regarding the nature of specific threats.**
- **Last week, the Director of CSIS spoke publicly about the attractive target that Canadian companies and research institutions represent for foreign actors or intelligence services seeking access to leading edge research to further their own economic, political or military interests.**
- **In his speech, the Director mentioned that academics and entrepreneurs are particularly vulnerable to this type of activity, because they often lack awareness and resources to protect themselves from this threat.**
- **While the details of meetings that CSIS officials conduct cannot be confirmed, for national security reasons, it can be said that CSIS briefs the U15 Group of Canadian Research Universities on national security issues relevant to them when necessary.**

## CSIS Engagement with Canadian Universities

### Background:

A December 10, 2018 Globe and Mail article reports that, on October 4, 2018, a Canadian Security Intelligence Service's (CSIS) Assistant Director of Intelligence, Michael Peirce, met with vice presidents from a group of leading research-intensive universities known as the "U15" to discuss national security issues. The article reports that at least one follow up meeting is planned for December 19, 2018.

The article states that CSIS expressed concerns about Huawei's development and deployment of next generation 5G wireless technology in Canada, in particular about Canadian universities research partnerships with Huawei.

A previous Globe and Mail article from May 2018, indicated that Huawei had established a vast network of relationships with leading research-heavy universities in Canada to create a steady pipeline of intellectual property that the company is using to underpin its market position in 5G. The Globe and Mail reports that the company has committed about \$50 million to 13 leading universities and close to 100 professors and their graduate students have worked on Huawei funded projects obtaining millions of dollars in government grants. In addition, in dozen of cases, the academics assigned all intellectual property rights to Huawei. Global Affairs Canada has routinely granted export permits to Huawei, allowing it to transfer the research back to China.

Three former Canadian intelligence chiefs have warned the deployment of Huawei products and 5G technology in telecommunications networks could provide China with the capacity to conduct remove spying, maliciously modify or steal information and even shut down systems.

In a December 4, 2018 speech to the Economic Club of Canada, CSIS Director stated that CSIS has observed a trend of state-sponsored espionage in fields that are crucial to Canada's ability to build and sustain a prosperous, knowledge based economy, including 5G.

### Contacts:

Prepared by:  
Approved by:

N/A

Tricia Geddes, Assistant Director Policy and Strategic Partnerships

## **Engagement du SCRS avec des universités canadiennes**

**Question :** Selon un article publié le 10 décembre 2018 dans le *Globe and Mail*, le Service canadien du renseignement de sécurité (SCRS) a rencontré des chercheurs d'universités canadiennes récemment pour les mettre en garde contre la participation à des projets de recherche et de développement en collaboration avec la société chinoise d'électronique Huawei.

### **Réponses proposées :**

- **Le SCRS a le mandat d'enquêter sur les menaces pour la sécurité du Canada, notamment celles qui, à long terme, pèsent sur les intérêts et la prospérité du pays.**
- **À cette fin, le SCRS noue régulièrement des relations avec des Canadiens de tous les milieux, y compris d'instituts de recherche, pour les sensibiliser aux menaces potentielles pour la sécurité et les intérêts du Canada et leur fournir des informations par rapport à la nature de certaines de ces menaces.**
- **La semaine dernière, le directeur du SCRS a parlé publiquement du fait que les entreprises et les instituts de recherche canadiens constituent des cibles attrayantes pour les intervenants ou les services de renseignement étrangers qui cherchent à avoir accès à des recherches de pointe en vue de faire progresser leurs propres intérêts économiques, politiques ou militaires.**
- **Dans son discours, le directeur a souligné que les universitaires et les entrepreneurs sont particulièrement vulnérables à ce type d'activités, parce que, bien souvent, ils ne sont pas sensibilisés à la question et ne disposent pas des ressources nécessaires pour faire face à cette menace.**



- **Pour des raisons de sécurité nationale, il ne peut pas confirmer aucun détail au sujet de rencontres réalisées par des représentants du SCRS. Toutefois, il peut dire que le SCRS, au besoin, informe le U15, c'est-à-dire le Regroupement des universités de recherche du Canada, des questions de sécurité nationale le concernant.**

## Engagement du SCRS avec des universités canadiennes

### Contexte :

Selon un article publié dans le *Globe and Mail* le 10 décembre 2018, Michael Peirce, directeur adjoint du Renseignement du Service canadien du renseignement de sécurité (SCRS), a rencontré le 4 octobre dernier les vice-présidents d'un groupe regroupant les universités les plus axées sur la recherche, appelé « U15 », afin de discuter de questions liées à la sécurité nationale. L'article indique qu'une des rencontres de suivi doit avoir lieu le 19 décembre.

Toujours selon l'article, le SCRS se dit préoccupé par le développement de la nouvelle génération de technologie sans fil, 5G, par Huawei et sa mise en œuvre au Canada, tout particulièrement par les partenariats que des universités canadiennes ont conclus avec cette société.

D'après un autre article paru dans le *Globe and Mail* en mai 2018, Huawei a mis sur pied un vaste réseau de contacts avec des universités très axées sur la recherche au Canada, afin de créer un flux constant de propriété intellectuelle qui lui sert de base pour renforcer sa place sur le marché de la technologie 5G. Selon le *Globe and Mail*, la société a versé environ 50 millions de dollars à 13 universités de renom et près d'une centaine de professeurs de même que des étudiants de cycle supérieur ont travaillé à des projets financés par Huawei et recevant des millions de dollars en subventions de la part du gouvernement. En outre, dans une dizaine de cas, des universitaires ont consenti tous les droits de propriété intellectuelle à Huawei. Affaires mondiales Canada a régulièrement accordé des licences d'exportation à Huawei, ce qui lui permet de transférer les travaux de recherche en Chine.

Trois anciens chefs du renseignement canadiens ont lancé une mise en garde, c'est-à-dire que la mise en œuvre de produits et de la technologie 5G de Huawei dans les réseaux de télécommunications pourraient donner les moyens à la Chine de se livrer à de l'espionnage à distance, de modifier ou de voler des informations à des malveillantes et même de paralyser des systèmes.

Dans le discours prononcé devant l'Economic Club of Canada le 4 décembre dernier, le directeur du SCRS, David Vigneault, a mentionné que le SCRS avait remarqué que les activités d'espionnage parrainées par des États avaient tendance à être menées dans des domaines essentiels à l'édification et au soutien d'une économie du savoir prospère au Canada, y compris la technologie 5G.

### Contacts :

Préparée par : Non-applicable

Approuvé par : Tricia Geddes, Directrice adjointe, Politiques et Partenariats stratégiques, 

## HUAWEI

- The Government of Canada is aware of the concerns and takes the security of its critical infrastructure very seriously.
- The Communications Security Establishment provides advice and guidance on information technology security to the Government of Canada, including equipment manufactures that are part of the Canadian supply chain.
- CSE works to address cyber security concerns In Canada's communications infrastructure. This is done in collaboration with telecommunications providers and equipment vendors.
- CSE, alongside its partner Public Safety Canada, also shares security advice and guidance with the private sector owners and operators of Canada's critical information infrastructures.
- While we are unable to comment on specific companies, products or providers, Canadians can be assured that the Government works diligently to monitor for security threats and that there are measures are in place to protect Canada's systems.

## HUAWEI

- Le gouvernement du Canada est au courant des préoccupations et prend la sécurité de ses infrastructures essentielles très au sérieux.
- Le Centre de la sécurité des télécommunications fournit des conseils et des directives sur la sécurité des TI au gouvernement du Canada, de même qu'aux fabricants d'équipement faisant partie de la chaîne d'approvisionnement canadienne.
- Le CST s'emploie à répondre aux préoccupations en matière de cybersécurité qui touchent l'infrastructure des communications du Canada.
- En partenariat avec Sécurité publique Canada, le CST fournit des conseils et des directives sur la sécurité des TI aux propriétaires et exploitants des infrastructures d'information essentielles du Canada.
- Bien que nous ne puissions émettre de commentaires sur des entreprises, des produits ou des fournisseurs particuliers, soyez assurés que le gouvernement s'emploie avec diligence à surveiller les menaces et que des mesures sont en place pour protéger les systèmes canadiens.

## **BACKGROUND:**

- On March 19, 2018, the Globe and Mail published an article entitled Former Top Canadian Security Officials Warn Ottawa to Sever Links with China's Huawei.
- The article cites comments made by former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warning the federal government to cut Canadian ties with Huawei, the Chinese smartphone and telecom equipment maker.
- The warning follows comments made by the heads of the CIA, FBI, National Security Agency and the Defence Intelligence Agency to the U.S. Senate intelligence committee that Huawei poses a cybersecurity threat to American customers.
- The article states that security officials are particularly concerned that Huawei products and the new 5G technology provide China with the capacity to conduct remote spying and maliciously modify or steal information or even shut down systems.
- John Adams, the former head of the Communications Security Establishment (CSE), is quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. spy services.
- Links may be drawn between this article and the ENCQOR announcement being made today by the ISED Minister related to 5G innovation.

## 2018-2019 Main Estimates

### CYBER SECURITY

#### PROPOSED RESPONSE:

- **The cyber threat landscape is constantly evolving and is challenging the Canadian government to develop new ways of providing domestic security and contributing to international cyber security.**
- **Public and internal consultations conducted by Public Safety over two years (2016-2018) through the Cyber Review revealed several key areas for action for the federal government. This includes demonstrating strong leadership in order to clarify cyber security roles, responsibilities, and accountabilities within the federal government; offering strong support for law enforcement to address cybercrime; developing and promoting established standards, best practices and certification, and legislation; and increasing public education and awareness.**
- **As part of Budget 2018, the Government proposes significant investments of \$507.7 million over five years, and \$108.8 million per year thereafter, to fund a new National Cyber Security Strategy. To implement this plan, the Government will work alongside key partners such as other levels of government, the business community, academia and trusted international partners. Canada will work to proactively solve mutual cyber issues, raising the cyber security bar for all Canadians.**
- **Additionally, in response to the increase in the frequency and magnitude of malicious cyber activity, the Five Eyes and likeminded countries are increasingly pursuing a coordinated approach to publically attribute such activities to the perpetrators. This is done with a view to deterring malicious activities in cyber space.**

## Backgrounder:

The Internet provides opportunities for Canadians to participate in a new global digital economy and enjoy many social and economic advantages resulting from technological advances. But as we rely more on information technologies, we also face greater vulnerability to those who would seek to attack and undermine our digital infrastructure. By taking action to protect the cyber systems on which Canadians rely, the Government is protecting Canadians' security, public safety, economic prosperity and way of life.

As part of the Minister of Public Safety and Emergency Preparedness' mandate letter, the department was tasked with leading a review of existing measures to protect Canadians and our critical infrastructure from cyber threats.

This review was carried out in collaboration with the Ministers of National Defence, Innovation, Science and Economic Development, Infrastructure and Communities, Public Services and Procurement, and the President of the Treasury Board.

It should be noted that the public consultation was only one part of the broader Cyber Review. The results from the public consultations were consolidated with the results of:

- **Internal consultations** on Government of Canada Information and Infrastructure; and
- the **horizontal evaluation** of Canada's Cyber Security Strategy, covering the period of 2010-2015.

With the 2018 Budget, the Government of Canada is implementing a plan for security and prosperity in the digital age to protect against cyber-attacks. The Government proposes significant investments of \$507.7 million over five years, and \$108.8 million per year thereafter, to fund a new National Cyber Security Strategy. The Strategy focuses on three principal goals:

- Ensure secure and resilient Canadian systems.
- Build an innovative and adaptive cyber ecosystem.
- Support effective leadership and collaboration between different levels of Canadian government, and partners around the world.

Canada's plan for security in the digital age starts with a strong federal cyber governance system to protect Canadians and their sensitive personal information. To that end, the Government proposes to commit \$155.2 million over five years, and \$44.5 million per year ongoing, to the Communications Security Establishment to create a new Canadian Centre for Cyber Security.

By consolidating operational cyber expertise from across the federal government under one roof, the new Canadian Centre for Cyber Security will establish a single, unified Government of Canada source of unique expert advice, guidance, services and support on cyber security operational matters, providing Canadian citizens and businesses with a clear and trusted place to turn to for cyber security advice. In order to establish the Canadian Centre for Cyber Security, the Government will introduce legislation to allow various Government cyber security functions to consolidate into the new Centre. Federal responsibility to investigate potential criminal activities will remain with the RCMP.

To bolster Canada's ability to fight cybercrime, the Government also proposes to provide \$116.0 million over five years, and \$23.2 million per year ongoing, to the RCMP to support the creation of the National Cybercrime Coordination Unit. The National Cybercrime Coordination Unit will create a coordination hub for cybercrime investigations in Canada and will work with international partners on cybercrime. The Unit will also establish a national public reporting mechanism for Canadian citizens and businesses to report cybercrime incidents to law enforcement.

Additionally, there are several noteworthy federal initiatives that are part of the Government's broader approach to cyber security; these include Canada's National Defence Policy, CSE's work with the Minister of Democratic Institutions, amendments to CSE's legislation, and ISED's Innovation and Skills Plan.

Canada has, as far back as 2012, attributed cyber attacks to government-backed hackers from China and Russia. A recent chronology is attached.

The 2018-19 Main Estimates include vote appropriations for the Public Safety Portfolio of \$15,992,321.

### CONTACTS:

Marc Goldfinger

Tel. no.  
613-991-9912

Approved by  
Monik Beaugard SADM

Tel. no.  
613-990-4976

### Public Attributions of Cybercrime

- **2012:** CSIS Public Report – Assessing Threats to Canadian Infrastructure: “Canada...[is] vulnerable to cyber-espionage and sabotage activities. Many of these cyber attacks are reportedly attributed to government-backed hackers from **China and Russia**.” “Canada’s dependence on digital networks and Internet-based communications has increased its vulnerability to cyber attacks, a large proportion of which have been reportedly attributed to government-backed hackers from **China and Russia**.” “Cyber attacks launched over the Internet are the fastest-growing form of espionage. Canada’s ...advanced industries such as telecommunications, mining, agriculture, biotechnology and the aerospace industry make it an attractive target.”
- **2014:** Treasury Board of Canada: A "highly sophisticated **Chinese** state-sponsored actor" hacked into the computer systems at Canada's **National Research Council**.
- **2014:** U.S. charges five PLA officers (the Chinese People's Liberation Army) for cyber espionage against U.S. corporations and a labor organization for commercial advantage
- **2015:** China named as leading suspect in investigation of OPM databases hacks by FBI Director James Comey.
- **2016:** CSIS: “**Russia and China**, in particular, continue to target Canada’s classified information and advanced technology, as well as government officials and systems.” (Toronto Star, citing briefing note prepared for Director Michel Coulombe’s appearance at a March meeting of the Senate committee on national security and defence, obtained through an Access to Information Request.)
- **2017 (Feb.):** UK Defence Secretary Michael Fallon: “[**Russia** has used] cyber weaponry to disrupt critical infrastructure and disable democratic machinery.” Examples provided included:
  - o France’s TV5Monde was taken off air
  - o Germany’s lower house of parliament’s network was shut down
  - o US Presidential election was targeted
- **2017 (Mar.5):** Minister of Foreign Affairs, Chrystia Freeland, told reporters in Parliament: “It is public knowledge that there have been efforts...by **Russia** to destabilize the U.S. political system. I think that Canadians and, indeed, other Western countries should be prepared for similar efforts to be directed at us.”
- **2017 (Jun.26):** Prime Minister’s Office: “[Canada and **China**] agreed that neither country’s government would conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”
- **2017 (Dec.19):** CSE Public Statement: “We are aware of the statements made by our allies and partners concerning the role of actors in **North Korea** in the development of the malware known as WannaCry. This assessment is consistent with our analysis.” The United States, United Kingdom, Australia, New Zealand, and Japan also attributed WannaCry to North Korea.
- **2018 (Feb.15):** CSE Public Statement: “CSE also assesses that actors in **Russia** were responsible for developing NotPetya.” The United States, United Kingdom, Australia and New Zealand also attributed NotPetya to Russia.
- **2018 (Mar.15):** US FBI & DHS: “Since at least March 2016, **Russian** government cyber actors—hereafter referred to as “threat actors”—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.”



s.15(1) - Int'l  
s.15(1) - Subv  
s.21(1)(b)  
s.24(1)

**SECRET**

**RETREAT OF THE DEPUTY MINISTERS' COMMITTEE ON NATIONAL SECURITY**

March 25, 2019

Time: 11:00 a.m. – 4:00 p.m.

Location: 80 Wellington Street, Room 415

**List of Participants**

<p>Ms. Greta Bossenmaier, PCO co-chair          Mr. Vincent Rigby, PS co-chair          Mr. David McGovern, ISED          Mr. John Ossowski, CBSA          Mr. Rob Stewart, FIN          Mr. Francois Daigle, JUS          Ms. Shelly Bruce, CSE          [REDACTED] CSIS          Ms. Nada Semaan, FINTRAC          Mr. Jeffrey Hutchinson, CCG          Gen. Jonathan Vance, CDS          Ms. Jody Thomas, DND          Mr. Ian Shugart, GAC          Ms. Brenda Lucki, RCMP          Mr. Michael Keenan, TC          Ms. Tina Namiesniowski, CBSA          Mr. Gordon Venner, DND</p>	<p>Mr. Ian McCowan, PCO          Mr. Matthew Mendelsohn, PCO          Mr. Bill Matthews, PSPC            Ms. Monik Beauregard, PS          Ms. Caroline Xavier, PCO          Mr. Martin Green, PCO          Ms. Cindy Termorshuizen, GAC          Ms. Mary Gregory, ISED          Ms. Riri Shen, PCO          Mr. Allen Sutherland, PCO            [REDACTED]            Note taker: Brett Hockley          Note taker: Ian McKierahan</p>
--	--

**1. Introduction**

[REDACTED]

**Pages 26 to / à 34  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 21(1)(a), 21(1)(b)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 35 to / à 46  
are not relevant  
sont non pertinentes**

**Pages 47 to / à 48  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 49 to / à 55  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 18(a), 21(1)(a), 21(1)(b)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 56 to / à 67  
are not relevant  
sont non pertinentes**



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**SECRET**

DATE:

File No.: PS-022826

**MEMORANDUM FOR THE MINISTER**

**RESPONSE TO QUESTIONS RELATED TO  
"PROJECT SIDEWINDER" REPORT**

(Information only)

**ISSUE**

In a recent meeting, Mr. Gordie Hogg, Member of Parliament for South Surrey – White Rock, provided information and questions from one of his constituents related to a draft intelligence report from 1997.

**BACKGROUND**

SIDEWINDER was a joint project between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) to assess the threat posed by the acquisition and control of Canadian companies by members or associates of triads involved with the Chinese Intelligence Services. The first draft of the report, titled *Chinese Intelligence Services and Triads Financial Links in Canada* was written in 1997 and extensively revised and finalized in 1999.

In the fall of 1999, various media outlets reported on SIDEWINDER based on a leaked classified draft dated June 24, 1997. A copy of the report and a Globe and Mail article forwarded by Mr. Hogg are attached at **TAB A** and **TAB B**, respectively. The media speculated that the project was mismanaged and that the revisions to the earlier draft failed to adequately notify the Government of an emerging issue.

s.15(1) - Subv



.../2

**SECRET**

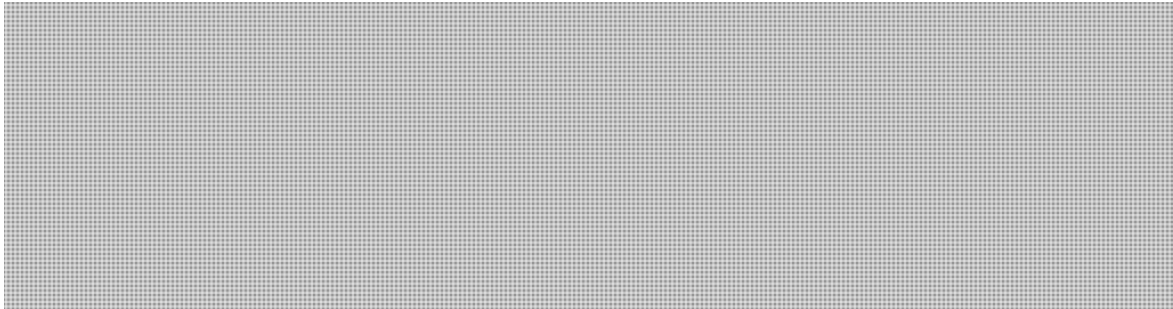
- 2 -

Additionally, the Security Intelligence Review Committee (SIRC) conducted a review of SIDEWINDER and provided details in their 1999-2000 Annual Report (**TAB C**). They found that the first draft was “deeply flawed in almost all aspects” and that there was “no evidence of any substantive or immediate threat of the sort envisaged in the first Sidewinder draft ... and no evidence that the Government had not been appropriately warned of substantive threats”.

**CONSIDERATIONS**

s.15(1) - Int'l

s.15(1) - Subv



Should you require any additional information, please do not hesitate to contact me at 613-991-2895 or Monik Beauregard, Senior Assistant Deputy Minister, National and Cybersecurity Branch at 613-990-4976.

Malcolm Brown

Enclosures: (3)





SUBSCRIBE

LOG IN

## China set up crime web in Canada, report says

ANDREW MITROVICA AND JEFF SALLOT  
TORONTO AND OTTAWA  
PUBLISHED APRIL 29, 2000  
UPDATED MARCH 27, 2018

ANDREW MITROVICA in Toronto JEFF SALLOT in Ottawa

The Chinese government and Asian criminal gangs have been working together in drug smuggling, nuclear espionage and other criminal activities that constitute a grave threat to Canadian security, a secret study by federal law-enforcement and intelligence analysts says.


"In many ways, China remains one of the greatest ongoing threats to Canada's national security and Canadian industry," the report says.

STORY CONTINUES BELOW ADVERTISEMENT

The study, titled Chinese Intelligence Services and Triads Financial Links in Canada, was prepared in June, 1997, by as many as five analysts from the Royal Canadian Mounted Police and the Canadian Security Intelligence Service who worked for about two years using classified files from both agencies.

Copies of the original draft were destroyed or kept under lock and key until The Globe and Mail obtained one this week.

The study, known as Project Sidewinder, was considered by some CSIS managers to be so controversial that it was watered down and rewritten before a sanitized version was circulated to other government agencies last year, according to sources familiar with the history of the document.

The  under report describes an alliance among the Beijing government and its intelligence services, Hong Kong tycoons and Chinese criminal gangs known as triads. The ultimate objectives included:

Winning influence with Canadian politicians.

Stealing high-tech secrets.


Laundering money.

STORY CONTINUES BELOW ADVERTISEMENT

STORY CONTINUES BELOW ADVERTISEMENT

Gaining control of Canadian companies in real estate, media and other sectors.

The RCMP and CSIS files revealed only "the tip of the iceberg," the analysts concluded. They recommended expanding their joint task force to include officials from the Department of Foreign Affairs and International Trade, Immigration Canada and Canada Customs.

 The recommendation was never followed. Instead, CSIS managers shelved the 1997 draft and dismissed its conclusions as a rumour-laced conspiracy theory, with little factual evidence to support its potentially explosive conclusions.

The Security Intelligence Review Committee, an independent watchdog body, is investigating allegations that the original Sidewinder report was suppressed because of political pressure. The committee is expected to complete its investigation and release the results to Parliament within weeks.

Chinese embassy spokeswoman Qin Xin denied that her government is involved in espionage or criminal activities in Canada or poses any threat to Canadian national security. "These kinds of accusations are totally groundless," she said.

Spokesmen for the RCMP and CSIS would not comment on the main conclusion of the study -- that China poses a grave threat to Canadian national security.

STORY CONTINUES BELOW ADVERTISEMENT

The Sidewinder study is still classified secret and thus the RCMP can't talk about it, Mountie spokesman Sergeant Andre Guertin said.

CSIS spokesman Dan Lambert said the service does not discuss targets, so it will not confirm or deny whether it considers Chinese activities in Canada a security threat. He did say that CSIS maintains a vigorous counterintelligence program.

Mr. Lambert denied that the original Sidewinder study was watered down and insisted there was no interference from the agency's political bosses.

Both the RCMP and CSIS subjected the 1997 draft to extensive review to make sure the final version, which was produced in 1999, could be supported by facts, he said.

CSIS, familiar with the 1997 version, however, bristled at Mr. Lambert's version of events and noted that the Liberal government has courted trade and business opportunities with China since coming to office in 1993. Prime Minister Jean Chrétien plans to lead another trade mission to China this year.

The analysts wrote in the foreword of their 23-page study that "this report presents concrete facts, not just ideas or speculation."

The study notes that an earlier RCMP investigation, code-named Project Sunset, turned up evidence that an international food-services company based in Southern Ontario was involved in smuggling heroin into Canada from Hong Kong. The company's chairman was affiliated with a triad. Company managers met regularly with Chinese trade and military representatives in Canada.

The report also says Ontario Hydro believes it was the victim of theft of nuclear technology "by an individual of Chinese origin." The man sent hours worth of material by fax to a telephone number at a Chinese state science and technology commission.


In two other cases the report cited, employees of Chinese origin at Canadian high-tech companies stole proprietary information and sold it to China.

The report says Chinese intelligence services send agents to Canada as part of business and trade delegations.

Chinese intelligence services have set up "front companies" in Canada solely for espionage purposes, including theft of business secrets, the report says. The companies have regular contacts with the triad gangs.

Drawing on intelligence developed by other Western countries, the analysts say there is a well-established relationship between the Communist government in Beijing and the Hong Kong-based triads.

More than 200,000 Hong Kong residents immigrated to Canada during the 1990s. The report says the great majority of these immigrants "were legitimate,

but  lian authorities detected a significant presence of Chinese organized crime elements." Some eventually acquired Canadian citizenship.

The study notes that a former Canadian citizenship court judge faces 33 fraud and forgery charges in connection with immigration applications by Hong Kong residents. The RCMP laid the charges in May, 1997, but the case has yet to come to trial.

Some Hong Kong investors and mainland Chinese with ties to the Communist Party leadership and Chinese intelligence services came here using the "entrepreneur" and "investor" categories for Canadian immigration, the report says.

Canadian intelligence indicates that some of these people have worked with the Beijing regime to establish companies that are used as cover for criminal and espionage activities, the report says. "This country is an excellent place to invest in companies to launder the profits derived from criminal activities."

Some companies controlled by Hong Kong executives with ties to the Beijing regime have obtained federal government classified contracts, the report says.

The study also says more than 200 major firms in Canada are influenced or owned by triads, tycoons or Chinese national companies.

The Chinese government buys or sets up a legal company in Canada that in turn buys other companies, the report says, creating "an effective domino effect . . . that acts like a well-spun web or network of strategic points."

Initially, the study says, Chinese intelligence agencies acquired firms in so-called soft-sector firms that attracted little attention from CSIS, but then moved to take control of more sensitive companies in high-tech sectors.

Thus, China is quietly but systematically acquiring sensitive Canadian technology, including nuclear information, and is exerting undue influence over Canada's political environment by assuming control of key portions of Canadian industry, the report insists.

The **THE GLOBE AND MAIL** says there is Chinese "interference" in politics through political donations. It said the U.S. Federal Bureau of Investigation is investigating about 2,000 companies to determine whether they are being used by the Chinese to funnel illegal campaign contributions to U.S. political parties.

In Canada, the study says, the same pattern can be discerned. Companies believed to be controlled by Chinese interests contributed money to the federal Liberal and Progressive Conservative parties between 1991 and 1994.

Prominent former Canadian politicians have been named to boards of Chinese state-owned corporations, the report adds. The report did not identify the politicians by name.

Beijing has a particular interest in Chinese-language media in Canada, the study says. It notes that one Chinese-language cable TV outlet was the target of a takeover bid by a Hong Kong triad figure in 1992. The bid was withdrawn after federal officials notified the Canadian Radio-television and Telecommunications Commission of the bidder's connections to organized crime.

A Chinese-language film-production studio in Ontario was owned by triad figures who were in regular contact with Chinese diplomats posted here, the report says.

The study notes various real-estate purchases, including hotels, in Toronto, Vancouver and other Canadian cities by the owner of a large south Asian gambling casino. The man was put on a Canadian police watch list 10 years ago because of his alleged involvement in organized crime.

FOLLOW US ON TWITTER @GLOBEANDMAIL

REPORT AN ERROR EDITORIAL CODE OF CONDUCT



SUBSCRIBE

LOG IN

BUSINESS SERVICES

CONTACT US

READER SERVICES

ABOUT US

© Copyright 2018 The Globe and Mail Inc. All rights reserved.

351 King Street East, Suite 1600, Toronto, ON Canada, M5A 0N1

Phillip Crawley, Publisher









There may be slight errors in the text below due to the illegibility of the acquired document copy. Web page 1 of 2

# Sidewinder

Secret

RCMP-CSIS Joint Review Committee

Draft Submission

SECRET  
Joint RCMP Study  
Information as of  
24 June 1997  
Translated text

## Chinese Intelligence Services and Triads Financial Links in Canada

Draft Submitted  
to the RCMP-CSIS  
Joint Review Committee

24 June 1997

### TABLE OF CONTENTS

Table of Contents <i>(Note: pages are for the original document not on this HTML)</i>	i
Foreword	iii
Summary	iv
Introduction	1
Beijing's Strategic Alliances, or the lessons of Sun Tsu	1
Immigration to Canada	3
Hundreds of Canadian Companies "Made In China"	4
Case Studies	5
-Multinationals	
CITIC (Canada)	5
Norinco and Poly Technology (Poly Group)	5
-Banks and financial institutions	
CIBC and the Hong Kong Bank of Canada	6
Wood Gundy, Merrill Lynch and Gordon Capital Corp.	6
-High technology	
Semi-Tech Corporation	7
China Huaneng Group, Unipec Canada and Goldpark China Ltd.	7
-Entertainment and Media	
Charles Y. M. Kwan Promotions	8
North American Studios	8
China Vision and Fairchild Entertainment	8
Hong Kong Telecommunications and Wharf Cable Ltd.	9
-Food-Services industry	
Tai Foong International	9
-Real estate and hotels	
Grand Adex Properties Inc. and Concord Pacific Development Corp.	9

World Financial Properties	10
Ramada Hotels, Harbour Castle (Toronto) and others	10
-Universities and research centers	
University of Toronto and University of Western Ontario	10
Chinese Intelligence Services Penetration of Canadian Companies	11
Interference by Financing of Canadian Political Parties	11
The Importance of the Chinese Diaspora	12
Consequences for Canada	12
Recommendations	14
Appendixes	
-Appendix I: Annual number of certifications of permanent residence in Canada for persons from Hong Kong since 1990: "entrepreneur" and "investor" categories	15
-Appendix II: Annual breakdown of the choice of province by permanent residents from Hong Kong "entrepreneur" and "investor" categories	16
-Appendix III: Origin and Description of the Triads	17
-Appendix IV: Description of a Typical Triad Member	
Profile A: Young Adult	20
Profile B: Mature Member	21
-Appendix V: Guanxi or networking	22
-Appendix VI: The Chinese Diaspora	23

## FOREWARD

In May 1996 a joint project was initiated by the RCMP Criminal Analysis Branch and the CSIS Analysis and Production Branch to assess the extent of the threat posed by the acquisition and control of Canadian companies by members or associates of triads and with affiliations to the Chinese Intelligence Services. The research team quickly realized that the initial premise was the tip of the iceberg with only a minute portion of a much more complex situation showing. It should be stressed that this report is a prospective document that makes to claim to provide a full survey of the issue; in fact, quite the opposite.

This document does not present theories but indicators of a multifaceted threat to Canada's national security based on concrete facts drawn from the databanks of the two agencies involved, classified reports from allied agencies and various open sources. This study has departed from the conventional and sometimes confining approaches followed by our respective methodologies. Although both organizations have fairly extensive expertise on Chinese matters, it is nevertheless very different. It is clear at the end of this exercise that both organizations have gained from cooperating on this research. When put together, these two bodies of expertise complement each other, providing a broader and more substantial perspective of the Chinese issues. (S)

The scope of the problem found after a few weeks of research dictated that the initial research results had to be presented in the form of case studies. At the moment, we estimate that over 200 Canadian companies are under the direct or indirect control of China. Although it was impossible to do all the research within the parameters initially given; however, sufficient details have been found to reveal the threat. It should be reiterated that this report presents concrete facts, not just ideas or speculation. We trust that we have demonstrated the need to continue the work within a broader and more elaborate framework. (C)

## Chinese Intelligence Services and Triads Financial Links in Canada SUMMARY

Since the mid-1980s, a substantial immigration flow from Hong Kong has taken place and Canadian authorities were first alerted when a significant presence of Chinese organized crime elements among this group was detected. Many came through the "entrepreneur and "investor" immigration program and some of these criminals even have succeeded to obtain their Canadian citizenship. Although not all immigrants in these categories are suspected, two particular groups of individuals raised attention. Two other groups have also taken advantage of the "entrepreneur" and "investor" categories to immigrate and to invest in Canada. First, a certain number of very rich Hong Kong Chinese business people (tycoons) who are known to have been cooperating with the

Chinese Government for years. Then a group composed of associates and relatives of China's leadership and the Chinese Intelligence Service (ChIS). Intelligence reveals that certain individuals of these three groups have been working for over fifteen years in concert with the Chinese government, and some of their "financial ventures" in Canada serve to conceal criminal or intelligence activities. (S)

Hand in hand with this situation, the ChIS [Chinese Intelligence Service] make very active use of their access to Canadian industries through exchanges of specialists and students, and also set up shell companies to pursue their acquisition of economic and technological intelligence. Cooperation between the Hong Kong tycoons, the triads and the Beijing leadership adds a new dimension to the well known "mass line collection" strategy followed by the ChIS. This situation substantially raises the level of the potential threat, revealing the effectiveness of Chinese efforts to obtain Canadian technology and their capability to interfere in the management of the country. Central points and essential for the understanding of the problem are the cultural singularities that characterize the Chinese as the concepts of "debt of honour", "duties", "*Hou Tai* or backers" and "*Guanxi* or connections." ) (S)

By using these alliances, the Chinese government is trying to gain influence on Canadian politics by maximizing their presence over some of the country's economic levers. To that end, they proceed initially to buy and/or legally set up a company in Canada that, once under their control, buys other companies and so on. An effective domino effect ensues that acts like a well-spun web or network at strategic points. It is estimated that over 200 Canadian companies have passed into Chinese influence or ownership since the early 1980s through the triads, tycoons or China national companies. These businesses are found in various sectors of the economy, ranging from multinationals to banking, high technology and real estate (CITIC, Norinco, Husky Oil, Grand Adex Properties Inc, Merrill Lynch, Gordon Capital, Inc, Tai Foong International, CIBC, Ramada Hotels, China Vision and Semi-Tech Corporation, etc.). The triads' companies are also used to pursue their criminal activities, such as money-laundering and heroin trafficking, as well as assistance to the ChIS. (S)

Being Canadian these businesses are also eligible to receive government subsidies for research or classified contracts from Federal Departments. The risk is that after the research is done, there results can be transferred to China. Other form of risk is with the access gain through classified contract. As an example, a Canadian company under Chinese influence was in contention for a contract to set up and run a classified communications system linking the main agencies of the Canadian intelligence community. A company in Toronto specializing in video surveillance was originally Canadian, but was bought by a Chinese multinational. It is impossible at present to say how many or which Canadian companies are in the same situation. These examples, however, raise questions about the integrity of some companies that have already installed security systems for various Canadian government institutions or Canadian research industries. (S)

Significant portions of some large Canadian urban centres are also owned by Chinese entrepreneurs. For example, it is estimated that Li Ka-Shing owns with his son at least one sixth to one third of downtown Vancouver. (S)

These "corporate" figures have become an influential presence on the political and economic landscapes of Toronto and Vancouver and at the provincial and federal levels. The triads, the tycoons and the ChIS have learned the quick way to gain influence is to provide finance to the main political parties. Most of the companies identified in this research have contributed, sometimes several tens of thousands of dollars, to the two traditional political parties, that is, the Liberal and the Progressive-Conservative Parties. (S)

The Chinese leadership continues to gain much direct or indirect influence over the Canadian economy and politics. Having bought significant real estate holdings and established businesses in Canada, China has obtained access to influential figures who are now or once active at various levels of Canadian society. In many ways, China remains one of the greatest ongoing threats to Canada's national security and Canadian industry. (S)

"Be so subtle that you are invisible.  
Be so mysterious that you are intangible.  
Then you will control your rival's fate."

Sun Tzu,  
The Art of War (c. 509 BC)

## INTRODUCTION

1. With the announcement of the return of Hong Kong to China in the mid-1980s, Canada witnessed the arrival of a substantial immigration and capital flow from that region. For example, between January 1990 and March 1997, 233,077 Hong Kong residents emigrated to Canada, of whom nearly 70,000<sup>1</sup> were in the "entrepreneur" or "investor" category. This exceeded the "family" category over the same period. Although the great majority of these migrants were legitimate, the Canadian authorities detected a significant presence of Chinese organized crime elements, among them, namely the triads and their associates, some of whom succeeded in obtaining Canadian citizenship.<sup>2</sup> (S)
2. Some wealthy Hong Kong Chinese investors and Chinese from Mainland closely affiliated or related with the country's leadership and the ChIS also took advantage of the "entrepreneur" and "investor" categories to emigrate in and invest in Canada. Few even bought or established companies on Canadian soil through family members who had obtained Canadian citizenship. Intelligence indicates that these specific individuals with these three groups: triads, Hong Kong investors and people close to China's leadership, have been identified working with concert with the Chinese government to gain influence through some of their "financial ventures" in Canada. Some companies which are also used to conceal criminal or intelligence activities. At the same time, the ChIS use their access to Canadian businesses through exchanges and technical or student visas to steal classified and technological information. They have gone so far as to set up shell companies to pursue their economic and technological information acquisition operations. (S)
3. A new triumvirate was born. This cooperation between Hong Kong Chinese business people, the triads and the Beijing leadership adds a new dimension to the known mass line collection strategy followed by ChIS. Economic, political and security indicators based on factual data revealed the potential threat and efforts made by the Chinese to obtain Canadian technology, but above all to obtain influence over economic levers and prominent Canadian figures. (S)

## BEIJING'S STRATEGIC ALLIANCES, OR THE LESSONS OF SUN TZU

4. When Deng Xiaoping came to power in the late 1970s, he introduced his economic reforms with the slogan "to get rich is glorious." To achieve that end, he had to move China onto the international markets. The isolationism of the former regime, however, handicapped the Chinese leadership. It therefore turned to the richest Chinese business people of Hong Kong, including, among many others, Li Ka-Shing, Henry Fok Ying-Tung, Wang Foon-Shing, Stanley Ho<sup>3</sup> and the man who would eventually be chosen by Beijing to head Hong Kong after the departure of the British, Tung Chee-Wa (C.H. Tung). On 23 May 1982, Li Ka-Shing and Henry Fok met with Deng Xiaoping and Zhao Ziyang in Beijing to discuss the future of the peninsula. Their task would be to advise and educate the Chinese authorities about the basic rules of capitalism. In return, Beijing gave them privileged access to the vast Chinese economic basin. These powerful international financiers played an important role in the preparations for the transfer of Hong Kong. (UC)
5. In 1984, the British Government of Margaret Thatcher announced that it would return Hong Kong to China on 1st July 1997. This was not news to the Chinese or the rest of the world since a treaty signed nearly a century before had stipulated that Hong Kong was to revert to China in 1997. The reality of the impending transfer, however, created insecurity that was strengthened by the tragedy of Tiananmen Square in June 1989. That incident made Beijing realize more than ever that it would have to prepare the ground for its arrival not only with regard to the financial community but also the population. In the late 1980s, Western intelligence services reported the very active presence in Hong Kong of the United Front Work Department (UFW).<sup>4</sup> For that purpose, the UFW was given the responsibility among other things for building alliance with the triads already affiliated with many business people. As early as 1992, Western intelligence services knew that, Wong Man Fong, formerly Head of the New China News Agency, was instructed to inform the triads bosses that if they agreed not to jeopardize with the transition process and the normal business in

Hong Kong, Beijing would assure them that they will be allowed to pursue their illegal activities without interference.<sup>5</sup> The Beijing authorities also created a front company in Hong Kong for Wong Man Fong to facilitate his contacts with the triads and so assist triads groups set up legitimate business in China, particularly in Guangzhou and Shanghai.<sup>6</sup> Following these negotiations, Deng Xiaoping himself was speaking of the triads as Chinese "patriotic groups", and the Hong Kong press published a photograph of Charles Heung, a senior officer of the Sun Yee On, conversing with the patriarch's daughter.<sup>7</sup> At the same time, Interior Minister Tao Siji indicated that there were patriotic members among the triads and they were welcome to do business in China. (S)

6. The political class has also been targeted by Beijing's leaders. Without any doubts for the communist masters it was essential to obtain the cooperation of key elements of influential local personalities. Their collaboration or their resistance in China's requests before July 1st was going to make the difference between the possibility to do business with China after the transition. To achieve this, political and business people have been approached and enthusiastic collaborators received positions within various transition committees. For example, in early February 1997, Rita Fan Hsu Lai-Tai was appointed by Beijing, chair of the Hong Kong Special Administrative Region (SAR) Provisional Legislative Council (LEGCO). Mrs. Fan Hus has been identified as a secret cadre of the Chinese Communist Party and an associate of Albert and Sonny Yeung, both officers of the Sun Yee On triad. She is also the daughter of one of the leaders of the Shanghai Triad criminal organization known as the Green Gang before the communist takeover in 1949. This group was known for its political assassinations on behalf of another triad boss, Chiang Kai Shek.<sup>8</sup> (S)

## IMMIGRATION TO CANADA

7. Canada has always been a preferred destination for the people of Hong Kong. It is estimated that 100,000 Canadians live on the peninsula, and most of them are natives of the city. Hong Kong alone has been for the last 10 years the top source of immigration to Canada, with over 500,000 Hong Kong people now living here and accounting for 22 percent of all immigration to Canada. Over half of the 66,000 persons who left Hong Kong in 1996 came to Canada. To that must be added 17,000 students, amounting to a fifth of all foreign students in Canada. (C)

8. Among legitimate immigrants in recent years, some persons affiliated with or members of the Chinese triads have succeeded in slipping in and obtaining Canadian citizenship. Several triad officers<sup>9</sup> and their associates even have family members residing in Canada. Their choice of Canada was no accident. This country is an excellent place to invest in companies to launder the profits derived from criminal activities while securing a portion of their assets outside Hong Kong and obtaining a Canadian passport. Most of these individuals are members or associates of the upper echelons of the triads and own or run large businesses in Hong Kong. As part of their secret agreements reached with the Beijing leadership,<sup>10</sup> these triads now use their Canadian acquisitions to engage in intelligence activities, such as intimidating individuals, identifying potential sources of facilitating visit of Chinese delegations on behalf of China. (S)

9. Two other types of investor represent another danger to the Canadian economy, namely, the rich Hong Kong Chinese business people and leaders of the Chinese civilian and military authorities of China. Like the "entrepreneurs" affiliated with the triads, Chinese investors from Hong Kong or Beijing have taken control of Canadian companies in various sectors of the economy. Some of these businesses have even obtained Canadian government classified contracts. The threat is more significant because the strategic alliance between the Beijing leadership and Hong Kong tycoons is reinforced by the powerful ethnic and cultural ties associated with *guanxi*.<sup>11</sup> This concept rules the links, the obligations or duties and the type of relations between individuals and is a characteristic of the Chinese culture. (S)

10. In all three cases, their commercial activities have enabled them to develop a position in the Canadian economy that affords them the opportunity to engage in intelligence activities, such as illicit transfer of technology, foreign influence and interference, identification and cultivation of persons favourable to China, and the acquisition of undue control in important Canadian economic and political circles. (S)

11. Even before Hong Kong's official return to the Communists, it was established by several Western agencies that their national immigration systems had been affected by illegal ChIS and triad interference. Laurence Leung Ming-Yen, a former director of the Hong Kong immigration service, is still under investigation after he had to resign under the pressure of allegations of corruption and illegally disclosing confidential information about residents of the peninsula. The controversy surrounding Leung was fed by his business relationship with the flamboyant tycoon Tsui Tsin Tong, well known for his pro-Beijing views and a member of the notorious Chinese People's Political Consultative Conference and Preparatory Committee. The murder of Leung's young daughter in Vancouver in 1993 by a crossbow bolt has still not been solved. The Vancouver police suspect the crime was committed by triad members.

12. In 1996, an extensive special investigation within the American immigration service led to the arrest of two former heads of this service stationed in Hong Kong. Jerry Wolf Stuchiner was found in possession of illegal Honduran passports<sup>12</sup> and was recently released after he accepted to collaborate in the trial of James DeBates.<sup>13</sup> James DeBates and his wife Heddy, an American of Chinese origin, were also arrested and questioned regarding their involvement in Stuchiner's activities and the illegal entry of Chinese immigrants into the United States. Canada has unfortunately its share of difficulties. Different cases were investigated and like the case of Robert Geddes, a former citizenship judge, whom was charged in May 1997 with 33 counts of fraud and misrepresentation in 13 known cases involving Hong Kong Chinese.

13. Analysis of the destination of immigrants broken down by Canadian province is an indicator of the concentration of the activities of these groups. Between January 1990 and March 1997, 39.1 percent of the persons registered in the entrepreneur and investor categories chose to settle in British Columbia, particularly in the south Fraser Valley. Ontario for its part received 28.5 per cent of immigrants, who settled mainly in the Toronto area. This pattern is explained by the large, long-established Chinese communities in these areas which are essential in the activities of the triads, Chinese investors and ChIS. Under the same program, 20.6 per cent of such immigrants settled in Quebec while Alberta received only 7.3 per cent. (S)

### HUNDREDS OF CANADIAN COMPANIES "MADE IN CHINA"

14. The influx of Chinese investors who are affiliated with the triads or new associates of Beijing poses a new challenge to Canada's national security. The central point of the strategy of the Chinese is first to buy a Canadian company so as to obtain a "local identity", legally concealing subtly their foreign identity. Then, using this acquisition, the Chinese-Canadian company invests heavily or buys other companies in various economic sectors, but always under the Canadian banner. In actual fact, control lies in Hong Kong or Beijing, and the financial benefits or fruits of research, often paid for by Ottawa or the provinces, are likely to make their way to Asia. (S)

15. Hand in hand with their ethnicity and their commercial ambitions, the financial network of the Chinese entrepreneurs associated to the organized crime and to the power in Beijing has grown exponentially and very rapidly in Canada. Their influence over local, provincial and national political leaders has also increased. In the game of influence, several of these important Chinese entrepreneurs have associated themselves with prestigious and influential Canadian politicians, offering them positions on their boards of directors. Many of those companies are China's national companies.

16. The analysis of the information demonstrates that their attention was not initially directed towards sensitive sectors like high technology or other even more sensitive areas, but towards what might be called "soft" sectors such as: real estate, hotels, transportation, oil companies and travel agencies. Commercial sectors that at first sight do not involve any security risks and did not attract the attention of the Canadian services responsible for security. The scale of their ventures or investments has now made them some of the most important figures present in the major centres, and their decisions to invest in one place or another are not a matter of indifference to anyone. Such projects are seen by the local or national business community as a "favour" or a "chance" not to be missed. (S)

### CASE STUDIES

17. It is estimated at the present time that over 200 Canadian companies are under Chinese control. These business are to be found in myriad sectors of the economy, ranging from multinationals to banking, high technology and real estate. Some typical cases are presented here to illustrate the various scenarios that are clearly worrying for Canadian security. At first site, these individual cases do not seem to be a great threat. It becomes, however more disturbing when the ownership links between various sectors of Canadian enterprises are revealed. (S)

### Multinationals

18. CITIC (Canada) China International Trust Investment & Company (*China International Trust & Investment Corporation*) is the largest Chinese operating internationally. It has subsidiaries operating in several Western countries, including the United States and Canada (Vancouver). Founded at the end of the 1970s, it now has assets worth US\$23 billion. Its subsidiary in Canada CITIC BC Inc., opened it doors in 1986. By 1995, it reported a turnover of CDN\$250 million (1995). The projections for 1996 aimed for \$290 million. (UC)

19. CITIC was initially established to encourage foreign investment in China. It has since taken the lead in Chinese investments outside China, in all areas from real estate to electronics. In 1979 Beijing appointed to CITIC's board of directors three Hong Kong financial giants, Li Ka-Shing, Henry Fok Ying-Tung and Wang Foon-Shing. With their assistance, in the following years, the Beijing acquired important companies such as Cathy Pacific Airlines, Hong Kong Telecom and Star TV. In Canada, it is estimated that CITIC has invested nearly \$500 million to buy up businesses in certain areas, such as Celgar Pulp Mill in British Columbia, Nova Corp Petrochemical in Alberta, real estate through Hang Chong Investments Ltd. and hotels. Eventually, CITIC developed also close business links with Power Corporation. (S)

20. CITIC recently attracted American media attention in the scandal over illegal contributions to the US Democratic Party and influence-peddling by the Chinese government (see section below). CITIC, China Resources and the Lippo Group (in which in both Li Ka-Shing is a large shareholder) are at the centre of the affair. CITIC chairman, Wang Jan, is also chairman of Poly Technology (see next section). CITIC has repeated the gesture by contributing through its Canadian subsidiaries to Canadian Political Parties. (UC)

21. Norinco and Poly Technology (Poly Group). Northern Industrial Corporation (Norinco) and Poly Technologies (a subsidiary of Poly Group) are both owned by China and under the control of CITIC. They have subsidies around the world, including Canada (Montreal) and the United States. Poly Group was until recently head by Deng Xiaoping's son-in-law, He Ping, and is part of the entrepreneurial drive of the People's Liberation Army (PLA). Several large quantities of arms manufactured by Norinco have been confiscated on Indian reserves, especially those of the Mohawks. In May 1996, US authorities what they described as the biggest arms seizure on American soil, confiscating 2,000 AK-47 assault rifles and other military weapons from a warehouse in California. The US-based Chinese representatives of Poly Technologies and Norinco were arrested in connection with this affair. Although the final destination of the arms has not been determined, the Amerindians "Warriors" and American militia trails are strongly suspected by US authorities. (S)

22. In another incident, the Rex International Development company of Hong Kong, in which Norinco is the majority shareholder, is currently under investigation possibly subject to prosecution for exporting components for the manufacturing of chemical weapons to Iran. Rex was established in 1982 as a joint venture with Norinco by Tsui Tsin-Tong, a financial partner of Li Ka-Shing. Tsui filed an application to emigrate to Canada in 1985 which has been renewed several times. His case is still not settled because he has never satisfied the Canadian authorities by providing adequate explanations of his contacts with the PLA and the ChIS. Silver City Development Ltd., which holds shares in Rex, has been used for several years by the ChIS and the Chinese leadership as an investment front and cover. (S)

23. Through the power of its multinationals industries and the billions of dollars they generate, China has been able to establish itself in the Western economy. This gave to the country an enormous advantage in the pursuit of gaining influence. In return



through these subsidies and influences, they are able to open channels to facilitate access to Western power and traffic of illegal weapons and technology. (S)

### **Banks and financial institutions**

24. CIBC and the Hong Kong Bank of Canada. The banking industry is one if not the most important economic leverage in this country. To control or to be able to influence the actions of a bank gives to a single or a group of important shareholders a very influential and privilege position in our society. In this domain, Canada might be in a disadvantage position. Of the G-7 countries, Canada has the fewest banks that is five major institutions including the CIBC which in return creates the highest concentration of assets in the same hands. Banks, as a whole, hold 57 percent of industrial shares, 54 percent of private deposits and 65 per cent of personal credit. Some analysts predict that the Canadian banks will hold 70 percent of the mutual fund market by the year 2000. (UC)

25. Rich investors like Li Ka-Shing and even the Chinese regime itself got interested in the 1980s to invest in banks and Canadian banks too. Li Ka-Shing owns 10 percent of the CIBC, which is the largest single individual share holder. He is also in partnership with the CIBC in many companies like development projects like of the land of Expo 86 in Vancouver (CDA \$3 Billion). This bank seems to be particularly used by Chinese investors. The 1980s saw several bank acquisitions and mergers in this country. The Continental Bank was sold to Lloyds Bank Canada which in turn was bought by the Hong Kong Bank of Canada. The latter is the sixth largest bank in Canada, and the largest foreign one. In 1986, it acquired the Bank of British Columbia. Li Ka-Shing and Stanley Ho<sup>14</sup> are share holders and on the Board of Directors of the Hong Kong Bank in Hong Kong which owns the subsidiary in Canada. The Government of China is also a share holder of that bank. (UC)

26. Wood Gundy, Merrill Lynch and Gordon Capital Corp. Other important financial sector linked to banks is the brokerage house business. In Canada, it is dominated by a few large banks. In 1993, eight of the largest Canadian brokerage institutions were owned by five banks and controlled 70 percent of the securities market. In 1988, CIBC bought 65 percent of the shares of Wood Gundy at a cost of CDA \$190 million, or three times the book value. (UC)

27. In 1990, the CIBC took over Merrill Lynch Canada, one of the eight largest Canadian institutions. Merrill Lynch International is owned by Thomas Fung (see below, China Vision) and Li Ka-Shing business associate. Another prestigious old Canadian firm is Gordon Capital Corp. became 50.1 per cent owned by Richard Li, son of Li Ka-Shing, in October 1995. That is two years after Richard began to work for the firm. After Richard joined the board, William (Ken) Davidson, former vice-president and executive director of the CIBC, received a promotion to the board, and Bob Fung the position of vice-president. His son Mark often travels on Team Canada trips to Asia. Again, it is not only the financial leverage that should be noticed but the gain of influence this sector offers. (S)

### **High technology**

28. Semi-Tech Corporation. Semi-Tech Corporation is a Canadian multinational corporation based in Markham, Ontario. It was formed from various public companies listed on several stock exchanges, including Toronto, Montreal, New York, Tokyo, Osaka, Nagoya, Frankfurt and Hong Kong, and has revenues of over US \$3.5 billion. This corporation, and its chairman James Ting in particular, have business ties with China. Stanley Ho is the principal shareholder through his company Shun Tak (Hong Kong) and sits on Semi-Tech's board. (UC)

29. This company has concentrated in particular on information technology, establishing Semi-Tech Microcomputers Ltd., Semi-Tech MicroElectronics Corp., Semi-Tech Electronics, Singer and STM Systems Corp. The last of these was established by the merger of Data Crown (Canada) and Canada Systems Group, two companies that count various federal government departments among their clients and some of whose employees are regularly in contract with Chinese diplomatic representatives. Of particular note is the fact that Canada Systems Group had applied to undertake the development of COSICS, the Canadian On-line Secure

Information and Communication System that was to link the Department of External Affairs, the RCMP, CSIS and National Defence. The project was suspended by the federal government due to the lack of financial resources. (S)

30. China Huaneng Group, Unipecc Canada and Goldpark China Ltd. On January 1997 Canadian newspapers announced that the Chinese companies China Huaneng Group Group Hong Kong Ltd. (CHG(HK)) and China International United Petroleum and Chemicals Co. (Unipecc) had concluded an agreement whereby Huaneng would buy 70 percent of the shares of Unipecc Canada Ltd. Unipecc Canada Ltd., in turn, holds 57 percent of the shares of Goldpark China Ltd. of Toronto which, holds exclusive world rights for the productions of photographic security systems. CHG(HK) is a subsidiary of the fifteenth largest Chinese State Company, China Huaneng Group. Unipecc for its part is a giant of the Chinese oil industry which has sought in recent years to diversify its activities. It is also famous for the many lawsuits against it and for its illegal transactions involving large arms sales to Iraq for oil. (UC)

### Entertainment and Media

31. It has been known for several years that the Hong Kong triads, particularly Sun Yee On, control the Chinese entertainment industry. In Canada, some promotion companies with affiliations to Chinese organized crime and the ChIS have organized tours for artists from China and Hong Kong. Significant investments have also been made by these groups in the Canadian Chinese-language media, including the Chinese-language television industry which is integrated into the general Canadian television system. (S)

32. Charles Y.M. Kwan Productions. Charles Kwan Yee Man<sup>15</sup> has been active in the Asian live entertainment business industry for years through his companies, including China Cultural Promotions Limited and Charles Y.M. Kwan Promotions Inc. In the course of his business activities Kwan is regularly in contact with prominent members of the Hung Lock and Sun Yee On triads. He also maintains relations with the Chinese Free Masons (CFM) in Toronto which have always been used by the ChIS to identify potential sources and promote Chinese policies. (S)

33. North American Studio (Canada). Although this company closed its doors in 1996, it was well known in police circles for its criminal origins. Also using the names North American (Canada) Motion Picture Corp. and North American (Canada) Television Corp., this company has been under the control of the Sun Yee On triad since its beginning. The firm attracted media attention recently as a result of the legal saga of Miranda Yuen, an employee of North American Studio and the ex-wife of the top boss of the Wo Hop To triad. In the early 1990s, members of the Sun Yee On triad bought a warehouse in Markham, Ontario which was converted at a cost of \$7 million into a film and television production studio. The group has since been the subject of ongoing investigation by police authorities in connection with certain criminal activities. Some of the company's executives were regularly in contact with representatives of the Chinese diplomatic missions in Canada and were regularly involved in Canadian political circles like serving as intermediaries in organizing a dinner between the mayors of Shanghai and Toronto. (S)

34. China Vision and Fairchild Entertainment. China Vision is a pay-TV station in Toronto, established by Francis Cheung in 1981. In 1991 it had about 110,000 Canadian subscribers of Chinese origin in the Toronto, Edmonton, Calgary and Vancouver areas. Pro-democracy groups across Canada submitted briefs to the CRTC alleging that Cheung received financial assistance from the Chinese government, and that China Vision's reports on China were approved and influenced by the government of that country. (UC)

35. In 1992, the CRTC entertained an initial offer of purchase for China Vision. This offer was made by John Sham, a Toronto resident, Hong Kong film promoter and an employee of Television Broadcast Ltd. of Hong Kong. Sham is an associate of Charles Heung, a senior officer of the Sun Yee On triad. The potential buyers of China Vision included John Sham and North American (Canada) Television Production Corporation, which was affiliated with the Sun Yee On triad.<sup>16</sup> This offer was withdrawn following information given to the CRTC by Canadian authorities. (S)

36. In 1993, Thomas Fung of Fairchild Communication Ltd. of Vancouver submitted an offer to purchase China Vision to the CRTC for CDN \$9.25 million. Fairchild Communications Ltd. is 80 per cent owned by Happy Valley Investments Ltd., also of Vancouver, and 20 per cent by Television Broadcasts Ltd. of Hong Kong, the largest global producer of Chinese-language programming. Various Canadian groups of Chinese origin opposed Fairchild's purchase offer because they were concerned that this sale would open the door for the Chinese government to influence Canadian television news broadcasting. They argue the station would be vulnerable to political pressure from the Chinese government, especially after 1997, and because the Hong Kong media often practiced censorship where China was concerned for fear of offending the government of that country. Although the CRTC shared some of the groups' concerns, in October 1993 it approved the purchase of China Vision by Fairchild Communications Ltd, granting it a license for four years. It should also be pointed out that Fung has bought an important amount of shares in Hollinger and Southam, two press giants in Canada. (C)

37. Hong Kong Telecommunications and Wharf Cable Ltd. In March 1997, these two companies formed in consortium with Li Ka-Shing's Hutchinson Whampoa Ltd., Cheng Yu-Tong's New World Development Co. and Heung (Jimmy) Wah-Shing's Win Film Co. Jimmy Heung is known in Hong Kong as a senior officer of the largest triad, Sun Yee On. He is the younger brother of Heung Wah-Yim, the Dragon Head of this group, who was officially identified in 1992 by the US Senate's Standing Committee on Asian Organized Crime. The output of these companies is used by the Canadian Chinese-language media. It should be noted that the company was bought by another Hong Kong company, Fairchild Communications, and CITIC is also the owner of Hong Kong Telecom. The productions of all the above mentioned companies are used by the Canadian Chinese language media. This transactions highlights well the close relationship among Chinese business people, the triads and China's power. (S)

### **Food-Services industry**

38. Tai Foong International. Triad members or their associates are also involved in the food-services industry, witness the example of Tai Foong International of Mississauga, Ontario. The company's chairman and managing director, David Lam, is affiliated with the Kung Lok triad.<sup>17</sup> Tai Foong International sells seafood around the world. The company has offices in Vancouver, Calgary and Montreal with headquarters in Mississauga. It has divisions in the United States, specifically Las Vegas and Seattle, and in Hong Kong. According to our information, Tai Foong International is believed to be involve in importing heroin into Canada from Hong Kong.<sup>18</sup> In addition, various members of the management have for several years maintained regular contacts with Chinese trade and military representatives in Canada, organizing meetings, paid visits of Chinese delegations and so on. Several, including David Lam, have travelled frequently to China on business. (S)

### **Real estate and hotels**

39. Everywhere in the world the core of Chinese economic activity is located in large urban centres. In Canada, the bulk of the country's economy is concentrated around a few large cities only. Real estate has always been a preferred area for the Chinese, and several have built large fortunes from it. In itself real estate is not a obvious threat to the security of Canada but it becomes an excellent vehicle to gain access to local politicians and their influence and power. You own one building is one thing, you own 10 or 30 commercial buildings and your influence is considerable. If you are located in the heart of the business activities, you are the focus of attention. The business of centres of Toronto, Vancouver and in part Montreal are now in large portion owned by Hong Kong or Beijing. (C)

40. Grand Adex Properties Inc. and Concord Pacific Development Corp. Grand Adex is wholly-owned by the Kaumo Hui and Li Ka-Shing families. In 1987, the two tycoons' sons Terry Hui and Victor Li, helped Li Ka-Shing acquire 80 hectares of Expo 1986 land in Vancouver for Concord Pacific. They are now pursuing a residential development mega-project estimated to be worth \$3 billion. In March 1997, Grand Adex and Concord Pacific repeated the same scenario by going into partnership with the Toronto company TrizecHahn Corp (80 percent foreign own), obtaining a \$2 billion project and 18 hectares of prime land west of Skydome in downtown Toronto. They also obtained an exclusive lease on the CN tower for the next 35 years with two possible 15-year

extensions. At 33, Terry Hui, who has now obtained Canadian citizenship, heads up these two companies and is considered the most important property developer in Vancouver. (UC)

41. World Financial Properties. In 1992, when the Reichman brothers' Olympia and York Development company faced a serious financial crisis, the CIBC was the Reichmans' largest Canadian creditor, and the Bank of Hong Kong the largest overall creditor. Li Ka-Shing's Dragon Holdings Ltd. acquired 51 percent of Olympia and York Development's New York office towers for \$20 million, and, in 1996, bought Olympia with the assistance of the Bronfman family, renaming it World Financial Properties. (UC)

42. Ramada Hotels, Harbour Castle (Toronto) and others. Large hotel chains and almost all the prestige hotels in Canadian urban centres are now owned by Chinese private or state interests. This is an easy service sector and is used mainly to generate income while increasing property holdings. Such is the case of the Ramada international chain, owned by Stanley Ho (25 hotels in Canada), the Sutton Place in downtown Toronto, acquired in 1993 for CDA \$29 million and the Meridien Hotel in Vancouver. The Harbour Castle Westin in Toronto was bought by Li Ka-Shing in 1981 at a price of \$93 million and a further \$20 million payment in 1989. Other examples, the Carlton Inn and the Carlton Place in Toronto are owned by CITIC. This, of course, is only a tiny part of what is to be found in Vancouver, Montreal and other Canadian centres. (S)

### Universities and research centers

*Sections 43-45 dealing with the University of Toronto and University of Western Ontario are missing from our copy of the report.*

### Source Notes

- 1 See Appendixes I and II, tables on Immigration from Hong Kong
- 2 See Project Stopover. CID/RCMP.
- 3 In 1996 FORBES magazine estimated the "official" personal fortune of Li Ka-Shing at US\$ 10.5 billion, Henry Fok Ying-Tung at \$2.5 billion and Stanley Ho at \$3.1 billion. (UC)
- 4 The United Front Work Department is one of the five components of the ChIS. See CSIS Report 95-6/33, The Future of Hong Kong: New Dogma, Old Tricks
- 5 In May 1996 the publisher of the Hong Kong tabloid Surprise Weekly, Leung Tin-wai, received two individuals in his office at height of the day. They cut off his arms with a kitchen knife because the newspaper was preparing to publish an article unfavourable to Beijing in relation to Hong Kong's return in July 1997. (UC)
- 6 Wong himself recently confirmed this information in a public conference in Hong Kong after defecting to Western authorities.
- 7 See Project Sunset. CID/RCMP
- 8 See Appendix III, Origin and Description of the Triads.
- 9 See Appendix IV, Profile of Typical Triad Member.
- 10 See CSIS report Report 95-6/06, Organized Crime Links to the Intelligence Services of China and Taiwan.
- 11 See Appendix V, Guanxi or Networking.
- 12 Several thousands of Hondurian passports were reported stolen last year
- 13 Stanley Ho, the Macao casino tycoon, is Honorary Counsel of Honduras in Macao.
- 14 Stanley Ho holds a monopoly on the six casinos on the Island of Macao which alone bring in US\$6 billion a year. (UC)
- 15 See Project Shehang. CID/RCMP
- 16 See Project Shehang. CID/RCMP
- 17 ibid.
- 18 ibid.
- 19

## A. Areas of Special Interest for 1999–2000

### Project Sidewinder

#### Report #125

##### BACKGROUND TO THE COMMITTEE'S REVIEW

In September and October 1999 a series of newspaper articles appeared about a RCMP–CSIS project with the codename “Sidewinder.” According to the reports, Sidewinder was a “top secret government project” launched in 1995 and staffed by a joint team of “civilian and police analysts and investigators” from both CSIS and the RCMP. The overarching theme of the media reports was that the project had been the subject of improper political interference damaging to the national interest.<sup>1</sup>

The principal assertions in the media were:

- that the goal of Sidewinder was to gather and analyze intelligence about efforts by the Chinese Government and Asian criminal gangs to influence Canadian business and politics;
- that the Project was terminated before completion because the Service anticipated political resistance;
- that CSIS improperly destroyed all copies of Sidewinder’s final report, as well as drafts, correspondence and other related documents;
- that ending the joint project in 1997 was premature and subsequently hobbled the government’s ability to deal with emerging threats to the country;
- that the Sidewinder team’s request for additional resources, and its recommendation to CSIS/RCMP management to launch a formal investigation into

the alleged activities were answered by the project being terminated and the team being disbanded;

- that the mismanagement of Project Sidewinder had significantly harmed overall relations between CSIS and the RCMP.

##### SCOPE AND METHODOLOGY OF THE AUDIT

The Committee’s review of Project Sidewinder encompassed all available documentation created or collected by CSIS since the project’s inception; interviews with Service and RCMP officers involved in preparing Sidewinder reports; correspondence with and interviews of outside parties offering information or documentation to the Committee; and an examination of all relevant documents in the Service’s files.

In view of the Committee’s mandate to review the activities of CSIS, our efforts were necessarily focused on the Service’s actions. Nevertheless, the Committee did gain access to some, though not all, Sidewinder-relevant files held by the RCMP, specifically those relating to project administration and report drafting. In addition, we were able to interview RCMP officials.

Of all the Sidewinder documents reviewed, the lion’s share originated from RCMP and not from Service files. In the period following the completion of the first draft report in 1997, the Service had disposed of most of the Sidewinder documentation in its possession. In response to a query from the Committee, the Service said that its action was appropriate and fully in accordance with standing CSIS practice for the disposal of files. This matter is discussed more fully below.

##### THE GENESIS OF SIDEWINDER

Only the second joint project of intelligence analysis ever undertaken by CSIS and the RCMP, the organizations signed a “Joint Analytical Plan” for Sidewinder in March 1996. Making use of public, open-source information, and data already at hand in CSIS and

---

## Main Points

---

- The Committee found no evidence of political interference as alleged. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.
- With respect to the Sidewinder first draft report, we found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.
- The Committee found no evidence of any substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design, and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.
- The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused, or were symptomatic of, difficulties in other areas of the inter-agency relationship.
- The Service disposed of what it regarded as “transitory documents” related to the Sidewinder first draft report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather “misfiled.” However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

---

RCMP files and those of co-operating agencies, the project was to assess the threat to Canadian security from certain foreign interests. Four people were assigned to work on the project; two analysts from each agency. During the course of the project, expected to take several months, the team would produce interim “intelligence briefs” updating the Government and allied agency clients on national and international links, and intelligence trends disclosed during the analytical process.

The final report would include link diagrams, flow charts and personal profiles. The Sidewinder team would also prepare, “as required,” a multi-media

presentation highlighting threats to Canada identified as a result of the project. According to the plan, the principal, or at least initial, clients for the project were to be RCMP and CSIS management, with the Service side of the project being managed by the Requirements, Analysis & Production Branch (RAP). RAP products are typically disseminated to a wider readership within government and, where appropriate, the intelligence services of allied countries. One can assume, therefore, that at least on the CSIS side, products of Sidewinder research were expected to reach a wider readership.

Sidewinder team members began by developing a “collection plan”—which data to collect and how.

Under the plan, information of interest was to be identified by cross-referencing information in RCMP and CSIS computer databases. Team analysts would make use of existing CSIS and RCMP files, and the assistance of two other government departments would be solicited to supplement the information base. Records checks would be run through departmental databases, and domestic law enforcement agencies with expertise in the area would also be consulted.

### **THE ILL-FATED FIRST DRAFT**

According to the plan, the project was to complete its analysis by mid-November 1996. However, the available records appear to bear out what the Service told the Committee, that, irrespective of the plan, "little action was taken beyond the production of an initial draft which proved to be unacceptable." Even in this, there was a delay of some six months.

The RCMP told the Committee that the frequent turnover of CSIS personnel dedicated to the project contributed to the delay. For its part, the Service told us that the staffing changes were the result of internal reorganization, transfers and retirements, all unrelated to Sidewinder itself.

The first draft, completed in May 1997, arrived at two key conclusions: that the potential threats warranted the deployment of additional government resources, and that the authorities (RCMP/CSIS) should take the steps necessary to alert operational managers in the RCMP and CSIS to the need to investigate further.

According to the RCMP, the two agencies were scheduled to examine the paper in a "joint review board" on June 9, 1997. Prior to the joint board, however, the Service convened its own internal review, and then shelved the report because, according to the Director General RAP, its findings were "based on innuendo, and unsupported by facts." The RCMP objected to the circumvention of the joint board review procedure and encouraged the analyst/authors

of the first draft to prepare a facting binder in support of the report's assertions. Work on Project Sidewinder was suspended, while discussions between the Service and the RCMP about its future continued.

### **SIDEWINDER RESUMES, DIFFERENCES EMERGE**

In January 1998, CSIS and the RCMP agreed to resume work on Project Sidewinder and the production of what would become the final report. The only change made in team staffing was to replace the senior Service analyst, which CSIS attributed to the internal RAP branch reorganization. The new CSIS analyst became the principal author of Project Sidewinder's final report, completed a year later.

Having resumed work, the Sidewinder team began producing new report drafts for Service and RCMP managers to consider. Disagreements between the two agencies soon arose. In May 1998, the RCMP Chief Superintendent in charge of the Force's side of the Project wrote to his equivalent at the Service (Director General RAP) about a number of factual errors he saw in the revised draft. He took issue with the draft's "Conclusion" and "Outlook" sections and asked that they be rewritten. It is apparent from the correspondence that the revised draft had taken a noticeably different tack from that of the contentious first draft.

In September 1998, a CSIS Sidewinder analyst wrote to his RCMP counterpart in the Criminal Analysis Branch requesting additional supporting information. The RCMP's Officer in Charge (OIC) responded to the request by writing to CSIS (Director General RAP) that the RCMP would provide no further information: "It is our opinion that we have provided sufficient background information in support of the materials provided by the RCMP."

In December 1998, the Deputy Director General RAP wrote the RCMP OIC pointing to innuendo in

the then-current report draft and asking that it be removed. She wrote: "We do not have factual evidence of our suspicions and the Service is uncomfortable with the obvious challenges that could be raised by the readership." She added that in her view both agencies had to concur with the inclusion of items in the joint paper, and "regrettably we [CSIS] cannot in this case."

#### **SIDEWINDER FINAL REPORT**

In January 1999, the Sidewinder final report was completed, which both agencies approved for distribution. CSIS informed us that the RCMP officially accepted the revised report and a copy of it bears the note "Good Report" penned by the responsible RCMP Chief Superintendent. In response to Committee queries, however, that official wrote that the Force

With respect to allegations of political interference in the course of Project Sidewinder, the Committee could find no evidence

was "not fully satisfied with the final report" because unlike the first draft it "fails to raise key strategic questions and to outline some of the more interesting avenues for research."

The Committee has read both Sidewinder versions and the differences between the two are considerable—the quality and depth of analysis in the final version is far higher than in the draft. Clearly a great deal went on between completing the first draft and releasing the final report many months later.

The essential issues for the Committee, therefore, were whether the Service's actions were appropriate during this time, in line with policy and Ministerial Direction and within the law; and whether the

Government, Parliament and the people of Canada were properly served by the advice they received from the agency responsible for assessing threats to Canada and Canadians.

### **FINDINGS OF THE COMMITTEE**

#### **Was There Political Interference?**

A media report early in the public discussion of Sidewinder asserted that the project was shut down in mid-stream because CSIS anticipated political resistance. Immediately obvious to the Committee was that the first claim, that Sidewinder was terminated, was simply wrong. Work on Project Sidewinder was suspended temporarily in June 1997 and restarted in early 1998.

The Committee could find no evidence of political interference as alleged. None of the documents or records we reviewed or received evidenced such interference, actual or potential. None of the CSIS and RCMP employees we interviewed had knowledge of political interference or interference by other agencies in Sidewinder or in other related investigations. None of the other parties who came forward to contribute to our review had knowledge of interference or offered substantiating information of any kind.

#### **Was the Service Right to Shelve the First Draft Report?**

The Committee studied the first draft report and found it to be deeply flawed and unpersuasive in almost all respects. Whole sections employ leaps of logic and non-sequiturs to the point of incoherence; the paper is rich with the language of scare-mongering and conspiracy theory. Exemplifying the report's general lack of rigour are gross syntactical, grammatical and spelling errors too numerous to count.

It is apparent to the Committee that, at its core, the Sidewinder first draft lacked essential definitional



clarity: if one purports to examine the extent of illegal and threat-based activities allegedly taking place alongside entirely legal and benign ones, it is vital to be able to tell the difference between the two. Sidewinder's first draft drew no such distinctions, providing instead a loose, disordered compendium of "facts" connected by insinuations and unfounded assertions.

The Committee believes that the Service correctly assessed the first draft and took appropriate actions to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality. The Committee believes further that both actions were consistent with the Service's responsibility to assess threats to Canada and Canadians rigorously and in a professional manner and provide objective advice to Government based on those assessments. As it stood in May 1997, Project Sidewinder's first draft report failed to meet those standards.

### **Did Sidewinder Harm the CSIS-RCMP Co-operative Relationship?**

That the CSIS-RCMP relationship continues to be productive and fruitful is vital to the safety and security of Canadians, and monitoring the quality of the Service's co-operative arrangements with the RCMP is of on-going concern to the Committee.<sup>2</sup> Although the Committee's review of Project Sidewinder revealed significant differences of opinion and institutional perspective between the Service and the RCMP over the project, we saw no evidence that the difficulties encountered here were symptomatic of a more widespread problem. Nevertheless, the Committee did attempt to identify the sources of friction and obtain each agency's views of the most significant problems.

The difficulties began after the joint analytic team completed the Sidewinder first draft report. Simply put, RCMP management believed the first draft was good work that went some way to proving the initial thesis, whereas the management of CSIS thought the report's findings were based on innuendo and were

not supported by the facts. The Service insisted on a radical rewrite.

CSIS managers told the Committee that among other things, difficulties arose from the inability of the team of analysts to take criticism well, from the fact that the report offered broad recommendations for action when RAP reports typically stopped at analysis and because the report's recommendations were an attempt by some in the RCMP to obtain more resources.

The RCMP's diagnosis was quite different. In interviews and correspondence with the Committee, RCMP management responsible for the project expressed frustration with the Service's approach to the approval mechanism for the joint report which both organizations had agreed to at the outset of Sidewinder. They said that their own analytical reports often came with recommendations and that it was evident that a difference of opinion existed on what constituted good strategic analysis. Finally, the RCMP expressed the view that Service management seemed prepared to ignore the results of a full and impartial joint review.

As noted above, the Committee believes that Project Sidewinder has inflicted no lasting damage to the broader CSIS-RCMP relationship.

### **Did Shelving Sidewinder's First Draft Imperil Canada's National Security?**

Some media reports about Sidewinder in late 1999 portrayed the rejection of the Sidewinder first draft report and its subsequent revision as having blinded the Government to certain emerging threats, such as the abuse of the immigration process. The Committee found no evidence of any kind that such was the case.

Although the delivery of the Sidewinder final report effectively marked an end to the joint effort, both CSIS and the RCMP have continued, separately, to explore and analyze the potential threats to Canada.

### Is There a Substantial Threat to Canada That Has Been Ignored?

The *CSIS Act* sets out the threats to national security the Service is responsible for looking into. Measured against these definitions, the Committee's review revealed no "smoking guns," no evidence of substantial and immediate threat, and no evidence that a threat was being ignored through negligence or design.

### Did CSIS dispose of documents improperly?

At the outset of our review, the Committee was informed that CSIS had disposed of almost all documents<sup>3</sup> related to producing the first draft of the Sidewinder report (documents pertaining to the final report had been retained and were reviewed.)<sup>4</sup> The question for the Committee was whether these actions were appropriate and carried out in accordance with policy and law.

The Service's document control procedures lack rigour and its reviews have not been as effective as the Service and we would have wished

In response to Committee inquiries, the Service stated that the disposal of working documents was standard practice for all analytical reports prepared by RAP (the anchor for the CSIS end of the joint project) and was fully in accordance with Government policy. The essence of the Service's case was that the documents disposed of fell into the category of "temporary or transitory records," used in preparing an analytical collaboration, and as such were not retained beyond their need in accordance with National Archives of Canada policy.

Subsequently, however, the Committee determined that some documents the Service was not able to provide to the Committee were not transitory in nature—specifically, inter-agency correspondence concerning the drafts, as well as the signed agreement between the RCMP and the Service setting out terms of reference for the original joint Project.<sup>5</sup>

When the Committee made the National Archivist aware of these particulars, he wrote to us that the Service had already responded satisfactorily to his own inquiries. When we brought the matter to the attention of the Service, it stated that those particular missing documents had not been disposed of like the others, rather they had been "misfiled" and so could not be located.

Because almost none of the Sidewinder first draft documents were to be found at the Service, the Committee is not in a position to render a judgement on the appropriateness of the original disposal. Some were legitimately disposed of and the balance were lost—but we are unable to determine with any certainty which was which.

The Committee finds the evident confusion over the documents' whereabouts disconcerting. The essential trade of security intelligence is meticulous document control and information management. We reiterate our comments made in the "Lost Documents" study (*see* page 9) that the Service's document control procedures lack rigour and its reviews of its practices in this area have not been as effective as the Service and we would have wished.

Notwithstanding our concerns over the Service's handling of some of the Sidewinder documents, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder. In any case, the Committee found no evidence that raw information, kept in Service files and used by the

Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

### **MAIN POINTS AND CONCLUSIONS**

With respect to allegations of political interference in the course of Project Sidewinder, the Committee could find no evidence. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.

With respect to the Sidewinder first draft report, the Committee found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.

The Committee found no evidence of substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design, and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.

The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused difficulties in other parts of the inter-agency relationship.

The Service disposed of what it regarded as "transitory documents" related to the first draft Sidewinder report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather "mis-

filed." However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

In conclusion, the Committee considers the vital lesson of Project Sidewinder to be this: It is the Service's responsibility to assess threats to Canada and Canadians rigorously, and in a professional manner, and provide objective advice to Government based on those assessments. The Committee is fully in accord with initiatives to bring the respective skills of CSIS and the RCMP together on appropriate projects. At the same time, the Service also has responsibility to ensure that this advice is of the highest possible quality. The Sidewinder first draft report did not meet that standard, and renewed efforts succeeded in producing a much-improved final product.

## **Lost Documents—A Serious Breach of Security**

---

### **Report #126**

---

#### **BACKGROUND TO THE INCIDENT**

On October 10, 1999, the vehicle of a CSIS Headquarters employee was vandalized in the Greater Toronto area. Inside the vehicle were a number of CSIS documents, several of which were classified. These were among the items stolen. The police were notified when the break-in was discovered, and the employee later reported the theft to a supervisor at the Service.

The police investigation revealed that the theft had been committed by petty thieves intent on supporting a drug habit, and that in all likelihood they had discarded the classified documents unread in a garbage dumpster, which was subsequently emptied at a landfill site. The documents were not recovered.

Following an investigation by the Service's Internal Security Branch—standard procedure in such cases—the employee was dismissed from the Service and more minor administrative actions were taken against other Service officers tangentially involved in the incident. In addition, the Service altered some of its procedures for document control and strengthened its internal “security awareness” program.

The Committee's review encompassed all elements of the incident: the circumstances that led to the Internal Security investigation, the manner in which the investigation was carried out, the results it yielded and all factors that would aid in assessing whether the incident pointed to systemic security problems within the Service.

## **FINDINGS OF THE COMMITTEE**

### **Was There Warning of the Employee's Inappropriate Behaviour?**

Our review of the Service's security records showed no previous security violations by the employee beyond those of a minor nature. Nothing in CSIS files presaged the employee's behaviour and the serious security breach that ensued.

### **Potential Damage to the Service and to the Security of Canada**

With a view to assessing the potential damage to national security should the classified documents be found and released, the Committee examined copies of the lost material. The Service's own damage assessment concluded that although some of the information in the reports was dated, or had already become public knowledge, the potential for damage was high. The information contained would have revealed the existence of certain CSIS investigations and, more critically in the Service's view, the nature of CSIS operational limitations. The Service's assessment noted two important factors serving to moderate the potential damage: no sources were identified nor were any operations compromised.

Based on our review of the documents, we concurred with the Service's view: the documents held the potential to expose the country unnecessarily to security threats.

### **Problematic document management**

In the course of its investigation, Internal Security had considerable difficulty determining the precise content of one item, and thus had to make an educated guess at what the employee held at the time of the burglary. This apparent lapse helped nudge the Committee toward the conclusion that there may have been a problem in CSIS internal document control procedures generally. The Service's explanation for the gap in information was that at the time the document was removed from CSIS premises by the employee, it had not been entered into the corporate file system.

Although not directly related to this security breach, a second document control issue emerged subsequent to the incident. The Committee learned about a case of unauthorized possession of documents. After seeking explanations from two operational branches about their respective control procedures, the Service investigation concluded that the case was an isolated one and that no changes in procedure were required.

To prevent either problem from recurring, the Service has reiterated to its personnel the importance of following proper document control and authorization procedures.

### **Other Issues Raised by the “Lost Documents” Affair**

As noted earlier, several other employees were involved—albeit peripherally—in the incident. Although the Service's internal investigation showed that most media allegations of procedural non-compliance were unfounded, in the Committee's opinion the incident highlighted a lack of rigour in the Service's control over the removal from its premises of documents by officers. The Service has since taken steps to address these gaps.

### **Policies and the Human Factor**

It is evident to the Committee that institutional scrutiny of the incident by us and the Office of the Inspector General, intense media interest, and the Service's own inquiries drew unprecedented attention to the Service's internal security mechanisms. As a result, changes have been made. Nevertheless, it is CSIS' view—and we agree—that no amount of regulation or policy can rule out the possibility of such incidents occurring. Intelligent intelligence work ultimately depends on conscientious people, as well as on strict rules.

### **“LOST DOCUMENTS” MATTER IN PERSPECTIVE**

#### **Previous Internal Security Cases**

As part of the Committee's review, we asked CSIS for information about previous internal security investigations and outcomes. Our analysis took into consideration the sea change in national and international security environments in the last fifteen years, and concomitant adjustments in CSIS policies and practices particularly in reporting security breaches.

Although we were unable to identify any single case identical to this most recent one, we did note that a wide range of penalties had been imposed on offending employees—including termination of employment—in cases that shared some of the same elements.

The Committee's review of security breach historical records gave rise to two observations. First, that changes to CSIS internal security policy and practices were often driven by security breach incidents, not considered analysis and review of procedures. The Service's approach to internal security was essentially reactive, notwithstanding internal and central Government agency policies that mandate periodic reviews.

Second, several of the cases in the Service's records have caused the Committee to consider new audit

and review procedures so as to ensure that Members have as complete an understanding as possible of such events, as and when they occur.

#### **The Service's handling of the investigation**

The Service's own “lost documents” investigation was conducted in a competent and professional manner, ultimately revealing how its classified materials went astray. Internal Security Branch staff maintained a focused and coordinated approach to handling the many issues and questions raised by the incident. CSIS Headquarters gave clear direction to Toronto Region which, in turn, successfully enlisted the very important co-operation of local law enforcement

No amount of regulation or policy can rule out the possibility of such incidents . . . intelligence work depends on conscientious people, as well as on strict rules

agencies—co-operation crucial to learning the probable fate of the documents. Finally, the policies and guidelines in place for performing and consolidating damage assessments by various operational branches proved effective.

#### **CONCLUSION**

As already noted, the Service's internal security policy framework has been in place for a number of years, with change usually stimulated by a security intelligence breach at home (“lost documents”) or abroad—the Aldrich Ames CIA case being one of the more notorious examples.

Although this most recent incident cannot be traced to faulty internal security policies, it has served to highlight a lack of rigour in certain of the Service's

procedures for implementing those policies. We are aware that the Service periodically conducts its own internal review of security procedures. Nevertheless, security breaches in recent years involving CSIS materials (and commented upon in these pages) suggests that these internal reviews have not been as effective as the Service and the Committee would have wished. The Committee will continue to monitor this area of Service operations closely.

## Threats from a Foreign Conflict

### Report #124

#### BACKGROUND TO THE STUDY

The focus of this study is a CSIS investigation of possible threats emanating from a conflict abroad. Canada is susceptible to the spillover from foreign wars and civil strife for a number of reasons: its open society and relatively porous borders, its activist international policies and robust defence alliances, and the presence in Canada of various "homeland" communities. It is in the nature of homeland conflicts that attempts are sometimes made by one or other of the warring parties to enlist the support (moral, political and financial) of compatriots in Canada.

In this instance, the perceived threat arose chiefly from the activities of foreign intelligence services operating in Canada. These included suspected attempts to raise funds, collect information on homeland communities, foment civil unrest in Canada, and illegally procure weapons and technology.

As with every review of a homeland conflict investigation, the Committee directs special attention to gauging the impact of the Service's investigation on the homeland communities themselves. Whenever the Service targets domestic groups or conducts interviews within homeland communities, we wish to ensure that it acted appropriately and entirely within the law.

The audit covers the two-year period from April 1997 through March 1999. The Committee examined all the information generated and retained by the investigation, the targeting authorities requested and warrant powers obtained, and the use made by the Service of information from human sources including its community interviews.

#### FINDINGS OF THE COMMITTEE

The Committee determined that the Service had sufficient grounds to conduct the investigation and to employ the investigative methods permitted in the targeting authorities and Court warrants. The level of investigation was proportionate to the seriousness of the threat and, with one exception, only information strictly necessary to the investigation was collected.

Three issues drew the Committee's attention:

- an overly general targeting authority;
- community interviews;
- retention of unnecessary information.

#### An Overly General Targeting Authority

The Service obtained two authorizations, and it was the second and most intrusive that raised some concerns. It set out to investigate the activities of foreign intelligence services, which could lead to the targeting of foreign diplomats and an individual resident in Canada thought to be associated with those agents. The intent was to learn the extent to which the intelligence officers or their associates were engaged in clandestine or illegal activities that constituted a threat to Canada.

Although the targeting authority in question stated that the investigation was required in order to assess three categories of threat—espionage, foreign influenced activities and politically motivated violence (subsections 2(a), (b) and (c) of the *Act*, respectively)—with one of the targets named in the Request for Targeting Authority (RTA), only one of the threat categories cited could reasonably be said to apply.

Current Ministerial Direction is careful to set various thresholds and standards that must be met for each type of threat. In the view of the Committee, all RTAs should specify how the threats any particular target is alleged to represent conform to these criteria.

**The Committee recommends that RTAs be structured and written to identify clearly the reasons for targeting each target named, under each threat definition cited.**

### **Community Interviews**

In general, the Service's contacts with individuals of homeland communities were conducted appropriately. The Committee did identify one instance where a CSIS investigator appeared to counsel an individual about whether to organize or participate in public demonstrations. Nothing we learned about the matter led us to doubt the officer's good intentions, however, we urged CSIS to remind officers that their task is to gather information, not to offer political direction.

### **Retention of Unnecessary Information**

The Committee's review of CSIS databases identified only one instance where the "strictly necessary" test for collecting information was not met. The information was clearly of a personal nature and had no investigative value. We strongly advised the Service of our concerns. The Service has agreed with this finding and ordered the information deleted from its database.

## **Terrorist Fundraising**

### **Report #122**

#### **BACKGROUND**

Beginning with the Halifax G8 Summit in 1995, the international community has paid increasing attention to the issues of illicit transborder fundraising in support of terrorism. In 1996, the G8 nations adopted a series of measures designed to curb the improper use of "organizations, groups or associations,

including those with charitable, social, or cultural goals, by terrorists using them as a cover for their own activities."<sup>6</sup> With the same goal in mind, the United Nations is expected in 2000 to adopt the International Convention on the Suppression of the Financing of Terrorism.

Relative prosperity, openness and diversity make Canada an ideal place for organizations devoted to using terrorism to achieve political ends to obtain needed funds through illicit means. Although a number

---

## **Management of Targeting**

---

### ***Target Approval and Review Committee***

CSIS' capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

### ***Levels of Investigation***

There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

### ***Issue-Related Targeting***

An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada and that are related to, or emanate from, that specific issue.

---

of countries, including the United States and United Kingdom, have implemented legislation proscribing known terrorist organizations and criminalizing all of their fundraising activities, Canada, for various reasons, has refrained from taking a similar step.<sup>7</sup>

The Government's efforts to deal with this growing international problem have focused on more effective exchanges of information among Canadian agencies, and more stringent enforcement of existing laws and regulations. At the centre of the Government's new initiative was the creation in 1996 of the *Interdepartmental Working Group on Countering Terrorist-Support Activities* (IWG). This body brings the regulatory, investigative and information collection skills of the RCMP, Citizenship and Immigration Canada, the departments of Foreign Affairs, Transport, Justice, Finance, and National Defence—as well as CSIS—to bear on the problem of terrorist fundraising.

The Service plays an advisory role to the Government through the mechanism of the IWG, and provides information about alleged terrorist fundraising in Canada directly to the relevant federal departments. The purpose of the Committee's study was to examine several facets of the Service's work in addressing the problems of terrorist fundraising in Canada.

#### **METHODOLOGY OF THE AUDIT**

The Committee's audit encompassed three types of source data:

- all relevant files documenting communications and exchanges of information between CSIS and the Government of Canada for the period from March 1, 1995 through March 31, 1999;
- interviews with relevant CSIS officers and their interlocutors in various departments of government;
- a selected sample of relevant Service investigations were subject to a thorough review, including all

relevant targeting documents, operational files, warrant files and information received from foreign agencies.

Our goals were twofold: to determine the effectiveness of Service advice and co-operation in assisting the Government's efforts to curb terrorist fundraising, and to ensure that all CSIS actions were appropriate and in conformity with the law.

#### **FINDINGS OF THE COMMITTEE**

##### **Service Investigations of Terrorist Fundraising**

The Service stated that, as a result of its investigations linked to international terrorism, it had uncovered several Canadian organizations suspected of facilitating terrorist fundraising objectives. Our own review of these investigations showed that CSIS did have sufficient information to believe that the links to international terrorist groups and to their fundraising efforts constituted a threat to the security of Canada.

##### **Information-sharing**

Information-sharing between CSIS and client departments has been ongoing for some time, although the Committee noted that a hiatus in relations with one department lasted several months. The lines of communication with that department have remained open ever since. CSIS and its departmental clients both expressed satisfaction with the liaison relationship. Recipients of Service reports said that the information had been most useful as "investigative leads" assisting in determining how and where to follow up.

The Committee's review of the information-sharing process identified a number of difficulties and potential obstacles:

- the use of CSIS information in court proceedings;
- the nature of the advice to government.



### **The Use of CSIS Information in Court Proceedings**

In providing information to client departments, the Service has experienced problems handling information of potential evidentiary value similar to those the Committee has encountered in other CSIS liaison relationships.<sup>8</sup> Current Canadian law makes it difficult to protect classified intelligence from disclosure in legal proceedings where the information is used to support prosecution. CSIS is concerned to protect domestic and international sources and, in the absence of modifications to current law, client departments' ability to use the Service's information in court will continue to be constrained.

### **The Nature of the Advice to Government**

After examining CSIS files, the Committee noted that the Service was selective in the information it gave to the client departments. In response to a query from the Committee, the Service stated that it refrained from distributing information that could adversely impact the security of human sources, Service operations or relations with third parties, for example allied intelligence agencies.

### **RECOMMENDATIONS**

Two recommendations emerged from this study. First, in respect of the nature of the Service's advice,

**The Committee recommends that in future, CSIS advise its client departments of substantive changes to the assessments it has previously given them, which arise as a consequence of new information.**

Second, although the Committee supports legislative changes that would allow more effective use to be made of the information shared between CSIS and its client departments, such enhanced procedures could well generate an increase in the number of complaints brought to the Committee. To address such an eventuality,

### **Lawful Advocacy, Protest, Dissent and Sensitive Institutions**

Sensitive operations invariably involve the use and direction of human sources, and, while human sources can be the most cost-efficient form of intelligence collection, their use also entails the greatest risk in terms of impact on social institutions, legitimate dissent and individual privacy.

The *CSIS Act* specifically prohibits the Service from investigating "lawful advocacy, protest or dissent" unless carried on in conjunction with threats to the security of Canada as defined in the *Act*. The Service is obligated to weigh with care the requirement for an investigation against its possible impact on the civil liberties of persons and sensitive institutions in Canada, including trade unions, the media, religious institutions and university campuses.

**The Committee recommends that the Ministry of the Solicitor General and Privy Council Office initiate special measures to keep SIRC apprised, on a timely basis and as appropriate, of the IWG's proposals as they impact on CSIS activities.**

The Committee will continue to monitor the Service's role in providing advice to the Government of Canada about this growing threat to Canada's security and Canadian interests.

### **Investigation of a Domestic Threat**

#### **Report #121**

#### **METHODOLOGY OF THE AUDIT**

During a previous review, the Committee learned of several CSIS source operations that sometimes involved the legitimate dissent milieu—specifically,

---

## CSIS Role in Preventing Politically Motivated Violence

---

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada," which it is specifically charged to investigate, include "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state . . ." [section 2(c), *CSIS Act*]

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in denying citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

---

certain protests and demonstrations. We subsequently conducted a review of the investigations.

Under the terms of the authorizations for the investigations, several individuals were targeted under sections 2(c) and 12 of the *CSIS Act* wherein the Service has the responsibility to investigate threat activities "directed to or in support of the threat or use of acts of serious violence against persons or property for the objective of achieving a political objective within Canada or a foreign state . . ."

During its investigation, CSIS collected information about the targets, as well as some information about protests and demonstrations in which the targets were

involved. Information the Service obtained was used in threat assessments given to federal government clients and relevant law enforcement agencies.

During the Committee's review of the investigation—and with particular reference to CSIS policy and Ministerial Direction concerning legitimate advocacy, protest and dissent—the Committee examined all reporting by CSIS sources, all information retained on targets and protests and other incidental intelligence collected. We reviewed all relevant targeting authorities, source handling files and Service internal memoranda. In addition, the Committee interviewed CSIS personnel responsible for the investigations.

### FINDINGS OF THE COMMITTEE

The Committee's review identified no violations of Service policy or Ministerial Direction. CSIS had reasonable grounds to suspect that the targets were threats to the security of Canada. None of the human sources engaged in illegal or *agent provocateur* activities, and the sources gathered information on appropriately approved targets. We saw no instances of influence by CSIS sources on the activities of legitimate groups or organizations.

Notwithstanding our general conclusions, this set of investigations was the source of some residual concerns for the Committee. During the course of investigations, which lasted several years, the Service made targeting decisions, chose investigative methods, collected information and advised government clients—all actions carried out in accordance with policy as written—which when reviewed as a whole left the Committee uneasy. Among these were:

- existing policies for managing human source investigative techniques did not ensure that executive management was fully seized with the fact that, because of unforeseen activities of the authorized targets after the original TARC approval, an organization not itself an authorized

target had become implicated in the Service's investigative activities;

- CSIS instructions that sources were only to report on "authorized subjects of investigation" was not fully implemented in practice in some instances;
- in two instances while conducting surveillance of authorized targets, the Service inadvertently collected some information on the activities of an organization. The Service did not retain the information in its active database;
- one threat assessment issued by the Service based on information gathered during these investigations did not, in the Committee's view, accord with the intent of the *Act*.

The Committee believes that these instances—admittedly few in number—point to an occasional lack of rigour in the Service's application of existing policies, which oblige it to weigh the requirement to protect civil liberties against the need to investigate potential threats. We brought these particular instances, and the Committee's overall concern about the need for rigorous weighing, to the attention of the Service.

In the Service's view, its existing policies, including the need for multiple levels of approval, adequately address the Committee's concerns. It believes it is in full compliance with Ministerial Direction which requires it to choose investigative methods and techniques proportionate to the threat, and to ensure that these are weighed against possible damage to civil liberties. The Service stated that "... the position that the [*CSIS*] *Act*, in combination with Ministerial Direction, requires evidence of 'weighing' in every single case before a targeting approval is given, is a distortion of both the *Act*, and of Ministerial Direction."

The Committee is in no doubt that, in all of its investigative activities, the Service takes the matter of civil

liberties extremely seriously. However, with respect to its position on the need for evidence of weighing in "every single case," we disagree.

It is an essential principle of administrative accountability that the processes by which judgements and decisions are made can be as important as the decisions and outcomes themselves. The Committee would like to see tangible evidence that significant investigatory decisions involving the legitimate dissent milieu are adequately weighed.

**The Committee recommends that the Service make the changes to its administrative procedures necessary to ensure that all significant investigatory decisions in the area of lawful advocacy, protest and dissent are weighed and so documented.**

The Committee believes that as well as providing an additional measure of comfort to the Review Committee, such changes would help maintain the day-to-day sensitivity of all CSIS staff to the need to protect civil liberties.

The Committee had an additional recommendation concerning the need to clarify a section of the CSIS *Operational Policy Manual* (a classified document).

## **A Long-Running Counter Intelligence Investigation**

---

### **Report #118**

---

#### **BACKGROUND TO THE REVIEW**

The Review Committee believes that an essential aid to ensuring the continued quality and appropriateness of CSIS activities is the periodic review of major investigations that span a number of years. We last reported on this counter intelligence operation some time ago.

### AUDIT METHODOLOGY

The Committee's inquiries and research were designed to answer certain key questions about the investigation:

- Did a threat (as defined in the *CSIS Act*) in fact exist?
- Was the nature of the Service's investigation (the level of intrusiveness, the quantity of resources deployed) proportionate to the threat?
- Were CSIS actions appropriate, in compliance with Ministerial Direction and internal policy and within the law?
- Was the advice given to the Government based on the investigation timely, balanced and accurate?

Our audit encompassed CSIS operational files for a selected set of investigations, documents supporting targeting requests and warrant applications, Service reports generated for clients throughout the Government and interviews with CSIS officers and with consumers of Service intelligence products in other departments of Government.

In addition to reviewing specific Service activities, the Committee took into account such factors as the

---

### CSIS and the Use of Surveillance

---

CSIS uses surveillance to learn about the behaviour patterns, associations, movements and "trade-craft" of groups or persons targeted for investigation. As an investigative tool, surveillance is used to detect espionage, terrorism or other threats to national security. Large amounts of personal information can be collected and retained in the course of surveillance operations. The Service's surveillance units use various techniques to gather information. In an emergency, surveillance can be used before a targeting authority has been obtained.

---

number of known and suspected intelligence officers in Canada, and less tangible factors such as the potential damage to Canadian interests should allied governments come to believe that Canada's counter intelligence efforts were inadequate or ineffective.

### FINDINGS OF THE COMMITTEE

#### The Nature of the Threat

It is the Service's view that the target of this investigation is engaged in intelligence-related activities that manifest themselves in classical espionage, foreign influence in various aspects of Canadian society and the theft of economic and scientific information through clandestine means.

In an earlier report the Committee stated that "the threats posed by the intelligence gathering activities of this [target] [were] at th[e] time, nebulous, and sometimes hard to define." Although events since then have served to confirm that the potential for serious threat to Canadian interests is serious and genuine, the current threat as measured in concrete and confirmed activity appears to us to be limited and infrequent.

This difference of opinion between CSIS and the Committee about the nature of the threat led us to conclusions about some of the target's activities that were at odds with those of the Service. Some of the activities investigated by the Service showed the target engaged in intelligence gathering in Canada, but others did not.

In one case the Service treated as a threat activity—an attempt to influence a Canadian official—what seemed to be routine diplomatic behaviour. In another, with little corroborating information, CSIS ascribed intelligence gathering motives to apparently normal consular contacts.

The Committee's review also raised questions about some beliefs the Service has about the nature of the

threat. We are of the opinion that these beliefs are sometimes overdrawn.

### Targeting Decisions

The Review Committee thoroughly examined a representative selection of Service targets approved for investigation by the CSIS Targeting and Review Committee. We reviewed the case the Service set out for each and studied warrant affidavits, supporting documentation and reports generated by the investigations.

The Committee believes each of the targeting decisions examined was justified by the evidence. However, in the Service's application to secure warrant powers against one target were a number of overstatements. In one instance, information put forward was more than a decade old and the information adduced was derived from one source's "feelings." In another, a source's speculation was quoted. Some assertions that the target engaged in "suspicious activities" appeared to us to be misleading or exaggerated. Despite these imprecisions, however, the Committee believes the evidence to proceed with targeting the individual was convincing overall.

### Investigative Activities and Retention of Information

The Committee identified several instances in which the Service acted in contravention of policy or without due caution:

- some information collected by the Service did not meet the "strictly necessary" test: a membership list, reports about a public meeting and particulars about individuals who were neither targets themselves nor known to have contacts with targets;
- Service actions in regard to one target appeared to carry significant risk;
- CSIS files about one aspect of an investigation appeared to show that a source rendered assistance

to a target in a manner that gave rise to the Committee's concern.

### Employment of Resources

The Committee was at pains to assure itself that the resources devoted by the Service to this investigation were appropriate to the threat. While our review turned up no acute difficulties, we will continue to monitor the Service's deployment of resources in this area.

### Advice to Government

The Service produces several classified publications to transmit its findings to various readerships in the Government of Canada. The Committee examined a selection of CSIS publications relating to this particular investigation, compared the statements in them to supporting information in Service files, and asked clients their views of the utility and accuracy of Service reports.

None of the clients we interviewed took issue with the accuracy, timeliness or analytical quality of the reports they received. Most considered the Service's reports to be useful background information. The Committee's review of the information in support of Service conclusions in selected CSIS reports did, however, reveal some anomalies:

- the Service stated that an action by a target was possibly for the purpose of "developing a network of agents." Our review showed that there was no documentation on file to support this premise;
- a report stating that a target had used a certain business practice to obtain proprietary advanced technology was not technically correct. In our view, the Service's information differed from the report's description;
- CSIS informed its readers that a target had engaged in a number of instances of "espionage" over a long period. In examining these instances, the Committee formed the opinion that the

evidence for some was weak, speculative or ignored reasonable, benign alternative explanations for the actions in question.

### CONCLUSION

The Committee believes that the potential threat to Canadians and Canadian interests arising from the activities of this target is significant. It is vital, therefore, that the Service take special care to ensure that the analysis and reporting generated by its investigations remain precise and unbiased. The Government of Canada faces a myriad of difficult international security, economic and diplomatic issues. It deserves the best possible national security advice—clear in analysis, as transparently obtained as law and prudence permit

The Government deserves the best possible national security advice . . . as transparently obtained as law and prudence permit and unencumbered by unfounded speculation

and unencumbered by preconceptions or unfounded speculation. Our review evidenced a few instances that pointed to the Service occasionally drawing conclusions not based on the facts at hand.

## Domestic Exchanges of Information (4)

### Report #119

In carrying out its mandate to investigate suspected threats to the security of Canada, CSIS co-operates and exchanges information with federal and provincial departments and agencies and police forces across Canada. The Service's mandate to enter into such arrangements is set out in section 17 of the *CSIS Act*.

The Service discloses information to various domestic departments and agencies "for the purposes of the performance of its duties and functions" under section 19(2) of the *Act*.

Under section 38(a)(iii) of the *Act*, the Committee is charged with the task of examining the co-operation arrangements the Service has with domestic agencies, as well as the information and intelligence it discloses under those arrangements.

### METHODOLOGY OF THE EVALUATION

This review focused on CSIS' domestic exchanges of information for calendar year 1998. In addition to reviewing the Service's information exchanges in all regions, the Committee also conducted an on-site review of one regional office.

The purpose of the review was to assess whether CSIS had adhered to its arrangements with the other agencies, and whether it had collected and disclosed information in compliance with the *CSIS Act*, Ministerial Direction and CSIS operational policies. In particular, the Committee's enquiries were meant to determine if:

- the threat was balanced with the infringement on personal privacy resulting from the passage of the information;
- the exchange of information was strictly necessary to meet the Service's operational requirements as per section 12 of the *CSIS Act*;
- the exchange of information involved the unnecessary use of personal and sensitive information;
- the information exchanged was reasonable and factually accurate;
- all CSIS disclosures of information were in accordance with the preamble to subsection 19(2) of the *CSIS Act*.

## COMMITTEE FINDINGS

### Overall Co-operation

The Committee found that CSIS co-operation with federal departments and agencies and its relations with provincial authorities and police forces was productive. Our review also showed a general willingness between CSIS and the RCMP to share information with each other.

In one region, however, the Committee found a list of outstanding requests for information from the RCMP. We questioned the delay and learned that the region had since implemented a tracking mechanism in an effort to deal with the problem.

### Exchanges and Disclosures of Information

Although the Committee found that the majority of CSIS exchanges of information in 1998 complied with policy, agreements and statutory requirements, we found some instances where, in the Committee's opinion, CSIS had retained unnecessary information.

### Unnecessary Retention of Information

The Committee found that one region had collected a report that did not meet the "strictly necessary" criterion under section 12 of the *CSIS Act*. CSIS has since removed the report from its database.

In another instance, our on-site audit of one CSIS region revealed that it had retained several reports in its operational database that it had received from two agencies about planned protests and demonstrations.<sup>9</sup> In our view, some of the information contained in the reports did not demonstrate reasonable grounds to suspect serious violence or a possible threat to public safety. The Committee recommended that CSIS report and retain only the information required to meet its obligations with regard to threat assessments.

### The Tracking System

The Committee found that, in general, CSIS' tracking of information exchanges with domestic agencies was

consistent. However, we did note variations in how the regions applied the tracking procedure, and a few cases in which the tracking information was not accurately recorded. We also expressed our concern about the fact that the policy on operational reporting was still under development for an inordinate length of time:

## Proliferation of Weapons of Mass Destruction

### Report #120

#### BACKGROUND TO THE STUDY

Canada's efforts to prevent or at least slow the proliferation of weapons of mass destruction (WMD)—chemical, biological and nuclear—to states that do not possess them are longstanding. Since the end of the Second World War, Canada has been at the forefront of every important diplomatic and political initiative aimed at creating an international regime to monitor and control the spread of such weapons, the means for delivering them and the technologies needed to build them.

Since the demise of the Soviet Union, the threat to Canadians' security from such weapons has become more diffuse and also more difficult to counter. Growing numbers of states, and even terrorist organizations, are gaining the wherewithal to purchase (or in some cases steal) the technologies and expertise needed to manufacture extremely lethal weapons that could be used against Canada or its allies.

Although Canada does not possess such weapons itself, a national infrastructure of advanced nuclear, chemical, biotechnological and electronic industries and research facilities makes the country vulnerable to illicit procurement. Many technologies used domestically for peaceful endeavours can also be used in weapons manufacture—so called "dual-use" technologies.

Stemming the improper flow of WMD and their supporting technologies has been a pillar of Canada's

foreign policy for many years. An important domestic element of this policy is the need to understand the nature of illicit and clandestine activities that may pose a threat to the security of Canada, Canadians and others. The Service has an important role in collecting and analyzing such information, stating in 1999 that "counter proliferation is one of its security intelligence priorities."<sup>10</sup> The goal of the Committee's review was to assess the Service's performance of its function to advise the Government in a clearly vital area.

The Service correctly viewed the target's efforts to circumvent Canada's laws as a threat to national security

#### **METHODOLOGY OF THE AUDIT**

The Committee reviewed all files for fiscal years 1997–98 and 1998–99 held by the Service in relation to its issue-based investigation of WMD proliferation. We interviewed Service personnel, attended briefings and examined CSIS Target and Review Committee (TARC) documents in cases representative of the Service's entire counter-proliferation effort. In addition, the Committee examined a number of cases that gave insight into the Service's Counter Proliferation Unit, its methods of operation and its relationship with domestic and foreign agencies.

#### **FINDINGS OF THE COMMITTEE**

##### **Threat from a Foreign Country**

From CSIS files it was evident that, because of consistent attempts to procure WMD, a certain foreign country was a particular focus for the Service's investigative efforts. Based on an extensive review of the documentation, we concluded that CSIS had reasonable grounds to suspect a threat to the security of Canada

under sections 2(a) and (b) of the *CSIS Act* and that the targeting level for the investigation was proportionate to the threat. The Committee determined that with one exception (which we brought to the Service's attention), the information collected met the "strictly necessary" test.

##### **Threat from a Particular Target**

The Committee examined the case of a particular counter-proliferation target that had recently come to our attention. We believe the Service correctly viewed the target's efforts to circumvent Canada's laws as a threat to national security.

##### **Certain Illegal Activities**

The Service received information that led it to believe some activities had taken place that constituted a threat to the security of Canada as defined in sections 2(a) and (b) of the *Act*. Subsequent CSIS investigation revealed that a violation of Canadian law had occurred and the appropriate department of the Federal Government was so advised. The Committee found that the level of investigation employed by the Service was proportionate to the threat and that CSIS had retained only strictly necessary information in its database.

##### **The Service's Counter-proliferation Effort in General**

It is evident to the Committee that the Service plays an important role in Canada's management of proliferation issues at the domestic level (co-operating with police and other enforcement agencies), and globally (acting in support of DFAIT counter-proliferation initiatives, and exchanging information with allied governments and other parts of the international antiproliferation regime). We noted that, overall, the Service's approach to proliferation matters was both strategically sound and flexibly managed. The Service was particularly concerned to give the counter-proliferation unit considerable leeway in its staffing decisions, reflecting the specialist and technical nature of the tasks being pursued.



s.15(1) - Subv

s.21(1)(b)

s.24(1)

**SECRET**

*Handwritten notes:*  
6/6/18  
18:31

**From:** PFR Government Liaison [redacted]  
**Sent:** June-06-18 5:31 PM  
**To:** [redacted]  
**Cc:** [redacted]  
**Subject:** Re: questions regarding Project SIDEWINDER

Classification: Secret  
Classification: Secret  
Restriction / Restriction d'accès: NTK / BDS  
File Number / No. de dossier: 520-1-12

Good afternoon,

Further to the questions you posed yesterday (appended below) regarding the above noted project, the Service offers the following note. Please feel free to contact me should you have additional questions or concerns.

Regards,

[redacted signature block]

Policy & Foreign Relations (PFR)  
Direction des politiques et des relations extérieures

[redacted]

<b>SUBJECT / CONTEXT</b>	Information regarding potential leak of CSIS-RCMP report
<b>CLIENT:</b>	PS
<b>QUERY DATE:</b>	2018 06 05
<b>RESPONSE DATE:</b>	2018 06 06
<b>ORIGINAL SOURCE:</b>	CSIS
<p><b>SECRET</b></p> <p><b>ISSUE:</b> Questions regarding alleged CSIS report being available online</p> <p><b>BACKGROUND:</b></p> <p>In the late 1990s various news media outlets had reported on a joint CSIS-RCMP project to assess the extent of the potential threat posed by the acquisition and control of Canadian companies by members or associates of triads with affiliations to Chinese Intelligence Services. The reporting was based on leaked information.</p> <p>The apparent source for the reporting was a draft version of the classified report dated June 24, 1997, and titled Chinese Intelligence Services and Triads Financial Links in Canada, and code-named SIDEWINDER.</p>	

**SECRET**

s.16(1)(a) s.21(1)(b)

**SECRET**

s.16(1)(c)

s.24(1)

s.24(1)

In 2001 it was confirmed that the entire SIDEWINDER report was available on the internet.

**COMMENT / NOTE:**

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE. THIS DOCUMENT IS THE PROPERTY OF THE CANADIAN SECURITY INTELLIGENCE SERVICE. IT IS LOANED TO YOUR AGENCY / DEPARTMENT IN CONFIDENCE, FOR INTERNAL USE ONLY. IT MUST NOT BE RECLASSIFIED OR DISSEMINATED, IN WHOLE OR IN PART, WITHOUT THE CONSENT OF THE ORIGINATOR. IF YOU ARE SUBJECT TO FREEDOM OF INFORMATION OR OTHER LAWS WHICH DO NOT ALLOW YOU TO PROTECT THIS INFORMATION FROM DISCLOSURE, NOTIFY CSIS IMMEDIATELY AND RETURN THE DOCUMENT.

Original question(s) from Public Safety:

*The Minister would like to know:*

>>>\*\*\*\*\*[INFO DEPOT START / DÉBUT INFO DÉPÔT]\*\*\*\*\*

Sender / Envoyeur : [REDACTED]

Recipients / Receveurs : [REDACTED] (PSEPC-SPPCC); [REDACTED] (PSEPC-SPPCC);

Subject / Sujet : Re: questions regarding Project SIDEWINDER

Date : 6/6/2018 5:30:31 PM

**SECRET**

**Pages 112 to / à 155  
are not relevant  
sont non pertinentes**

**Pages 156 to / à 157  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**13(1)(a), 15(1) - Int'l, 15(1) - Subv, 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Page 158**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 159 to / à 163  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Page 164**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**13(1)(a), 15(1) - Int'l, 15(1) - Subv, 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 165 to / à 168  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**



**Pages 169 to / à 184  
are not relevant  
sont non pertinentes**

**Pages 185 to / à 207  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 20(1)(c), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 208 to / à 217  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 21(1)(c), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 218 to / à 221  
are not relevant  
sont non pertinentes**

**Pages 222 to / à 227  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Page 228**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 19(1), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Page 229**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 230 to / à 231  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 19(1), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**



**Page 232**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**13(1), 15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 233 to / à 235  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 19(1), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 236 to / à 263  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 21(1)(a), 21(1)(b)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 264 to / à 273  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 274 to / à 275  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Subv, 21(1)(a), 21(1)(b)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 276 to / à 301  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 302 to / à 308  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**13(1)(a), 15(1) - Int'l, 15(1) - Subv, 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Page 309**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 19(1), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**



**Page 310**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**13(1)(a), 15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b), 24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Page 311**

**is withheld pursuant to sections  
est retenue en vertu des articles**

**13(1)(a), 15(1) - Int'l, 15(1) - Subv, 16(1)(c), 19(1), 20(1)(c), 21(1)(a), 21(1)(b),  
24(1)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 312 to / à 321  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**13(1)(c), 15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b)**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 322 to / à 331  
are withheld pursuant to sections  
sont retenues en vertu des articles**

**15(1) - Int'l, 15(1) - Subv, 16(1)(c), 20(1)(c), 21(1)(a), 21(1)(b)**

**of the Access to Information  
de la Loi sur l'accès à l'information**