Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SIGINT 101

Orientation Program

The Office of Cryptologic Studies

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Forward 3

Chapter 1: Introduction 11

Chapter 2: Introduction to SIGINT: Programs and Requirements 13

Chapter 3: SIGINT Oversight and Compliance 19

Chapter 4: ITS Policy Oversight & Compliance 25

Chapter 5: Introduction to SIGINT Tools 27

Chapter 6: Access Fundamentals for SIGINT 31

Chapter 7: Introduction to [redacted] 37

Chapter 8: [redacted] Overview 41

Chapter 9: Introduction to [redacted] 47

Chapter 10: Introduction to Core SIGINT Systems 59

Chapter 11: Introduction to Data Analysis and Enrichment 63

Chapter 12: SIGINT Systems Development Overview 69

Chapter 13: Intelligence Branch Overview 75

Chapter 14: SIGINT Collaboration using Web 2.0. 87

Chapter 15: Introduction to D2 and OPS-1 Policy 95

Appendix A: The World of SIGINT 107

Appendix B: Supplementary Information: History of SIGINT 115

Appendix C: Supplementary Information: Government of Canada Requirements 133

Appendix D: Supplementary Information: Access Fundamentals for SIGINT 137

Appendix E: Supplementary Information: DAE Crypt Samples 149

Appendix F: Supplementary Information: SIGINT Collaboration using Web 2.0 159

Appendix G: Supplementary Information: Part V.1 of the *National Defence Act* 163

SIGINT 101: Acronyms and Glossary 169

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

WELCOME TO SIGINT 101

The SIGINT 101 program has been developed to give new SIGINT employees a common baseline knowledge and introduction through a sequence of modules designed and delivered by the Office of Cryptologic Studies (OCS) and SIGINT subject-matter experts. The aim of our program is to help you understand the larger context within which you are working, both within and beyond CSEC and the SIGINT business line. We want to give you a general awareness of a wide range of SIGINT approaches to confronting intelligence problems at every point along the end-to-end SIGINT process. This course will not answer all your questions about SIGINT, but the hope is that SIGINT101 will provide you with an overall understanding of the business of SIGINT, and establish some points of contact for you throughout the organization.

Each of you will be bringing your own specialized skills and knowledge of CSEC and SIGINT to this program. If you find that you already know some of the information we present to you, remember that this may not be the case for many of your classmates who come from different backgrounds. In turn, some of the material that is new to you may be known to them. That is the nature of an orientation course. Everyone is starting from a different point and thus brings a different perspective to the course. Take dvantage of the diversity of the class and talk to your colleagues, share your experience and make new contacts.

Throughout the course, your OCS Facilitator will be available to answer any questions you may have about working in SIGINT, or how CSEC conducts operations. As with all our courses, we welcome your comments and feedback, as participant input is a major driving force in improving the content and the delivery of the program.

We hope that you will enjoy your experience on SIGINT101, and we wish you all the best as you embark on an exciting journey working in SIGINT.

[redacted]

Sincerely,

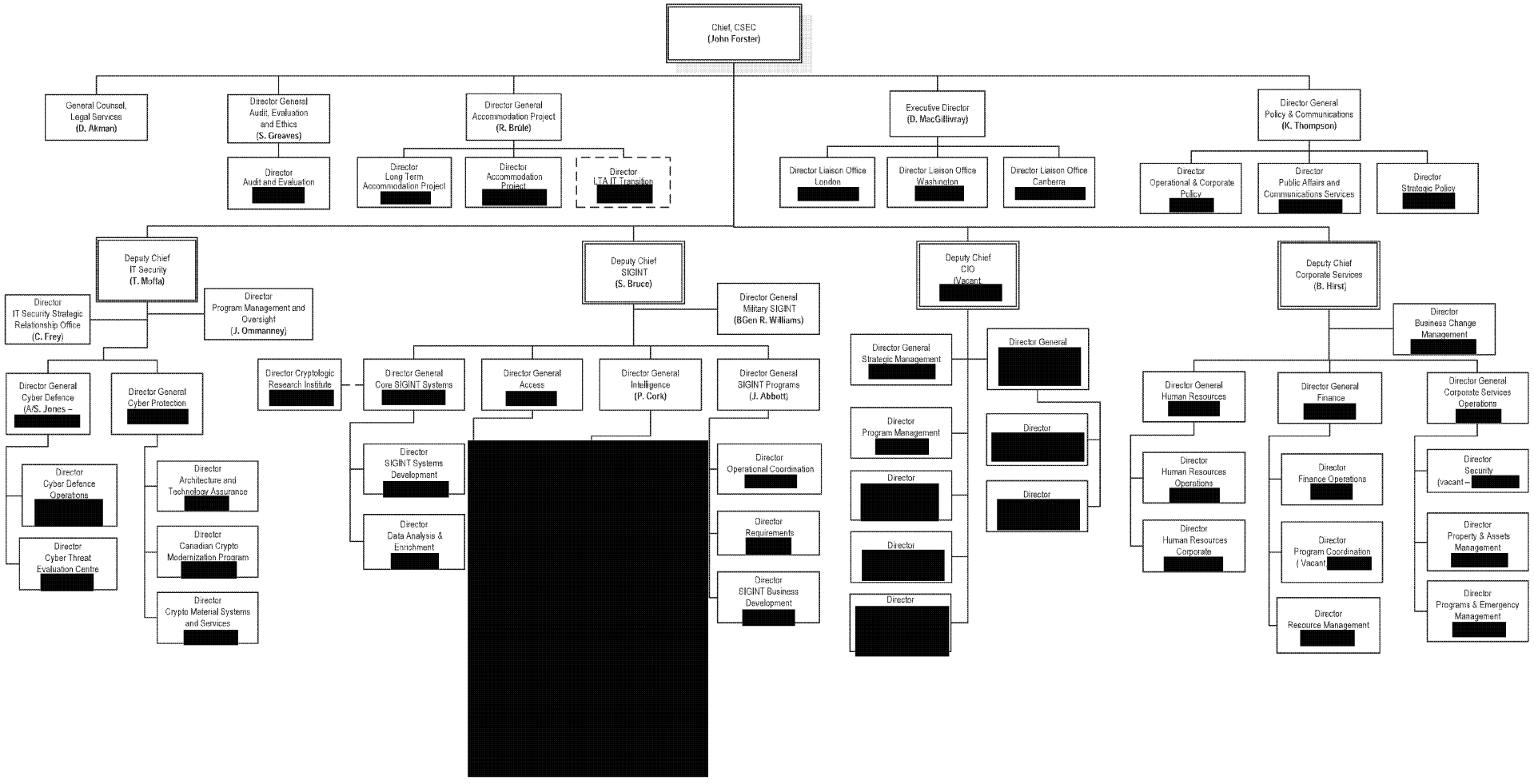
[redacted]

Manager, The Office of Cryptologic Studies

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

A-2017-00017--01832

CSEC ORGANIZATIONAL CHART

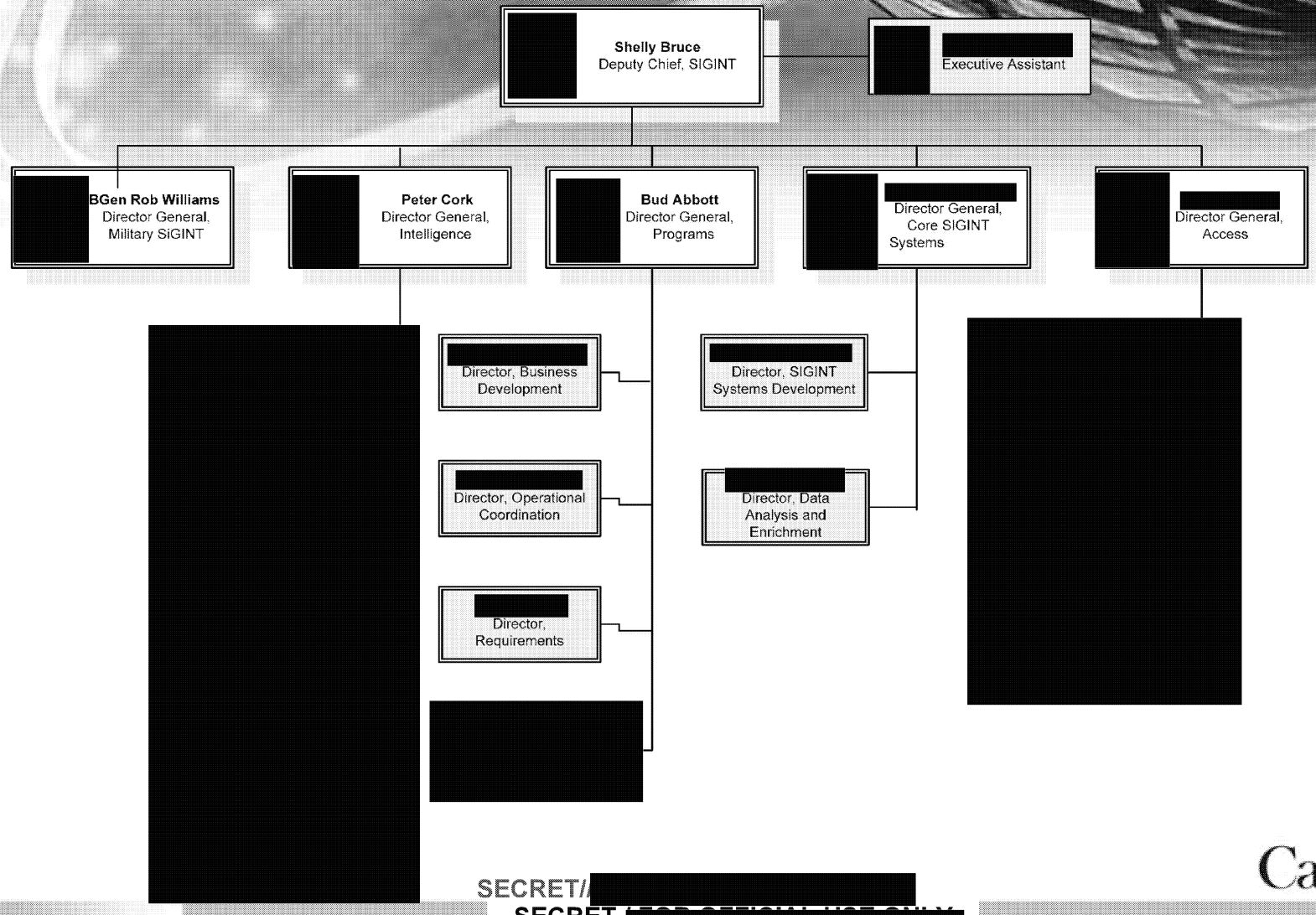


Updated: March 14, 2012
By: Management Resourcing and Development, HR

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SIGINT Organization



TOP SECRET//SI

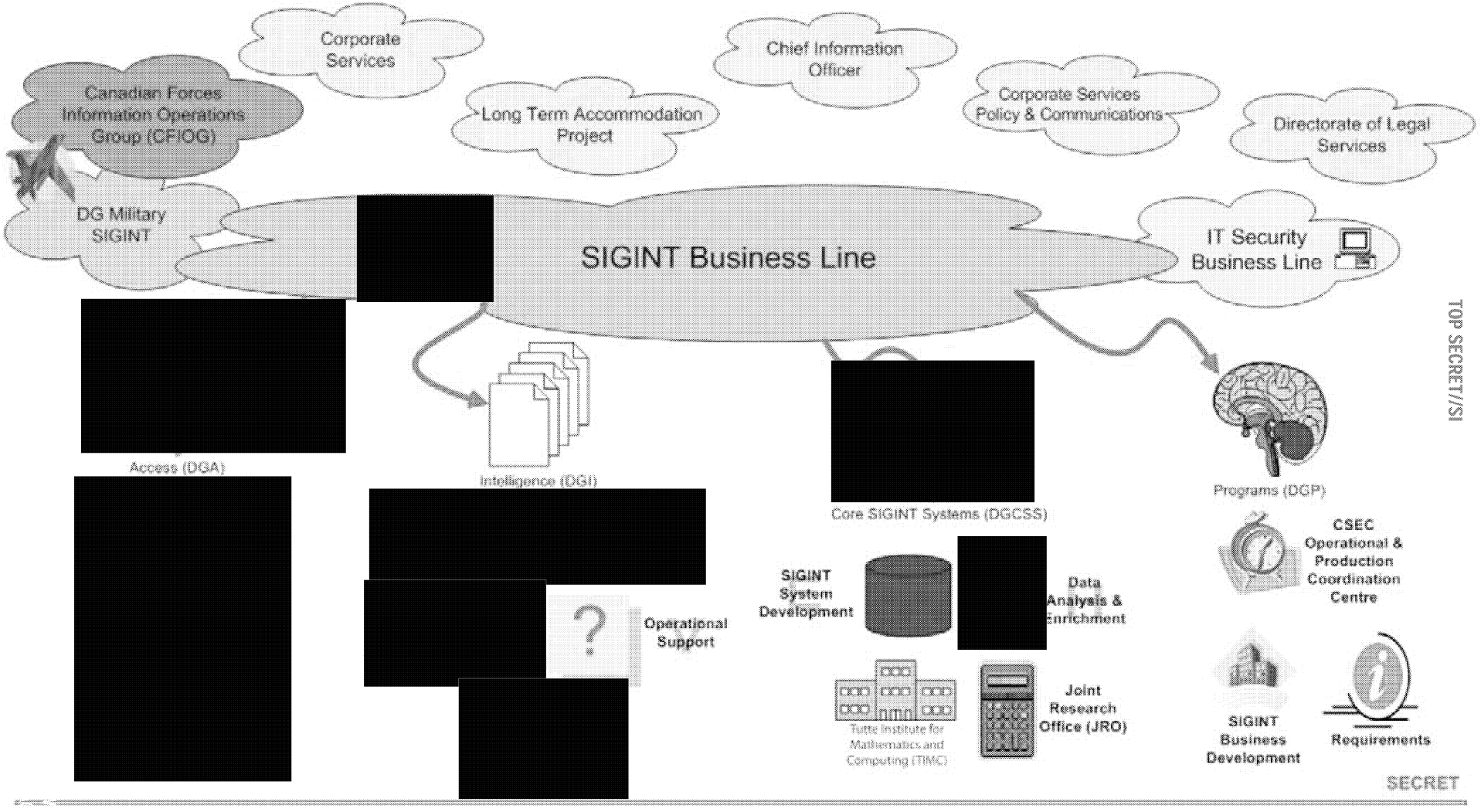
SECRET/[redacted]

SECRET//[redacted]

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

SIGINT ORGANIZATIONAL CHART



TOP SECRET//SI

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 1

Introduction

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

The SIGINT101 orientation program is designed to provide SIGINT employees with background on the various operational and support areas within the SIGINT business line. CSEC has two major operational business lines: ITS (IT Security) and SIGINT (Signals Intelligence). As members of SIGINT, you will need to understand how various groups within the area work together to produce intelligence reports for CSEC's clients within the Government of Canada. In addition, SIGINT101 aims to provide participants with an introduction to the SIGINT requirements, capabilities, analysis, and techniques used to exploit communications signals of entities of interest (targets) in order to provide the Government of Canada with key information to protect our national security and our national interests.

The program is divided into short modules. Each module covers a specific topic within SIGINT, a piece of the puzzle, so to speak. At the end of SIGINT101, new employees would be able to combine the knowledge gained from this program to create a fairly high-level view of SIGINT as it is being conducted in Canada.

This textbook was written based on the content of the various modules presented in the SIGINT101 program. It is designed to serve as a supplementary reference guide for new SIGINT employees. The following modules and sections are included in this text:

- History of SIGINT
- OPS-1 Awareness
- Introduction to SIGINT Programs and Requirements
- SIGINT Oversight and Compliance
- Intelligence Branch Overview
- SIGINT Collaboration using Web 2.0
- SIGINT Systems Development Overview
- Data Analysis and Enrichment
- Access Fundamentals for SIGINT
- [redacted] Overview
- [redacted] Overview
- [redacted] Overview
- SIGINT Tools Reference Guide
- SIGINT101 Glossary

In addition to reference information, this textbook is also designed to allow participants to contribute their insights, questions, and notes throughout the course. Some activities covered in the modules will also be included in this text.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

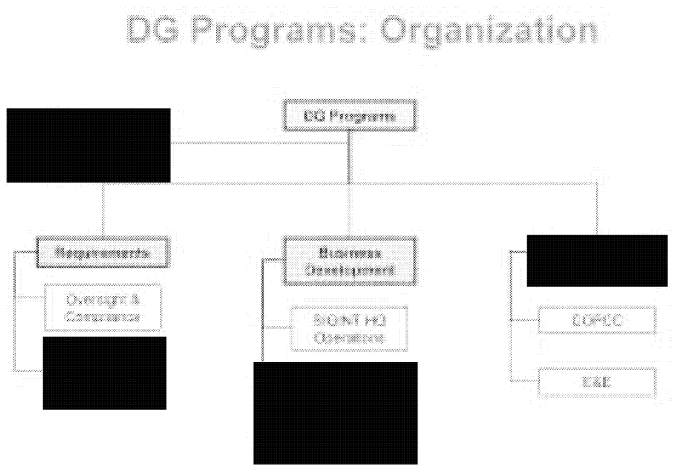
chapter 2

Introduction to SIGINT Programs and Requirements

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT Programs (DGP) is an area of work within CSEC SIGINT business line that serves as the "honest broker", coordinator, and monitor of the entire SIGINT process. Headed by Director General (DG) Bud Abbott, DGP performs a numbers of separate, but related Horizontal coordination functions on behalf of DC SIGINT. DGP is also responsible for the coordination of various business and strategic activities within SIGINT and with CSEC's clients.

This chapter will provide an overview of the work conducted under the SIGINT Programs Directorate, as well as a description of the SIGINT Requirements process.



SIGINT PROGRAMS

Organizationally, DGP is divided into four specific groups: Requirements (SPR), [redacted] Business Development [redacted], and [redacted] Each group addresses different aspects of the overall responsibilities of the SIGINT Programs Directorate.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Figure 2.1 shows the activities within DGP.

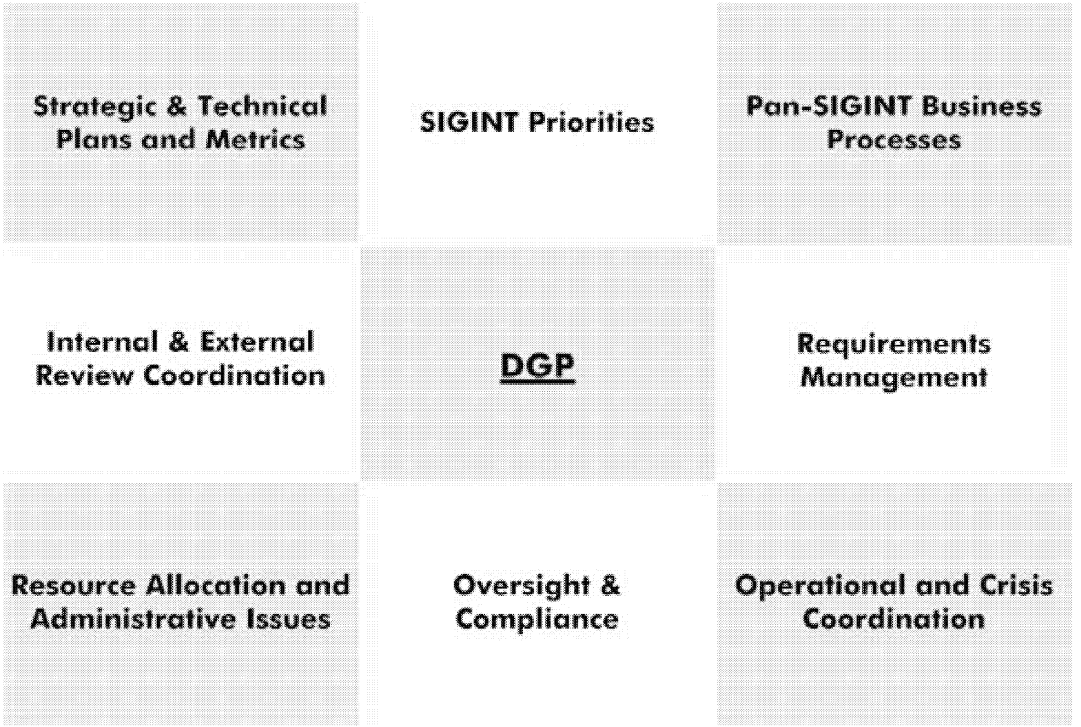


Figure 2.1

CRITICAL SIGINT QUESTIONS:

Do we know what we're doing?

Do we know where we're going?

Are we making a difference?

Are we using our powers responsibly?

Are we worth the cost?

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT PROGRAMS REQUIREMENTS

SIGINT Programs Requirements (SPR) is responsible for formally stating operational, and compliance requirements on behalf of the Deputy Chief of SIGINT. These requirements include: the National SIGINT Priorities List (NSPL); CSEC SIGINT Operations Instructions (CSOIs); [redacted] internal & external review coordination; strategic pursuit support; prioritization for all SIGINT functions; Operations Approval Authority; and SIGINT security-related functions.

Under the direction of SPR, there are two offices: the SIGINT Programs Oversight and Compliance (SPOC); and SIGINT Programs Operational Requirements (SPOR). Table 2.2 outlines the main responsibilities of each office under SPR.

Areas under SPR and their primary functions:

SPOC	SPOR
• Legal/policy framework and compliance » SIGINT compliance validation monitoring » Production of CSOIs • Internal and external review coordination • SIGINT interface with CSEC Commissioner and oversight bodies	• Collects and evaluates operational requirements • Maintains the NSPL and GCR systems • IRRELEVANT • Prepares [redacted] documents for [redacted] • Managers SIGINT Security via SPOR's SIGINT Security Management Office • Acts as the secretariat for the Innovations Board

Table 2.2

Each year, the GC establishes its key intelligence priorities. These are strategic in nature, and must be refined in order for SIGINT to act on them. The Privy Council Office (PCO) leads focused discussions on requirements with representatives from across government, and SIGINT Requirements uses the results of these meetings to further engage with its key client departments. Requirements can also be gathered by Client Relations Officers (CROs), and individual clients can also submit them via [redacted] Based on analysis of these sources of information, SPR develops the NSPL.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

It is important to remember that requirements are vetted for approval and tracked for tradecraft development and capability development. The NSPL drives SIGINT's operational activities, while the Innovations Board evaluates capability development in support of operational activities. Requirements may call for multidisciplinary teams, cross-program integrations, or all-function teams (with members from various areas of expertise) to focus on [redacted] priorities. This may also require joint development of capabilities between Core SIGINT Systems (responsible for [redacted] and SIGINT Access (responsible for [redacted]. The SIGINT Requirements Process provides mechanisms for collaboration and joint projects. Success depends on the clear definition of roles and responsibilities, the standardization and transparency of decision-making consultations, the robustness of the SIGINT committee structure, and valuable coordination from the SIGINT Programs Directorate.

[redacted]

Under [redacted], key tasks involve coordination of the CSEC Operational Production and Coordination Centre (COPCC) 24-hour Watch Office for the Five-Eyes community and emergency helpdesk support.

[redacted]

As the eyes, ears and point of contact for CSEC, the [redacted] monitors [redacted] reporting 24/7. It provides timely support to Government of Canada (GC) departments and agencies, Canadian Forces (CF) Commands, CSEC management, [redacted] The [redacted] also liaises with Canadian and Second Party partners in response to crisis situations, and keeps abreast of issues of current or future interest to Canadian or allied interests [redacted] Outside of business hours, the [redacted] supports internal CSEC operational or service support areas, backs-up [redacted] in threat-to-life situations.

OFFICE OF NETWORKS AND COMMUNICATIONS

The Office of Networks and Communications (ONOC) provides [redacted], and helpdesk functions. The ONOC coordinates and supports [redacted] after-hours, ensuring that systems, databases, secure communications devices and other SIGINT equipment are operational. They are also responsible for [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

EVENTS AND EXERCISES TEAM

COPCC also coordinates CSEC operations across activity areas via the Events and Exercises (E&E) team. This centralized operations structure brings together critical skills from CSEC activity areas to concentrate on top priorities. The Events Team operates in collaboration with [redacted] ONC to provide continuous support to high priority operations. E&E provides logistical, technical and operational support as required, which can include:

- scheduling VTCs;
- leading CSEC involvement in [redacted] exercises;
- tailoring operational space (custom software environments, stand alone testing labs, etc.);
- informing senior management of operational updates;
- capturing daily situational updates;
- documenting progress;
- chairing coordination meetings;
- liaising with GC clients and Second Parties; and,
- [redacted] planning and coordination.

SIGINT BUSINESS DEVELOPMENT

The Business Development Group within SIGINT Programs focus on financial and assets management, business plans and policies, SIGINT training and development, performance and resource reporting, and strategic support. These are managed by three different offices, each responsible for the above-mentioned tasks. Specifically, the [redacted] develops, implements, and evaluates comprehensive training to support the SIGINT workforce. SIGINT staff members would come in contact with the [redacted] most frequently for their training needs. Members of this group also support the new SIGINT governance structure comprised of the [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 3

SIGINT Oversight and Compliance

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

The Office of SIGINT Programs Oversight and Compliance (SPOC) falls under SIGINT Requirements, which is located within the SIGINT Programs activity area, under the SIGINT business line.

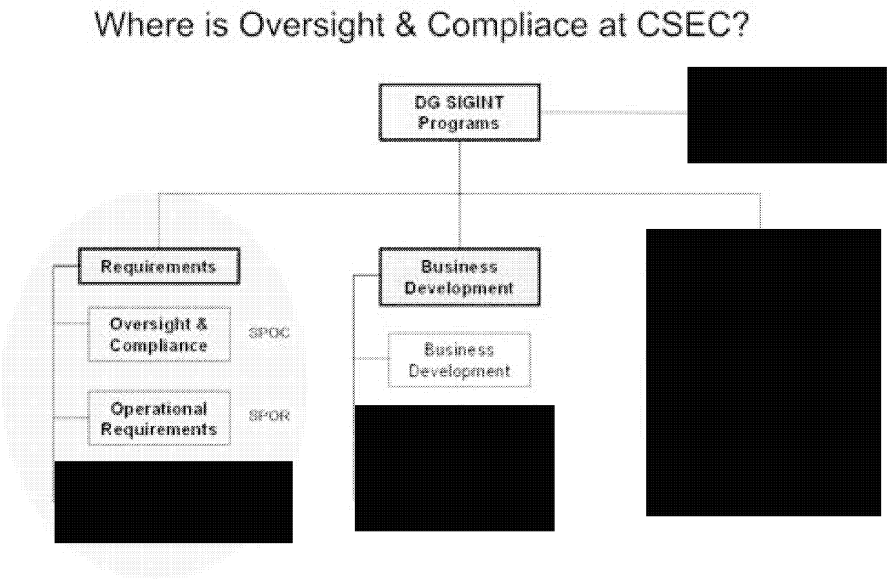


Figure 3.1

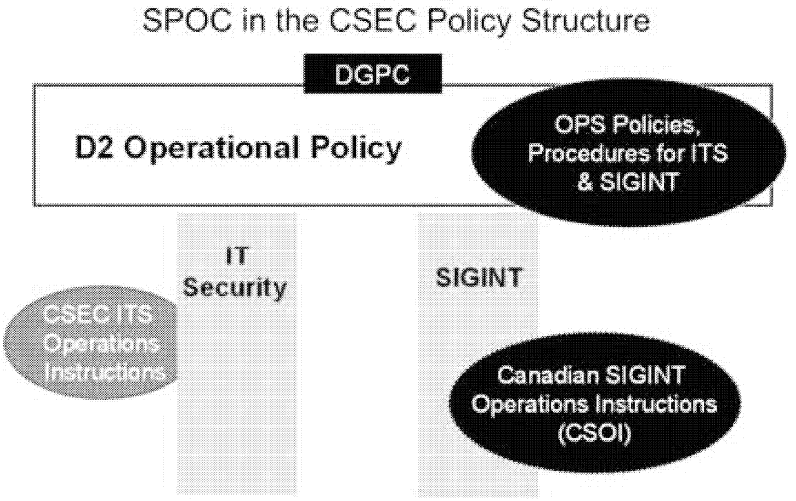


Figure 3.2

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SPOC's functions stem from CSEC's organizational values, particularly those of Lawfulness, Integrity, Teamwork and Professionalism. CSEC must demonstrate lawfulness, meet the conditions of Ministerial Authorizations and Ministerial Directives, and establish internal controls and awareness. All of these tasks are aimed towards the ultimate purpose of SPOC — ensuring that CSEC remains operational. Figure 3.1 is a visual representation of the relationship between legislation, policies and procedures, and operational decisions.

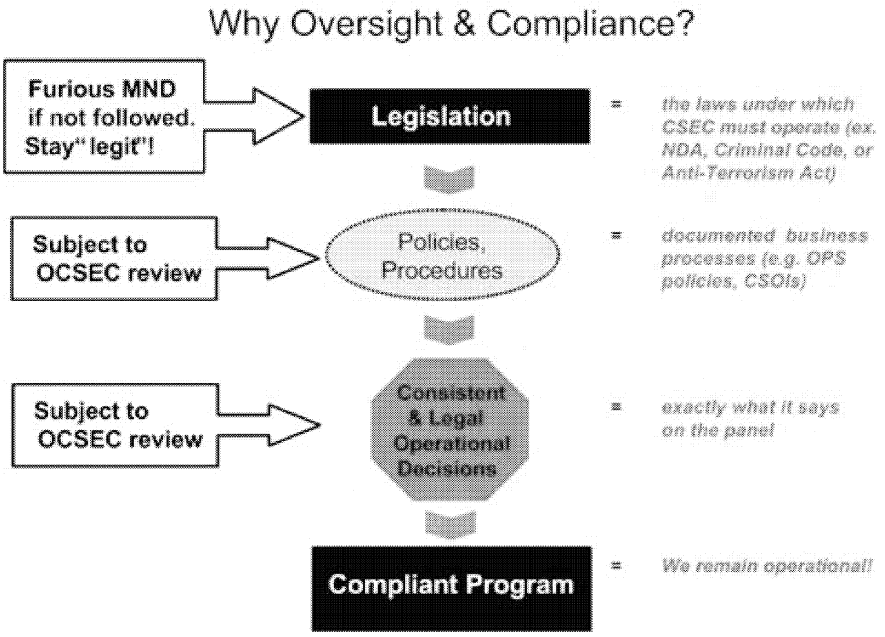


Figure 3.3

Under the authority of Deputy Chief (DC), SIGINT, SPOC is responsible for drafting CSEC SIGINT Operational Instructions (CSOIs) documents which ensures that operations are conducted in accordance with CSEC's operational policies and legislation. Ultimately, CSOIs assist SIGINTers in making sound operational decisions. SPOC also plays a role in ensuring that disciplined accountability and compliance are key components of SIGINT activities. Figure 3.4 shows how CSOIs address various aspects of SIGINT operations.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Figure 3.4

SPOC's other functions include:

- Being the SIGINT point-of-contact for internal audits, government inquiries, and ATIP requests;
- Monitoring issues related to 5-Eyes [redacted] to ensure CSEC can work effectively with its SIGINT partners while respecting its own legal and policy obligations;
- Developing SIGINT processes;
- Answering questions related to the access, handling and use of SIGINT;
- Preparing reporting based on SIGINT activities under Ministerial Authorizations;
- Providing direction and guidance on SIGINT practices and technologies (from a compliance perspective); and
- SPOC also serves as the SIGINT point-of-contact for Office of the CSEC Commissioner (OCSEC) reviews of activities and public complaints that involve the SIGINT business line.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

What are Ministerial Authorizations (MAs) and Ministerial Directives (MDs)?

- MAs protect us legally from the incidental collection of private communications while conducting our foreign intelligence collection activities, subject to explicit conditions
- MDs provide us with specific guidance from the Minister of National Defence (MND) as to how we should do our business

SPOC exists to ensure we...

- demonstrate lawfulness
- meet the conditions of CSEC's MAs and MDs
- establish internal controls and awareness
- identify and address procedural weaknesses and risks
- **REMAIN OPERATIONAL!**

More on CSOIs...

- issued under DC SIGINT's authority
- provide direction on how activities are to be conducted within existing legal and policy framework
- capture "lessons learned", so less time is spent thinking about how we could/should do something and more time actually doing it!
- CSOI-4-1 SIGINT Reporting, CSOI-4-4 Targeting and Selector Management Using [redacted] National SIGINT Systems For Intelligence Reporting Purposes

The Office of the CSEC Commissioner (OCSEC)

- Office of the CSEC Commissioner (OCSEC) Reviews
- has existed since 1996
- is separate from and independent of CSEC
- *Anti-Terrorism Act* of Dec 2001 formally established the OCSEC in legislation, through amendments to the *National Defence Act* (Part V.1)

OCSEC's Mandate

- to review the activities of CSEC to ensure they are in compliance with the law and to advise the Minister and Attorney General of Canada of any activities that may not be in compliance with the law
- to receive complaints about the lawfulness of CSEC's activities
- to carry out specific duties under "the public interest defence" provisions of the *Security of Information Act*

Final Thoughts on Compliance

- How we do things is as important as what we do
- Oversight & Compliance ensures:
  - » SIGINT activities are conducted legally
  - » CSEC powers are not abused
  - » CSEC can maintain the trust of the government and the people
  - » Public complaints can be avoided as a matter of principle and practicality
  - » Privacy of Canadians in maintained

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Some sample questions:

[redacted]

Considerations:

- [redacted]
- Is there a policy or a CSOI covering this issue?
- What does the [redacted] data look like?
- Are there privacy issues with sharing the data in question?

[redacted]

Considerations:

- Note: Usually, an email address that ends in ".ca" suggests the user would be a Canadian – policy stipulates that an analyst cannot target this person.
- What information does the analyst have to suggest the user is not Canadian?
- How does the analyst know the user is not located in Canada?

WHO DO I CONTACT IF I HAVE A QUESTION ABOUT:	SPOC	D2
The application of OPS-1 procedures		X
Sanitization or Sensi-check		X
How a certain SIGINT procedure applies to my work	X	
Whether my activities are compliant – "Can I do this?"	X	
A specific SIGINT procedure or CSOI	X	

SPOC welcomes questions about SIGINT policy and compliance. Should you have any questions regarding your work, or if you come across policy issues that you wish to clarify, please contact: [redacted]-dl@cse-cst.gc.ca.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 4

ITS Policy Oversight & Compliance

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

IPOC OVERVIEW

ITS Policy, Oversight and Compliance (IPOC) enables ITS Cyber Defence operations and is the ITS version of SPOC. IPOC provides advice, guidance, and compliance monitoring to analysts operating under part (b) of CSEC's Mandate. IPOC contributes to the development of OPS-1, OPS-1-14, OPS-1-15 and OPS-1-6, as well as controls the IT Security Operational Instructions (ITSOIs) for cyber defence. IPOC gives policy briefings and administers the annual mandatory ITS Policy Quiz for everyone who needs access to ITS Cyber Defence data.

IPOC ensures that ITS operations focusing on cyber threats to systems of importance to the Government of Canada respect Canadian privacy laws. ITS operations fall under two categories: those that require a Ministerial Authorization (MA) and are governed by OPS-1-14, and those that do not require an MA such as Data Provided by System Owner (DPSO) or non-MA that are governed by OPS-1-15. Depending on how the data is collected, different policy and legal requirements apply.

AUTHORITIES

MA Operations

Government of Canada departments can sign Memorandums of Understanding (MOU) with CSEC, allowing [redacted] collection of the department's data for cyber defence purposes (as set out in OPS-1-14). All data needs to be relevant to part (b) of CSEC's mandate, and if it contains a private communication, essential to identify, isolate or prevent harm to GC computer systems or networks. Data can be shared with the Government of Canada and Second Party cryptologic agencies (see OPS-1-14 for policy conditions).

Non-MA Operations

Government of Canada departments can request assistance without an MOU, and can provide their data directly to ITS. In this instance, the system owner collects the data, which may include private communications, and provides it to CSEC. ITS staff analyze this data to detect and mitigate the perceived cyber threat. This data may include private communications, and it is the responsibility of the system owner to determine whether it was essential to provide ITS with the private communications for the purpose of protecting their systems.

Non-MA (tool deployments)

ITS can also, with client permission, deploy tools that do not intercept private communications on systems of importance to the GC. IPOC's role, due to the privacy implications, is to ensure that tools adhere to CSEC policy. ITS can use the data generated and collected by these tools to inform the analysis in other cyber defence activities.

SHARING WITH SIGINT

Employees in SIGINT can be considered as part of a cyber defence team. These employees are normally working on the cyber portfolio, and can receive permission to access raw cyber defence data. These employees must complete the SIGINT OPS-1 test as well as the ITS Policy Quiz.

Members who are not considered part of a cyber defence team who need access for other purposes, such as triaging, can receive access upon request.

For MA Operations, data can be shared with SIGINT under certain circumstances and with specific restrictions (see OPS-1-14 for details).

IRRELEVANT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 5

Introduction to SIGINT Tools

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

The business of SIGINT requires a multitude of computer applications and software to aid in the collection, processing, and analysis of data in order to generate intelligence. Throughout your career you will be introduced to, and familiarized with, many of these SIGINT tools. Before an overview of the process of SIGINT takes place, this chapter will help identify and explain the basic functions of the various SIGINT tools that will be mentioned in the SIGINT101 program.

[redacted] is Canada's SIGINT end-product repository and report creation tool, and contains all SIGINT end-product reports that CSEC produces, receives from Second Parties, as well [redacted]

From a client's perspective, [redacted] is used to as a database, where users can search on keywords, Government of Canada Requirements (GCRs)[1], or report serial numbers. CSEC's Client Relations Officers also access [redacted] in order to compile relevant intelligence reports for high-level Government of Canada clients.

[redacted] is CSE's [redacted] is a multipurpose tool that features three main functions: [redacted] can also

1. For more information about GCRs, please refer to Appendix C.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

This list of tools is by no means exhaustive. Additional information on each SIGINT tool mentioned in this chapter, as well as a more comprehensive list of tools, can be found on the [redacted] at [redacted] Chapter 13 in the textbook will discuss in more detail the [redacted] and other Web 2.0 tools being used at CSEC and other SIGINT organizations.

In addition to the tools mentioned above, many CSEC analysts will make mention of legacy systems that, while they are no longer in use, are still being spoken of. Below is a brief description of these tools, which will give you a better idea, and some context, as whence the currently tools have evolved.

2. CSEC's secured computers are often referred to as [redacted] computers. Unsecured computers are known as [redacted] computers.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 6

Access Fundamentals for SIGINT

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

In previous chapters, you have read about CSEC's operational policy, oversight and compliance bodies, as well as topics relating to requirements, reporting, and horizontal support. This chapter is an introduction to SIGINT Access. This chapter will provide a high-level view of the basic [redacted] Access, identifying [redacted] strengths, weaknesses, and dependencies, and highlighting some of the challenges that have arisen as a result of the advances in communications technology. The details of the various [redacted] will be covered in later chapters.

Before we look at the specifics of SIGINT Access, we first need to look at the [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

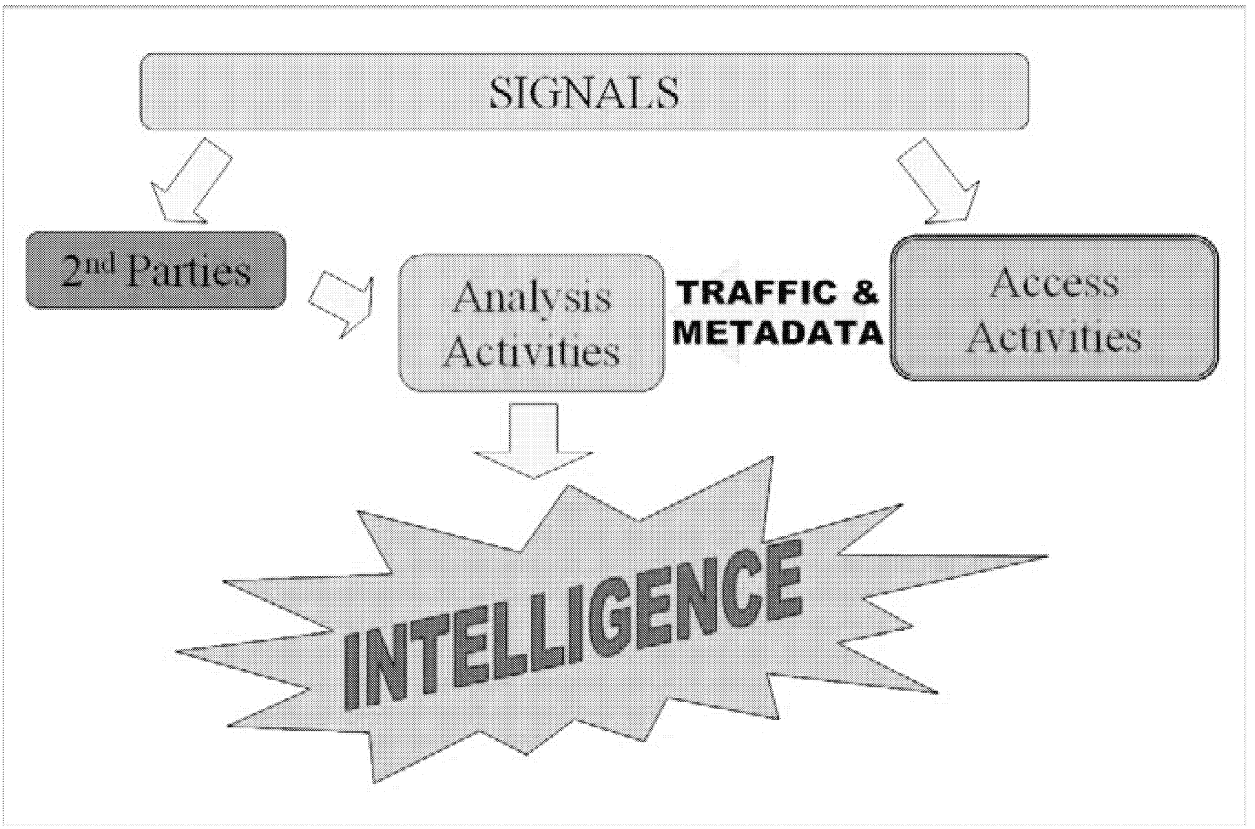


Figure 6.3

Figure 6.3 depicts a simplified version of the SIGINT cycle where Access is situated within the "process" as the leading edge to the production chain of Intelligence. [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 7

Introduction to [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] provides [redacted] solutions to meet foreign intelligence requirements for the GC including IRREL

IRRELEVANT

[redacted] **MISSION:**

[redacted] mission is to provide solutions, through the development of [redacted] capabilities and operations that contribute to CSEC's mandate.

[redacted] **DEFINITION:**

[redacted]

There are 5 main activity areas in [redacted]

[redacted]

Conducts and coordinates all [redacted] operations.

[redacted]

Responsible for critical systems and products assurance.

[redacted]

The research and development of techniques and capabilities to [redacted]

[redacted]

The research and development of [redacted] technologies.

[redacted]

Enables the [redacted] mission through cross-program coordination and support.

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

CHALLENGES FACING [redacted]

As the pace and complexity of [redacted] continues to increase, [redacted] faces many challenges such as:

[redacted]

Therefore, to ensure [redacted] success, it is imperative that [redacted] leverage not only the work being done within the other [redacted] areas but also from other groups across SIGINT [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

OVERVIEW OF [redacted] LIFECYCLE:

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 8

[redacted] Overview

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] is a branch of the Directorate General Access (DGA) within the SIGINT business line. [redacted] is a [redacted] and is an important source of collection for any SIGINT agency. The program allows CSEC to collect information [redacted] Like other areas within SIGINT, all [redacted] collection is directed by the NSPL[2]; second party requirements received by CSEC should be linked back to a Canadian requirement on the NSPL.

At CSEC, it is the responsibility of [redacted] Group) to ensure that its [redacted] programs are effective, agile, [redacted] and decision-ready to acquire foreign intelligence by accessing the Global Information Infrastructure (GII) [redacted] To this end, [redacted] mission is stated as:

> *To Manage and Develop SIGINT's capability to access and process information from the GII ensuring long-term success. The [redacted] Program manages and develops all [redacted] programs,* [redacted]

[redacted] Group is responsible for designing and developing [redacted] systems [redacted] to obtain broad, effective, and efficient [redacted] access to foreign intelligence [redacted]

Technological advances provide an imperative for [redacted] to keep pace with the telecommunications changes, particularly as network technologies are converging. [redacted]

[redacted] Group projects are aimed at furthering SIGINT's understanding [redacted]

1. [redacted]
2. More information on the NSPL can be found in Appendix C: Government of Canada Requirements
3. [redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

[redacted] is responsible for the following collection and [redacted] support programs within CSEC:

[redacted]

IRRELEVANT

[redacted]

CSEC's [redacted] collection was established under Ministerial Authorization. In accordance with the *National Defence Act*, the [redacted] Program has specific parameters as articulated in a Ministerial Directive. The operational policy for this program is found under OPS-1-13[4]. Traffic collected are specific to foreign communications [redacted] facsimile, as well as internet communications and metadata. The information can be categorized into Digital Network Intelligence (DNI) and Dial Number Recognition (DNR).

Metadata, which contains information on the communications events and the collection source, can be used for contact chaining, network analysis[5] and prioritization, [redacted] and other target-related information.

Particular challenges associated with the [redacted] program include the resources required for [redacted] the legal parameters on collecting and retaining only targeted foreign traffic, and changes in communications technology.

As part of the [redacted] collection program, [redacted] Group helps to manage and maintain CSEC's collection [redacted] program. CSEC's contribution to [redacted] collection is made possible by a Ministerial Authorization and by various authorities given to CSEC by various senior officials of the Government of Canada, including:

- Chief of CSEC;
- [redacted]
- Minister of National Defence; and
- Prime Minister.

The program provides [redacted] In addition, the information collected is [redacted] which allows CSEC to intercept communications that may be important for providing intelligence to CSEC's GC clients.

4. OPS 1-13 can be found at [redacted]
5. Information on network analysis can be found in Chapter 8: Introduction to [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

CSEC [redacted] collection program. CSEC's [redacted] this [redacted] collection, which enables CSEC to [redacted] access opportunities.

[redacted]

Figure 8.1

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] CSEC is able to collect [redacted] to produce intelligence reports of interests to CSEC's clients. CSEC shares this [redacted] with 5-Eyes partner agencies, and in turn, benefits from [redacted] those agencies.

Figure 8.2 illustrates [redacted] program.

[redacted]

Figure 8.2

In accordance with the NSPL, [redacted] has, as its top priority, support to deployed forces. [redacted] provides engineering and technical support to CFIOG [redacted] sites in Alert, Masset, Gander and at Canadian Forces Station (CFS) Leitrim. To support Canada's mission in Afghanistan, [redacted] coordinated with Canadian Forces Information Operations Group (CFIOG) [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

IRRELEVANT

By understanding developing tools, techniques, databases, and data sources works with the Intelligence Branch to ensure that the works of SIGINT continue to meet the requirements as it is outlined in the NSPL.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 9

Introduction to [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

As was discussed in previous chapters, a key consideration in the business of SIGINT is: how do we gather the data required to generate foreign intelligence reports? Within the Directorate General of Access (DGA), the [redacted] group handles immediate requirements for Access services from other areas of SIGINT. This chapter will consist of 3 sections. The first part will cover a general overview of the [redacted] followed by an outline of the responsibilities within the [redacted] The chapter will conclude with an introduction to the [redacted]

[redacted]

1. For more information on the responsibilities of the [redacted], see Chapter 12, Intelligence Branch Overview

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Figure 9.1

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted]

Figure 9.2

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Figure 9.3

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

2. [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted]

The [redacted] Group is responsible for [redacted] also monitors tasking compliance with CSEC policy and Canadian laws.

Some commonly-used terms carry different meanings depending on the area of SIGINT with which one is interacting. Table 9.1 provides different meanings to three terms widely used within SIGINT. It is important for new SIGINTers to understand that depending on the work area, colleagues within the same business may understand these terms in drastically different ways, and this would have a significant impact on the ways in which different areas within SIGINT communicate with one another.

DEFINITIONS OF SIGINT TERMINOLOGY

	COLLECTION	ANALYSIS
Task	[redacted]	
Target	Selectors	[redacted]
Collect	Selector [redacted] combined	

Table 9.1 - The difference in the use of the terms "Task", "Target", and "Collect"

Since collection is a key component [redacted] in SIGINT, it is important to understand the terminology associated with collecting data. The following is a list of terms used to refer to different kinds of metadata[3]:

[redacted]

DNI

(Digital Network Intelligence) The use of keywords (selectors) to intercept [redacted] communication over the Global Network

DNR

(Dialled Number Recognition) The use of phone numbers (selectors) to intercept [redacted] fax [redacted] communication over the Global Network

3. Metadata refers to information associated with a telecommunication to identify, describe, manage, or route the data, but excludes any information pertaining to the content of the telecommunication. For more information, consult the [redacted] article on Metadata

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

CSEC collects traffic from communications intercepted [redacted] is the Canadian [redacted] site and is located at CFS Leitrim.

[redacted] IRRELEV

IRRELEVANT

DNI and DNR are mentioned above, and deserve a more detailed explanation here. Intelligence analysts submit DNR/DNI selectors to intercept [redacted] Fax [redacted] communications over the Global Information Infrastructure (GII). [redacted] coordinates targeting at authorized collection assets and conducting quality control for targeting; ensuring that all requests are compliant with Canadian and allied laws, and that they are consistent with the current GC SIGINT requirements (GCR). Collection equipment [redacted] contains "dictionary" or "telephone number directory (TND)" of targeted selectors. [redacted] within [redacted] is responsible for:

- Creating and maintaining CSEC's [redacted] data flows;
- Creating and maintaining CSEC's [redacted] End Product report exchanges;
- Performing acceptance testing on new or modified data flows;
- Managing CSEC SIGINT [redacted] program [redacted]
- Providing 24/7 support to SIGINT Operations;
- Identifying, analyzing and correcting data flow problems;
- Providing Management information statistics;
- Proactively monitoring [redacted] and
- Responding to client trouble calls, such as: "Where is my data?"; "Can I have my data in a different format?"; and "Why can I not find my data in the repository?".

---

4. [redacted]
5.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Some details on the specific tasks performed by [redacted] include:

- Rules management:
  - » using rules to exercise control over data flows and data types;
- Change management:
  - » understanding the impact of [redacted] and customer requirements;
  - » applying changes as necessary;
- • Problem Management:
  - » Pro-actively responding to prevent data flow incidents and problems, including [redacted]
- • Managing [redacted]
  - » understanding metadata and [redacted] issues ([redacted]
  - » conducting quality control of usage; and
- • Improving standardization:
  - » improving cooperation and understanding within CSEC [redacted] of conducting dataflow management

Should you encounter a problem in your work that requires trouble-shooting or help from the [redacted] below is the contacts for the various offices within [redacted]

AREA	EMAIL DISTRIBUTION LIST	INFORMATION TO BE INCLUDED IN EMAIL
Tasking	[redacted]@cse-cst.gc.ca	[redacted]
DNR Targeting	[redacted]@cse-cst.gc.ca	
DNI Targeting		
[redacted]	[redacted]@cse-cst.gc.ca	

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

[redacted]

[redacted]

The [redacted] group is responsible for coordinating pan-access requirements within the Directorate-General of Access (DGA), between DGA and the Directorate-General of Intelligence (DGI), [redacted] provides:

- Crisis and event coordination across DGA: [redacted] is the DGA point of contact (POC) for COPCC in cases of "event" planning/coordination.
- [redacted] ensures that the appropriate DGA areas and capabilities are represented during coordination meetings.
- [redacted] coordination: [redacted] liaises with SIGINT Programs (DGP) to render stated [redacted] into consumable formats for the appropriate DGA functional areas.
- [redacted] develops and recommends [redacted]
- Representation for DGA on various coordination bodies: [redacted] participates in [redacted]
- [redacted] gathers and prioritizes requirements for [redacted]

What can [redacted] do for you?

- If you have an access problem with your target, [redacted] will contact every DGA group who may be able to help to coordinate the process for solving your problem.
- [redacted] can answer your access questions and/or help you find a POC either in DGA or in [redacted]
- [redacted] can also recommend the best access options and approaches for your target.

Contact: [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 10

Introduction to Core SIGINT Systems

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

The Directorate of Core SIGINT Systems is responsible for providing capabilities to safeguard Canada's security through information superiority, and to enable the [redacted] This area within CSEC provides operational and technical support throughout SIGINT, ensuring that we can both develop and apply our tradecraft to meet the Government of Canada's highest priorities.

Four offices fall under the Director General, Core SIGINT Systems: SIGINT Systems Development (SSD, [redacted] Group), Data Analysis and Enrichment (DAE, also known as [redacted] Group), Joint Research Office (JRO), and the Tutte Institute for Mathematics and Computing (TIMC).

[redacted] is a concept that is being used as part of the Core Systems [redacted] Below is an image of the [redacted]

[redacted]

Figure 10.1 – [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

CSEC conducts a regular review of systems and objectively classifies them in line with the [redacted] the Core Systems [redacted] details and analyses results from recent reviews.

The Directorate employs over [redacted] employees who are mostly engineers, computer scientists, and mathematicians. Many of them have Masters and Doctorate degrees in their respective fields. Together, they interact with all parts of the cryptologic system, and manage databases containing [redacted]

In addition to maintaining and acquiring the [redacted] to store and process data, DG Core SIGINT Systems decrypts approximately [redacted] files annually, allowing SIGINT analysts to [redacted]

To decrypt [redacted] DG Core has approximately [redacted]

[redacted]

Figure 10.2 – Photographs of the [redacted] housed in SLT and maintained by DG Core SIGINT Systems.

The Directorate was notionally formed in 2007 as part of the SIGINT reorganization. This area was created to meet the significant computer science and mathematical challenges that CSEC faced, and its mandate spans from long-term research and development to systems operation.

1. [redacted]
2.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

The [redacted] area within DG Core has been the technical lead for [redacted] R&D since 1990, devoting resources on areas such as: [redacted]

The SIGINT Systems Development area focuses on developing and supporting various SIGINT applications and tools, which allows the Intelligence Branch (DGI) to provide over [redacted] SIGINT reports to Government of Canada clients each year.

The Data Analysis and Enrichment area is responsible for decrypting approximately [redacted] files annually. [redacted]% of Canadian SIGINT reporting is based on encrypted sources. In addition, they are responsible for [redacted] annually.

The following chapters will provide more details on the 2 aforementioned operational areas within DG Core SIGINT Systems: SIGINT Systems Development, and Data Analysis and Enrichment.

The Joint Research Office (JRO) reports to the JRO Executive which provides joint ITS and SIGINT oversight to ensure CSEC's research program as a whole is responsive to the continuously evolving operational environment.

The primary activities of the JRO are:

1. Evolve, refine and continuously validate Research Requirements and Activities [redacted]
2. Perform Science & Technology Foresight [redacted]
3. Provide advice and guidance on Technology Transfer [redacted]
4. Foster Research Relationships [redacted]
5. Foster Out-of-Program Research [redacted] and
6. Align research program through Research Management [redacted]

As one of its many deliverables, research recommendations are presented to the JRO Executive which provides guidance on how to leverage internal research capacity, research relationships and predictive analysis to ensure that the research requirements and focus areas are appropriately addressed.

The Tutte Institute for Mathematics and Computing (TIMC) is a classified mathematical and computational research institute within the Communications Security Establishment Canada (CSEC).

The TIMC is housed in the Insurance Building (IB) on CSEC's campus. The institute is working towards expanding CSEC's strategic technological and research capabilities, with a broader mission of supporting the Canadian Cryptologic Program and its international partners by providing leading-edge solutions to emerging complex problems. These solutions will have real-life implications for the security of Canadians and of our Allies.

TIMC's work today will help CSEC's operational work in the future while maintaining and supporting current capabilities. The institute works in collaboration with a distinguished network of organizations and individuals: leading researchers from Canadian universities and our international partners' research institutes; renowned mathematicians, computer scientists and engineers at the national and international level; and various Canadian governmental agencies.

The first classified research institute of its kind in Canada, the TIMC is a significant step forward by Canada as a valuable partner and contributor to the international mathematical and computational research institutes arena.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 11

Introduction to Data Analysis and Enrichment

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Having discussed the contribution of SIGINT Systems Development (SSD) in providing support to operational SIGINT within CSEC, let's now turn our attention to Data Analysis and Enrichment, also known as [redacted] Group. The Data Analysis and Enrichment group is responsible for providing services using expertise in crypt [redacted] as well as research and development in [redacted] to meet the needs of CSEC's clients in support of [redacted]

It should be noted that many [redacted] Group capabilities are subject to information and data that are mostly classified as [redacted] information will be discussed here.

Data Analysis and Enrichment is divided into [redacted] areas:

- [redacted]

Before a more detailed elaboration on the various responsibilities of the areas within [redacted] Group, one aspect of the work done within Data Analysis and Enrichment requires some explanation. Part of [redacted] Group's work involved data-mining, which refers to the process of searching data for previously unknown patterns and using those patterns to predict future outcomes. Table 11.1 provides a more in-depth look at data-mining as it applies to SIGINT.

DATA-MINING: WHAT IS IT?

WHAT IS DONE?	[redacted]
WHAT IS USED?	
WHAT ARE THE RESULTS?	

Table 11.1 – Explaining data-mining

1. For more information on [redacted] please see [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] focuses primarily on ensuring a sustained cryptologic capability [redacted] through: cryptanalysis [redacted] diagnosis of new and unknown cryptographic challenges; [redacted] within [redacted] Group ensures that important, encrypted information can be deciphered in a timely fashion to facilitate the production of SIGINT, and helps to [redacted] based on the information analyzed by [redacted]. Within [redacted], the [redacted] is responsible for analyzing [redacted] to support SIGINT and military operations, as well as IRRELEVAN Specifically, [redacted] may conduct [redacted] cryptanalysis in support of IRRELEVANT or to look for information to better pursue CSEC's targets.

Within [redacted] the focus of work is mainly the research and development on [redacted] solutions to problems in cryptanalysis, [redacted] data mining, [redacted] also advises CSEC on [redacted] systems that can be used by SIGINT. Also, the [redacted] area maintains the [redacted] for users in [redacted]. One of the projects [redacted] has started [redacted] is [redacted] which is funded by DND, [redacted]

The [redacted] focuses on applied research and experimental development in various fields of computer science and computer engineering, including:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

In addition, [redacted] initiates innovations through the development of [redacted] and maintains research partnerships with [redacted]

The [redacted] area seeks to find new and improved mathematical methods to develop tools and techniques [redacted] data mining [redacted] for SIGINT. [redacted] also conducts research and development on important SIGINT problems including [redacted] tools. The Data Mining [redacted] supports a variety of areas and in particular the [redacted] within the Intelligence Branch. Examples of the team's support include assistance for [redacted] projects and analysis of [redacted] datasets from different sources.

As part of the [redacted] Group efforts to [redacted] Data Analysis and Enrichment provides timely cryptographic support on a daily basis to the analysts [redacted] Group also provides [redacted] especially on [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

CRYPTOLOGY

Aside from research and development, DAE directly impacts on the success of SIGINT in their efforts to conduct crypt on the data that is being collected. The aim of crypt is to decipher [redacted] Interacting with [redacted] also helps to provide support in [redacted]

The following definitions are essential to the understanding of cryptology:

Cryptology: The branch of mathematics embodying both cryptography & cryptanalysis
Cryptography: The art and science of rendering information unintelligible to outsiders
Cryptanalysis: The art and science of breaking the unintelligible information
Plaintext: The original information
Ciphertext: The unintelligible information
Encryption: The process of transforming plaintext into ciphertext
Decryption: The process of transforming ciphertext into plaintext
Cryptosystem or Cipher System: A method or process for transforming properties of the plaintext in order to conceal its meaning
Cryptovariable: Component which is shared between the sender and receiver of the information (this may vary for each encryption)

The graphic below depicts the relationship between some of the terminology covered above:

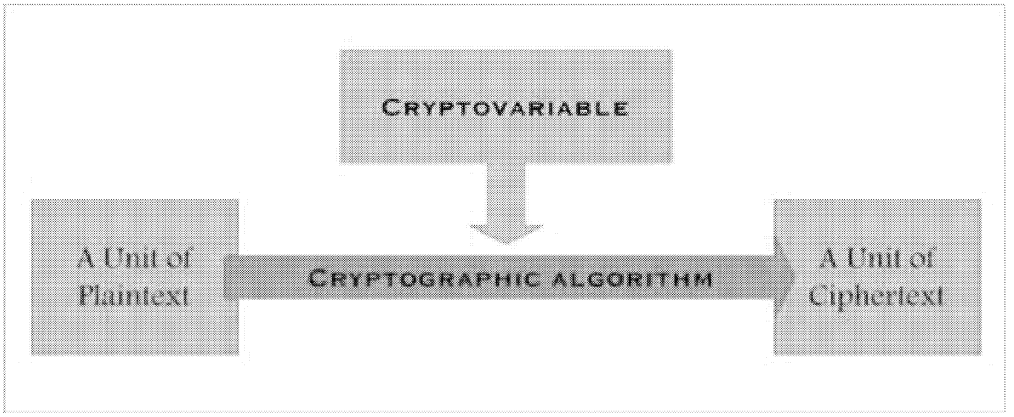


Figure 11.2

It is assumed that the cryptographic algorithm is known while the cryptovariable is kept secret. In other words, the strength of the system depends on the cryptovariable. This is known as Kerckhoff's Principle. Keeping secrets is always difficult so the less that it is secret, the better. in addition, managing the distribution of secrets is hard, so we want to check the amount of secret information to a minimum. Remember that for the system to work, both the sender and the receiver must have a copy of the cryptovariable, but no adversary can have a copy.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

CRYPTOGRAPHY

Cryptography has a long history of concealing vital, secret information. The Caesar cipher is a character-based cryptosystem, where "A" is replaced by "D" in the alphabet (when this is applied to the entire alphabet, "X" is replaced by "A"). In the 1920s, rotor machines were created to automate the process of encryption. The Enigma used by the Germans during the Second World War is one example of this type of device.

With advances in technology, computers allowed bit-based cryptosystems, and common computer algorithms include DES (data encryption standard), AES (Advanced Encryption Standard, Rijndael), RAS (Rivest, Shamire, Adleman), and DH (Diffie Hellman).

There are three types of cryptosystems: symmetric (such as classical, conventional, and private key encryption), asymmetric (public key), and hybrid (a combination of symmetric and asymmetric).

In symmetric cryptosystems, the encryption and encryption keys are the same, are easily computed from each other, and are kept secret. Manual cipher systems include substitution and transposition. Mechanical or electro-mechanical cipher systems are also considered symmetric, such as the already-mentioned Enigma. Nowadays, the vast majority of symmetric systems are implemented on computers, either in software or hardware.

The strength of these systems is usually based on the fact that it would take too long for an adversary to guess all possibilities for the cryptovariable.In asymmetric systems (public key), on the other hands, every user has a public encryption key and a secret decryption key.

the strength of this system is that it is very difficult to construct the decryption key from the encryption key. These public key systems rely on the difficulty of certain math problems. Public key systems make key management easier (in other words, the distribution of secrets which underlies any cryptographic system), but are usually much slower than a symmetric cryptosystem.

In order to get the best of both worlds, hybrid systems are often used, where public key encryption is used for key distribution while asymmetric algorithm is used to send the actual message.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 12

SIGINT Systems Development Overview

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

In order to ensure that SIGINT analysts are able to cope with the technological advances and the changing communications environment, SIGINT Systems Development (SSD), also known as [redacted] Group, has a mandate to provide state-of-the-art SIGINT-specific Information Technology (IT) solutions and support to SIGINT staff and clients in the Government of Canada, while researching potential IT alternatives for the future. Specifically, SSD is responsible for addressing changing SIGINT business requirements with IT capabilities; assisting SIGINT in identifying potential new technologies; developing SIGINT IM/IT[1] strategic and tactical plans; formulating SIGINT IT standards and practices; representing CSEC SIGINT IT externally; and maintaining the IM/IT SIGINT environments[2].

Unlike other areas in CSEC and SIGINT, SSD systems analysts work in a matrix environment. Every member of SSD is a resource that can be assigned to any task that needs them the most. The matrix environment allows SSD to quickly reallocate human resources should critical SIGINT systems require immediate attention. Alternatively, SSD systems analysts are able to tackle major projects and are not inhibited by the organizational structure of the group. Analysts work collaboratively to address the highest priority tasks while maintaining a baseline level of support for SIGINT systems.

[redacted] percent of SSD's resources are devoted to operational support and maintenance, while the other [redacted]% is devoted to new capability development.

SSD is responsible for a large suite of tools used by SIGINT systems analysts in their daily work. Table 12.1 shows the functions of various tools developed by SSD for CSEC SIGINT.

FUNCTION/ USER REQUIREMENT	TOOL DEVELOPED[3]/ SUPPORT PROVIDED
Client Interface & Metrics (for reporting and dissemination)	[redacted]
Processing and Decryption	[redacted]
Analytical Services	[redacted]
Database Management	[redacted]
Targeting and Tasking	[redacted]
Metrics	[redacted]
Metadata Analysis	[redacted]
Specialty Services	[redacted]
[redacted] Analysis	[redacted]

Table 12.1 – Various applications/ support provided by SSD to SIGINT

There are steps that SSD follows when setting up a project to ensure that resources are available, the end-product will be useful to SIGINT clients, and that the requirements have been vetted and confirmed by the clients. Figure 12.2 outlines the steps through which SSD sets up a project, from the inception of the idea to the development of a solution

1. IM/IT refers to Information Management/ Information Technology.
2. Whereas the IT Security branch of CSEC focuses on the defence of Canadian networks (as outlined in Mandate B), SSD's responsibility is to ensure that SIGINT's IT needs are met in terms of developing tools in-house to address SIGINT-specific challenges.
3. For detailed explanation on the functionalities and capabilities of these tools, consult the SIGINT Tools Reference or the [redacted]
4. [redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

One of the largest projects spearheaded by SSD is the development of [redacted] The project was conceived based on analyst input and request for more updated [redacted] and allow analysts to perform multiple tasks efficiently. Figure 12.2 shows the steps involved in setting up a project within SSD.

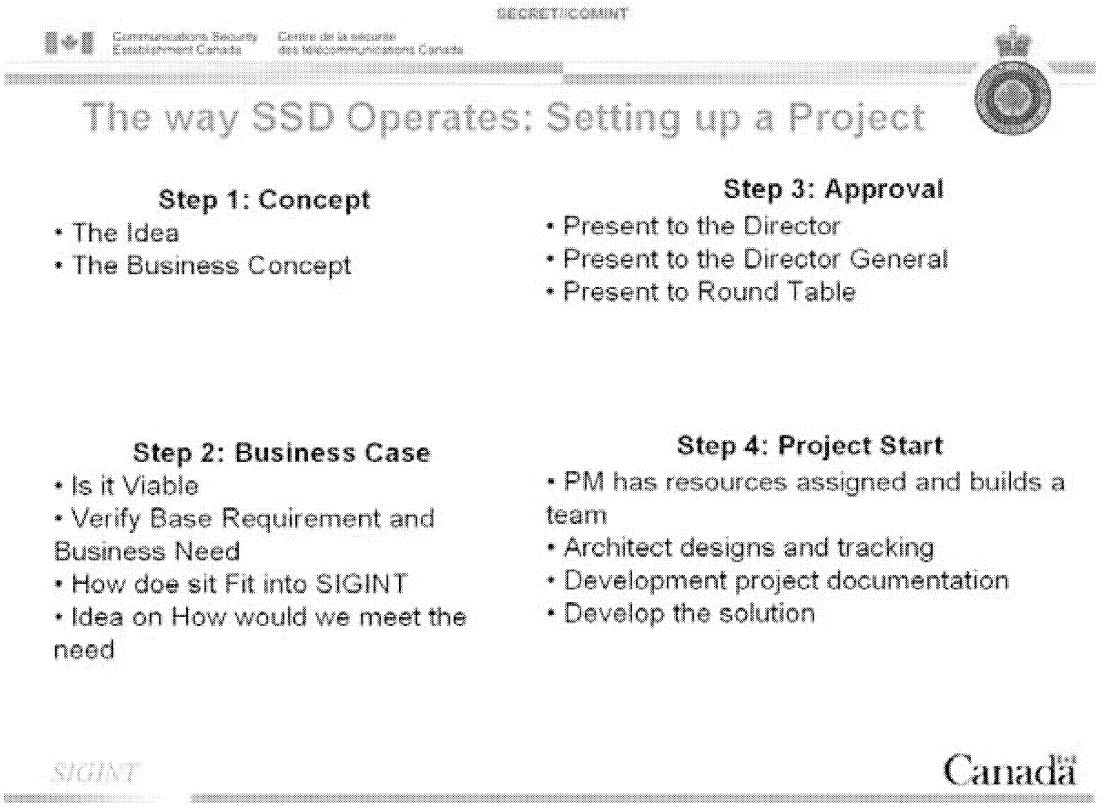


Figure 12.2

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

As CSEC missions change, SIGINT has evolved to meet new requirements. The analytical process has also changed and become more multifaceted. Accordingly SSD's structure has been integrated from one divided into multiple groups. These developments have enabled SSD to embrace technology and find new uses for systems to continue [redacted] Figure 12.3 depicts the roles, relationships, and interactions between various areas within SIGINT to address a specific project.

[redacted] and Systems

[redacted]

Figure 12.3

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

While SSD tackles projects and systems needs based on changing technologies, users' requirements play an important role in providing SSD with information on what SIGINT needs, and how the systems in development can be improved. In articulating requests or problems, the SSD occasionally has to decipher user requirements; frequently, a user will perceive a solution to his/her problem, and propose the solution to SSD. Yet, from a programmer point of view, it is more helpful to SSD to gather information on precisely what the analysts are attempting to do. Here's an example of a request submitted by a user, and the actual requirement:

- Users' Request:
  - » We need a [redacted] capability.
- Actual Requirement:
  - » [redacted]

It is evident from the above example that users and programmers will conceptualize a problem in different ways; it is not always easy for a user to articulate precisely the capabilities he/she means. SSD strives to maintain open dialogue with users to ensure that the product developed will meet the users' requirements.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Roles of SSD and CSEC's SIGINT Community

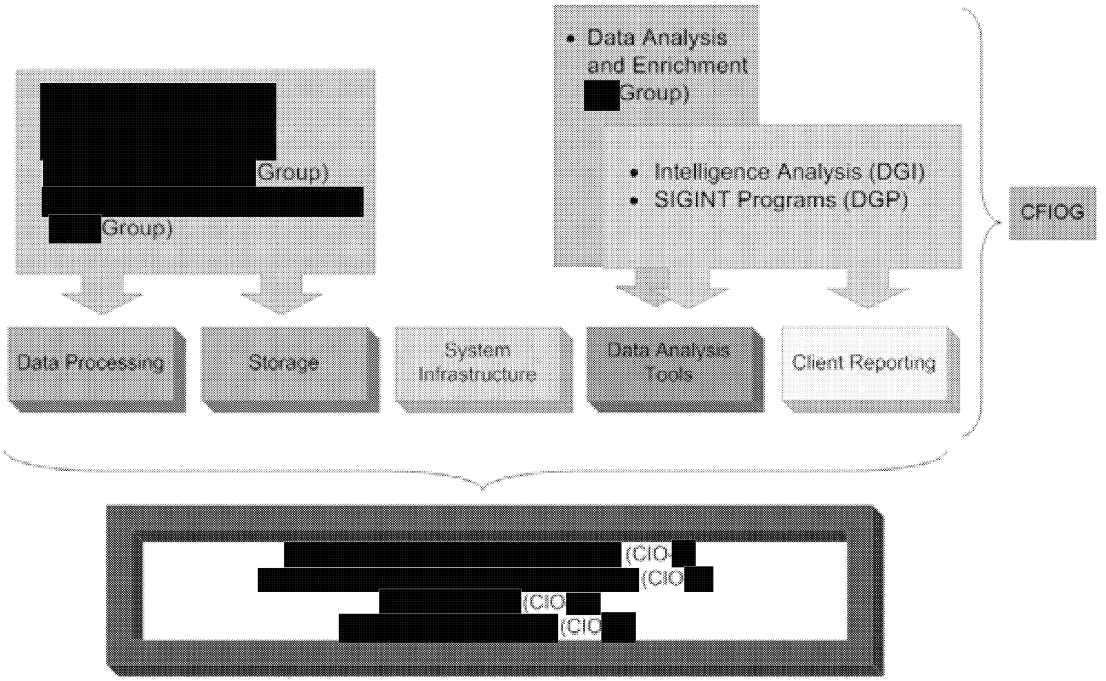


Figure 12.4

Figure 11.4 illustrates the role that SSD plays within the SIGINT community. As shown, there are many different priorities to be maintained to facilitate the smooth operations of SIGINT. CIO plays a crucial role in ensuring that systems run smoothly, protecting and monitoring SIGINT systems, managing and improving new systems, and maintaining the architecture within which SIGINT operates. SSD works with for systems and applications; and

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 13

Intelligence Branch Overview

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

Part of the process of gathering and producing foreign intelligence is the analysis of the data that CSEC collects from communications signals. The Intelligence Branch, also called the Intelligence Directorate (DGI), within the SIGINT business line, is responsible for the provision of intelligence reports and activities in support of Government of Canada intelligence priorities. DGI's main operational responsibility is analysing and producing end-product reports (EPRs). This chapter will provide an overview of the work of the Intelligence Branch, the various reporting lines and priorities, as well as a brief introduction to the work that is put into an intelligence report, as a Government of Canada (GC) client would receive it.

Recall the National SIGINT Priorities List (NSPL) in Chapter 5, the Standing Issues column provides a glimpse into how the Intelligence Branch has been organized, and the Watching Briefs column show the specific priorities on which SIGINT is currently focusing its efforts.

The Intelligence Branch is divided into [redacted] groups, [redacted] of them are [redacted] – named [redacted] while the other [redacted] provide [redacted] – called the [redacted] group. Analysts working in DGI possess various linguistic, technical, and analytic skills. Many of them also develop specialized expertise through training and work experience on [redacted]

The [redacted] mandate is to deliver SIGINT services and products in support of the GC's requirements on targets. It is the [redacted] group in DGI. It consists of the following offices:

[redacted] – OFFICE OF COUNTER-TERRORISM

The Office of Counter-Terrorism consists of [redacted] offices, [redacted] SIGDEV) [redacted] has [redacted] teams, focused on [redacted] SIGDEV, respectively. [redacted] consists of [redacted] teams focused on the [redacted] The primary clientele are CSIS, RCMP and DND, as well as allied intelligence agencies and military bodies. Counter-Terrorism reporting has resulted in the [redacted] and helped save the lives of Canadian and allied personnel both in Canada and abroad.

[redacted]

[redacted] provides actionable intelligence on [redacted] issues. This Office is responsible for reporting on [redacted] The primary clientele are CBSA, DND, CSIS, and the RCMP.

[redacted]

This Office provides actionable intelligence on activity linked to the [redacted] reporting supports [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SUMMARY OF [redacted] GROUP RESPONSIBILITIES:

- Internationally-based and/or globally conducted security issues.
- Targets and priorities tend to change quickly.
- It supports the protection of [redacted] needs.
- A lot of reports are "building block" type which can take months to complete.
- Some areas have shift work [redacted]
- [redacted]

The [redacted] group consists of [redacted] teams: [redacted] The [redacted] offices focus on issues related to [redacted] cyber security, and liaises with Government of Canada departments and other business branches within CSEC to provide support and protection to Canada.

[redacted]

Working closely with CSIS and 5-eyes partners, the [redacted] team identifies and monitors threats from [redacted] As part of its IRRELEVANT [redacted] reporting often results in IRRELEVANT IRRELEVANT

[redacted]

This team works to identify the [redacted] threats. The reporting from this office helps to protect the Government of Canada [redacted] and members of this group frequently collaborate with ITS business branch to promote cyber security.

The [redacted] Group)'s mandate is divided along [redacted] lines:

[redacted]

The [redacted] team addresses issues linked to specific [redacted] targets. [redacted] covers [redacted] The team also focuses on [redacted]

[redacted]

The [redacted] team addresses Government of Canada foreign intelligence requirements from [redacted] The [redacted] teams address issues linked to support to military operations as well as [redacted] The current areas of [redacted] focus are: [redacted] In addition to monitoring [redacted] also provides support to the Canadian Forces and generates intelligence on [redacted]

[redacted] is comprised of [redacted] teams: [redacted] The [redacted] teams work in a matrix structure, where staff report to all Team Leaders (TLs) and can work on all issues covered by the section. Analysts from these teams work closely with CSEC's military counterpart at CFIOG to provide support to troops in-theatre. The [redacted] team covers [redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

SUMMARY OF [redacted] GROUP RESPONSIBILITIES:

- Primary clients are [redacted]
- IRRELEVANT
- The group reports on [redacted]
- Reporting supports Canadian forces in theatre.
- [redacted] Group provides surge efforts to support [redacted]

The [redacted] Group) consists of the [redacted] the [redacted] and the [redacted] The [redacted] focuses on developing and disseminating advanced techniques in acquiring [redacted] SIGINT data and knowledge. The [redacted] focuses on advanced techniques of [redacted] data and analysis throughout CSEC.

[redacted] INITIATIVES:

PROJECTS	SPECIFIC RESPONSIBILITIES
[redacted] Analyst Community of Interest	This community of interest (COI) brings together [redacted] Analysts from across DGI in order to resolve gaps in SIGINT capability or knowledge, share techniques and best practices for target development, and exchange information [redacted]
Advanced Metadata Analysis	[redacted]
[redacted] Development	
Business Analysis	
Liaison with NSA	
Open-Source Intelligence (OSINT)	Collects information from unclassified sources and analyzes it to produce usable intelligence (Open Source research and intelligence).
[redacted]	[redacted]
The Map Library/ Map Librarian	Builds relationships with other Government of Canada departments in order to access maps and imagery.

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] CAN HELP DGI ANALYSTS IN THE FOLLOWING WAYS:

- Produces [redacted]
- Supports SIGINT Access (DGA) activities such as [redacted]
- Liaises with 2nd Parties through the [redacted]
- Provides surge capability and guidance for [redacted]
- Develops [redacted]
- Trains CSEC employees on the use of [redacted] software for SIGINT analysis
- Creates [redacted] to provide quick and easy situational awareness and analysis
- [redacted]
- [redacted]

[redacted] OPERATIONS INCLUDE:

- Collection of [redacted]
- [redacted] based on DGI submitted requests,
- Collection of [redacted] and other resources helpful to SIGINT development,
- Develop or acquire software [redacted] and
- Create new [redacted] connections to new and existing data repositories and analytic platforms for DGI analysts.

SUMMARY OF [redacted] GROUP RESPONSIBILITIES:

- Leads tradecraft development for the Intelligence Branch
- Employee backgrounds range from [redacted] engineering, computer science, [redacted] and math to psychology, library science, and business administration
- Reporting produced is primarily metadata based
- Focuses on analytics, [redacted] and needs analysis
- Primary clients are Intelligence Branch analysts

The [redacted] **Group** supports the critical business functions of the Intelligence Branch through the activities of [redacted] and [redacted] Group also supports Canadian military [redacted] operations in theatre [redacted]

[redacted]

- Provides coordination and advice regarding Intelligence Branch resources, including budget projections
- Acquires and validates unique skill sets through recruiting, testing, and linguistic assessment
- Develops and refines analytic tradecraft skills through in-house training and orientation

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] - CLIENT SERVICES

- Provides support functions such as web maintenance and application development
- Supports the [redacted] application for CSEC reporting; application trouble-shooting, and client interaction
- Ensures access for CSEC analysts, CFIOG personnel, and GC clients to MANDRAKE, Canada's secured computer network
- Manages and provides support to Client Relations Officers

[redacted] PROGRAM

- Provides ongoing support to the Government of Canada [redacted]
- Created in February 2006, is responsible for the [redacted]

SIGINT DEVELOPMENT (SD OR SIGDEV)

Besides writing reports, analysts are also tasked to conduct SIGINT Development (SD). SD can be defined in the simplest terms as work in preparation of and leading up to successful FI-yielding [redacted] It encompasses signal analysis and development, research, network analysis, and target development. It is the art of defining (through analysis and investigative techniques) a comprehensive and definitive description of foreign targets' [redacted]

SD is conducted usually done on a new target, as identified by the analyst as having merit or having potential to provide FI, with approval from the Team Leader (TL). SD work is also done on existing targets to further enhance collection. Typically SD work includes:

- Researching SIGINT and Open Source intelligence and identify potential targets that would potentially produce FI;
- Identifying selectors and inputting them into [redacted]
- Contact-chaining selectors [redacted]
- [redacted]
- Analyzing traffic (both the communications content and metadata) collected through new selectors; and
- Updating and modifying the targeting with a view to obtain reportable FI.
- Conducting analysis of a target's [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

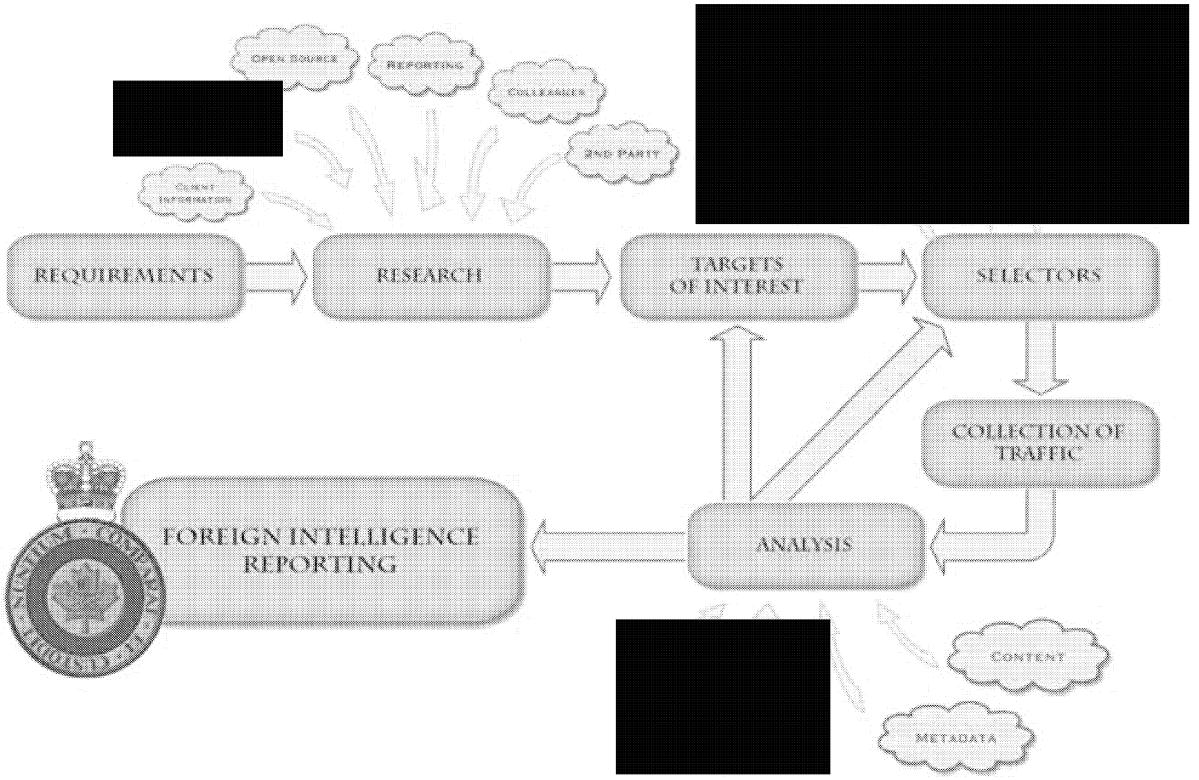


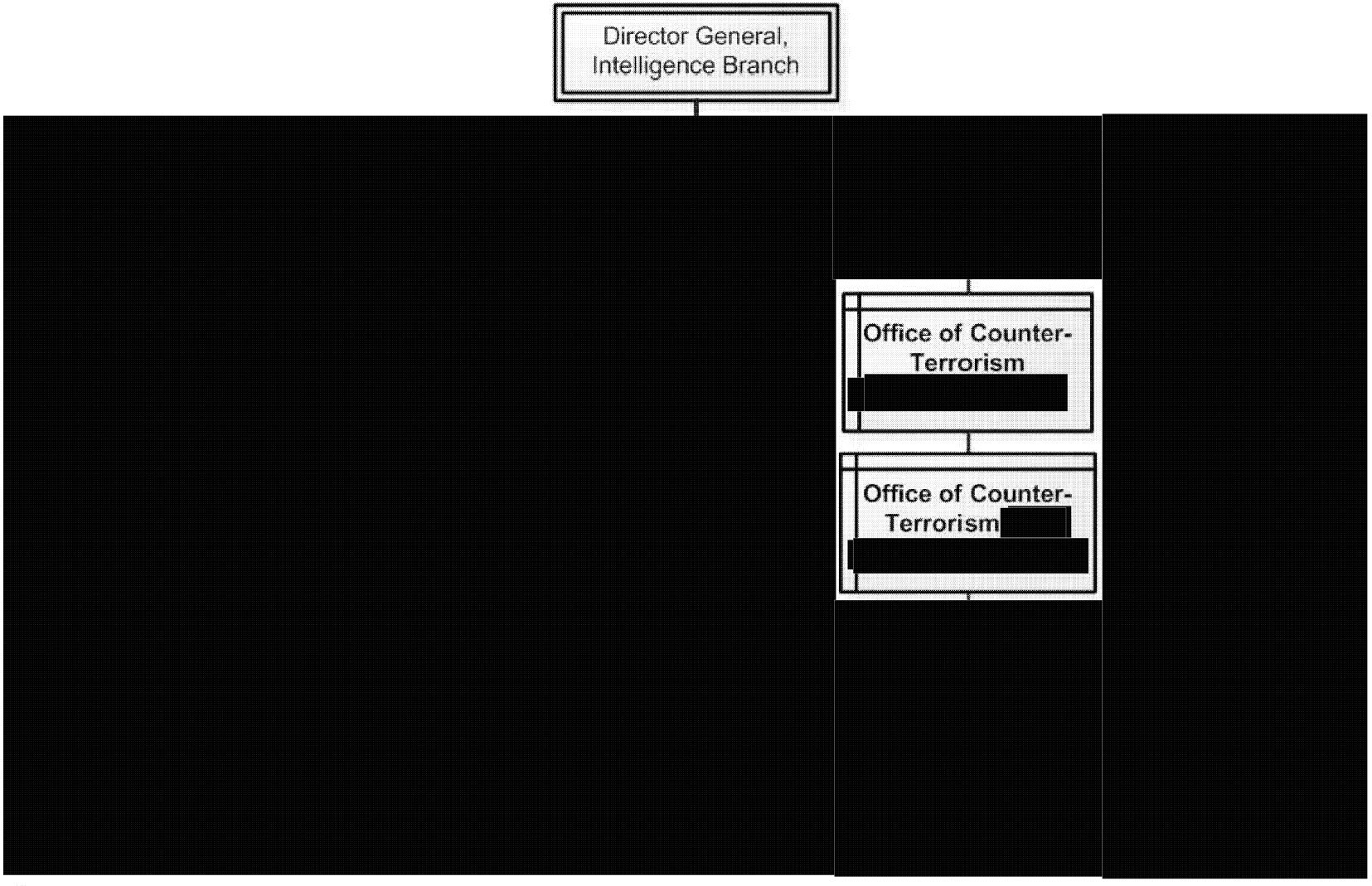
Figure 13.1

Figure 13.1 illustrates some of the work involved in conducting SIGINT development. Each team within the Intelligence Branch – and each analyst – will, with experience and expertise, establish a well-documented SD process [redacted] Different teams and target sets have different methods when it comes to approaching SD. What works for one team and one target may not necessarily produce the same results for another target.

SD involves the use of target tradecrafts developed by [redacted] group and collaborations with other areas across SIGINT and 5-eyes partners. [redacted] operations are sometimes resulted from SD efforts depending on the [redacted]

DGI Team Leaders are the core guide and the first line of support behind an analyst's SD work. [redacted] Analysts and Specialists also provide help on various SD challenges encountered by DGI analysts.

Intelligence Branch – Fiscal Year 2010/2011



Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

PRODUCTION AND DISSEMINATION OF SIGINT REPORTS

The end goal of SIGINT is the dissemination of intelligence. CSEC not only produces intelligence reports, but also ensures that the clients receive those reports in a timely fashion. To this end, SIGINT relies on a team of Client Relations Officers (CROs), who are responsible for identifying intelligence reports of interest to various senior clients within the GC, and delivering these EPRs. Other consumers of SIGINT may have their own accounts on [redacted] and conduct their own searches.

Key clients within the Government include:

- Department of National Defence (DND)
- Department of Foreign Affairs and International Trade (DFAIT)
- Canadian Security and Intelligence Service (CSIS)
- The Privy Council Office (PCO)

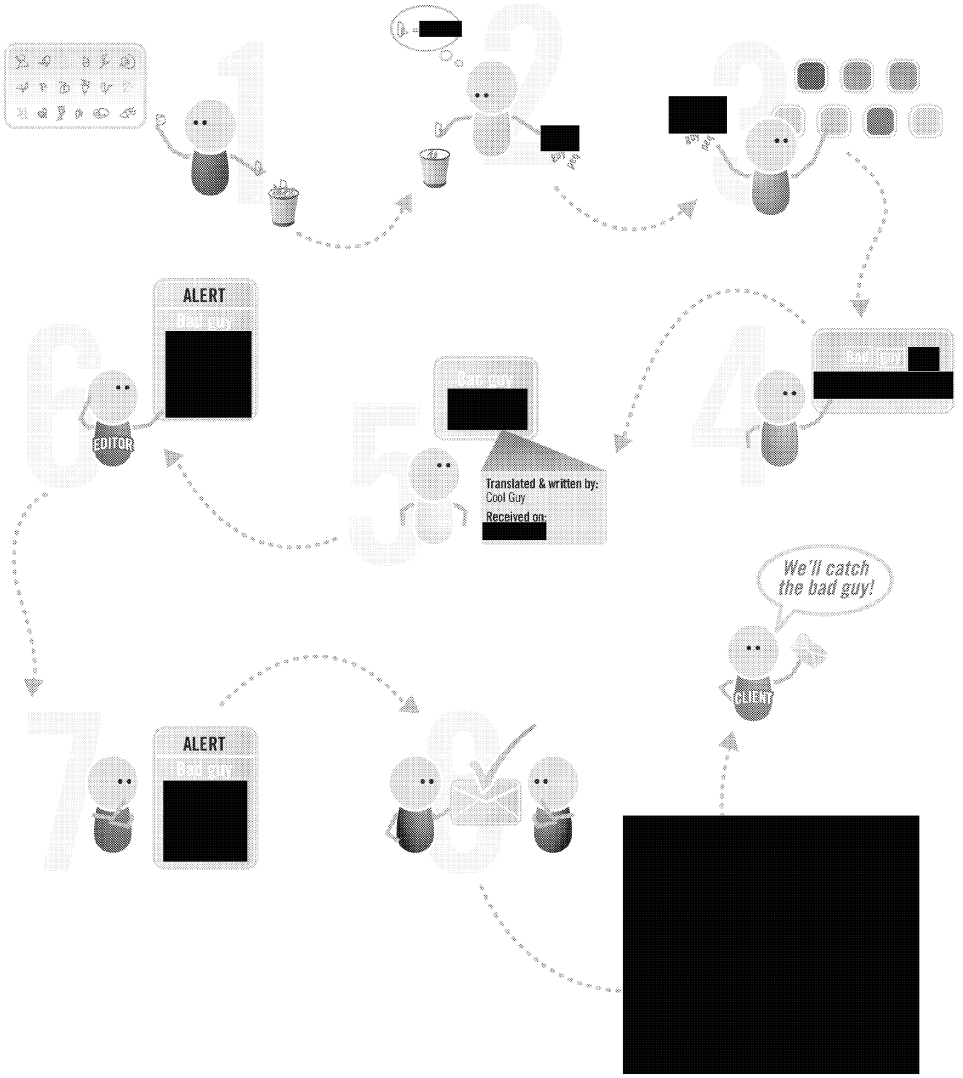
Other clients who receive CRO service include:

- Canadian Food Inspection Agency (CFIA)
- Industry Canada (IC)
- Canadian Border Services Agency (CBSA)
- Health Canada (HC)

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Analysts in DGI, regardless of the reporting line he/she works for, follow a similar path in the production of an EPR. Below is a generalized step-by-step look at the process of producing SIGINT intelligence reports in CSEC.

REPORT PRODUCTION ROADMAP



Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

STEP	ACTION	DESCRIPTION
1	Scan traffic	The analyst is responsible for scanning and annotating traffic (if necessary). In order to determine if a piece of traffic is reportable, the analyst will ensure the topic falls under foreign intelligence, meets the clients' need and would not be available through open sources.
2	Translate the traffic (if necessary)	If the traffic is in a foreign language, a linguist analyst produces a polished translation that will be checked by a co-worker.
3	Research	The analyst consults previous reporting and open source resources in order to bolster the information contained in the traffic. This may be used to provide context or to clarify information that is not clear in the traffic. Information in a report not derived from SIGINT is called collateral, and can be classified (e.g. from HUMINT reporting) or unclassified from open source.
4	IRRELEVANT	
5		
6		
7		
8	Obtain the necessary sign-off(s)	If required, a CSEC senior manager IRRELEVANT will receive the report package and review it to ensure all policy concerns are addressed before authorizing the release of the report.
9	Release the report	Once authorized for release, the analyst releases the report using [redacted]

Table 13.2 – Overview of the report-writing process.

Table 13.2 provides an overview of the steps involved in the production of a SIGINT intelligence report. It is important to note that while the analyst relies on his/her colleagues, supervisors, and SIGINT management in the process of report-writing, the analyst's responsibilities are numerous, from translating (or transcribing, if needed) the intercept, collecting collateral and related data for contextual information, IRRELEVANT and releasing the report. As was stated above, the actual process will differ from one analyst to another and from one reporting line to another. Nevertheless, the basic steps have been outlined here to provide a more comprehensive look at how reports are generated.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Listed below are several scenarios designed to provide some examples of the specific topics that each group within DGI would address and their respective contributions to the analysis and production of SIGINT reports. To understand and contextualize what has been explained in this chapter about the activities within DGI, several questions should be considered in conjunction with the scenarios:

- Who are the clients likely to coordinate/ request for SIGINT on this topic?
- What linguistic support might be needed? Who would coordinate and respond to this need?
- Which reporting line does this fall under [redacted] Why?
- What legal considerations are there?
- How might the [redacted] Group or the [redacted] Group provide support on this issue?

SCENARIO A

[redacted]

SCENARIO B

[redacted]

SCENARIO C

[redacted]

SCENARIO D

[redacted]

SCENARIO E

[redacted]

SCENARIO F

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 14

SIGINT Collaboration using Web 2.0

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

As technological advances continue to present new challenges for SIGINT, analysts within CSEC must learn to take advantage of the tools we have, and to adapt existing applications in order to maximize their use to [redacted] This chapter will provide some key features of Web 2.0, and discuss how CSEC [redacted] adopted Web 2.0 concepts and tools to further knowledge-sharing and collaboration. The advantages and disadvantages of the current social software tools, like wikis, blogs, mashups, and social networks will also be covered.

Web 2.0 has two components, one social and the other technological. The social component is the idea that the web should focus on people, rather than documents. Instead of only connecting people to information, the web would connect them to each other. This encourages rich information exchange and enables ad-hoc collaboration with anyone, anywhere. Social applications associated with Web 2.0 (such as MySpace and Facebook) reduce the need for wide email distribution lists to convey information to a large audience and create an environment for richer interactions.

Within SIGINT, the need to break free of silos and work in a collaborative environment has been encouraged by CSEC's strategic policies:

- The workforce will soon be shrinking due to the massive retirement of baby boomers; and we need more environments that allow generations to interact
- The people we hire increasingly expect to work in an environment that allows for creativity and social connectivity
- This change of corporate culture towards greater collaboration will necessitate usage of new systems/tools and education

There is a variety of open-source tools which SIGINT is adopting for internal use, including:

- Wikis: an online knowledge-sharing tool (ex. Wikipedia.org, the collaborative encyclopaedia);
- Blogs: online journal which can be organized by an individual or community of interest (ex. LiveJournal, Blogger);
- Microblogging: exchange of quick, frequent answers to short questions (ex. Twitter or status update in Facebook);
- Social bookmarking: collective repository that users can store, organize and share their online bookmarks (ex. Delicious);
- Social networking sites: web-based services that allow individuals to construct a public or semi-public profile within a bounded system (ex. MySpace and Facebook).
- Forum: An internet forum, also known as a bulletin board, allows people to post messages and comment on other messages.

Wikis allow analysts to share information, questions and discussions on issues relating to SIGINT targets and tradecraft within the secured computer network environment.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Table 14.1 shows the various wikis available to CSEC and the various accesses that SIGINTers in CSEC have to read and/or edit the content of the wikis.

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

One of the key features of wikis is the ability for different users to input, change, and save information in the same platform without using multiple copies of a document, as traditional emails would create in a collaboration setting. Figure 14.2 depicts how wikis decreases the amount of transfers between users.

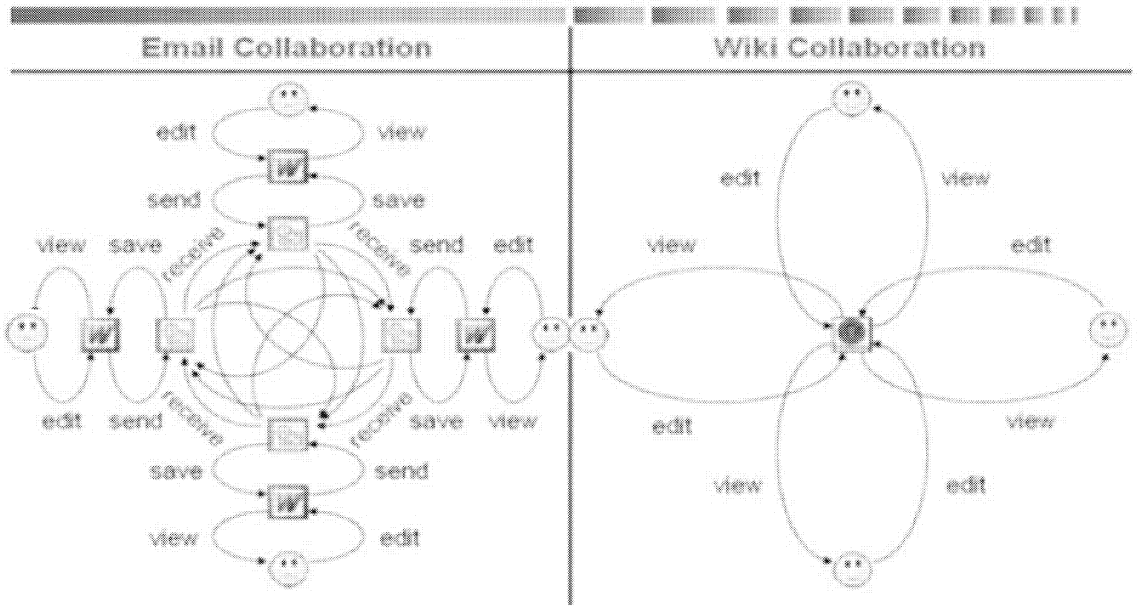


Figure 14.2

As CSEC employees, when searching for SIGINT-related information, it is recommended that you start at the [redacted]. The [redacted] provides the CSEC perspective on various articles, and is written largely by CSEC SIGINTers.[redacted]

An internet forum, also known as a bulletin board, allows people to post messages and comment on other messages. A thread, also known as a topic, is a collection of posts displayed from oldest to newest. A thread can contain any number of posts, including multiple posts from the same people, even if they occur afterwards. Forums differ from chat rooms and instant messaging in that forum participants do not have to be online simultaneously. Forums allow for asynchronous communication. CSEC has had forums for many years and they are very popular across the organization.

1. Website can be found at [redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

A new SIGINT forum, the [redacted] was launched in 2010 to be used as a resource for CSEC SIGINT analysts to have SIGINT-related questions dissiminated to the community with the aims to create discussions and possible solutions. CSEC analysts need to log in with [redacted] authentication and integrees can also participate. But, be aware that the forum is [redacted] accessible and [redacted] content should not be posted. Posts must be relevant to SIGINT, ITS, National Security or tradecraft-related information . Before posting a question on [redacted] analysts are recommended to search the [redacted] as well as the CSEC and various [redacted] home pages to see if your question has been answered elsewhere. When solutions are found on the forum, analysts are being encouraged create or update an appropriate [redacted] article with the information as the [redacted] is much better suited for documenting tradecraft knowledge.

Blogs are commonly used as online journals authored by one main user where entries or posts can be recorded. Community blogs serve as a place for members of a specific interest community to discuss common issues. There are a couple of key features of blogs that make them different from wikis: with a blog, the most recent post is usually displayed first, and older ones are archived in case they need to be retrieved. Many blogs also have feedback sections where readers can contribute comments and questions. Blogs usually have a more informal tone than wikis as blog postings tend to express personal sentiments.

In a professional context, blogs can be useful communication tools. They can be used to let people know the progress of different initiatives, provide descriptions of events (meetings, conferences, etc), or give them an insight into a particular job. They can also be used to educate people about a topic or service. The CSEC 2.0 corporate web has a blogging service intended for all employees which is [redacted] accessible ([redacted] cannot reply or create entries [redacted] CSEC employees also have access to [redacted]

Microblogging is a form of blogging. Micro-blogging differs from traditional blogs in that its content is much more concise and consist of a sentences, an image or embedded video. Microblogging are useful as a method to make widely known general updates, breaking news, reminders or feedback. People can also reply to micro-blogging comments in a similar fashion to blogs. Open-source micro-blogs like the Internet website Twitter can be updated using people's mobile phone (with SMS capability), which allows for updates to be posted quickly and remotely. The CSEC 2.0 corporate web has a micro-blogging capability which is known internally as Tweets. CSEC employees may find it useful to track a DGs activity by following their updates via their Tweets. [redacted]

Social bookmarking, unlike wikis, blogs, and micro-blogs, allows users to store, organize, and manage bookmarks of web-pages. It is a personal collection of bookmarks that are categorized with descriptive tags and these bookmarks are shared with other users to facilitate the research of new sources of information on similar topics. CSEC employees have access to [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

One of the most popular Web 2.0 tools in recent years has been social network sites (SNS), which are web-based services allow users to construct a profile (public or semi-public) within the system; identify and connect with a list of other users; and view connections made by others within the same SNS. Currently, [redacted] Table 14.3 illustrates some of the advantages and disadvantages of various Web 2.0 tools, including wikis, blogs, micro-blogs, social bookmarking; mashups, and social networking sites.

STRENGTHS	LIMITATIONS/CHALLENGES
Wikis + wiki syntax is easy to learn + content appears instantaneously + articles are created by the community through collaboration + people (authors) are attributable + content is usually unique (not found on intranets/ websites) + people can discuss topics on wikis + it is easy to revert changes	Wikis - it is a challenge to keep content and links current - articles are perpetually "work in progress" - all members can add or edit the work of others, which may cause disputes over content
Blogs + comment feature allow people to provide feedback on postings + all entries are dated (easy for users to determine the currency of information) + blogs can build the profile of the writer	Blogs - it is more difficult to piece together disparate information (blogs are more restricted to one conversation thread) - blogs are easy to start, but difficult to maintain - content may not always be up-to-date
Micro-blogs + great tool for getting a sense of news and happenings at the moment + users can choose contacts to receive the information and updates + users can access micro-blog posts quickly	Micro-blogs - micro-blog posts tend to be sarcastic, silly, non-technical (compared to blogs or wikis)
Forums + People participating in a forum may create social networks and interest groups for a topic made from the discussion + Forum postings can either be brief and straight to the point or lengthy, depending on the topic + The process of posting to an internet forum can become a mental exercise that can help clarify one's thoughts and direction	Forums - A user might send the same post to multiple forums, which causes problems since forums lack the ability to link these posts. Therefore, replies in one forum will not be visible to people reading the same post in another forum

2. For more information on [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

STRENGTHS	LIMITATIONS/CHALLENGES
Social bookmarking + bookmarks provide more relevant search results than search engines since the pages are tagged by users + tool ranks resources based on how many times it has been bookmarked by other users + social bookmarking allows users to organize and share a large number of bookmarks	Social bookmarking - there are no standardized set of keywords or tags to categorize bookmarks - there are no standard structures for tags - there are no mechanisms for users to indicate the hierarchical relationships between tags
Social Networking Sites + social networks improve the ability for people to advance professionally by finding, connecting, and networking with others + users can customize their privacy settings on individual profiles and workspaces + social networking sites provide an environment within which other social services can be used (ex. blogs)	Social Networking Sites - there is potential for duplication of efforts occurring with corporate blogs and wikis - most people use social networking sites for socializing, and not for professional/ work-related collaborations

Table 14.3 – Advantages and disadvantages of Web 2.0 tools

Within CSEC, the CIO is spearheading a number of Web 2.0 initiatives known as CSEC 2.0. CSEC 2.0 includes a new, modernised web interface with many Web 2.0 services such as blogging, micro-blogging, video sharing [redacted] and multimedia galleries. The aim is that students will be able to use the CSEC 2.0 tools to collaborate, communicate and share information across the organization.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

In addition, there is a chat tool, called [redacted] Everyone with access to the CSEC [redacted] Currently, the highest chat classification is TOP SECRET// COMINT. In the future, there are plans to create chat rooms to enable conversations at a [redacted] with [redacted]

Having now discussed a number of Web 2.0 tools available today, as well as the strengths and weaknesses of these tools, this chapter will now compare these tools in terms of its use. Figure 14.4 shows the spectrum of synchronicity and formality of the various tools.

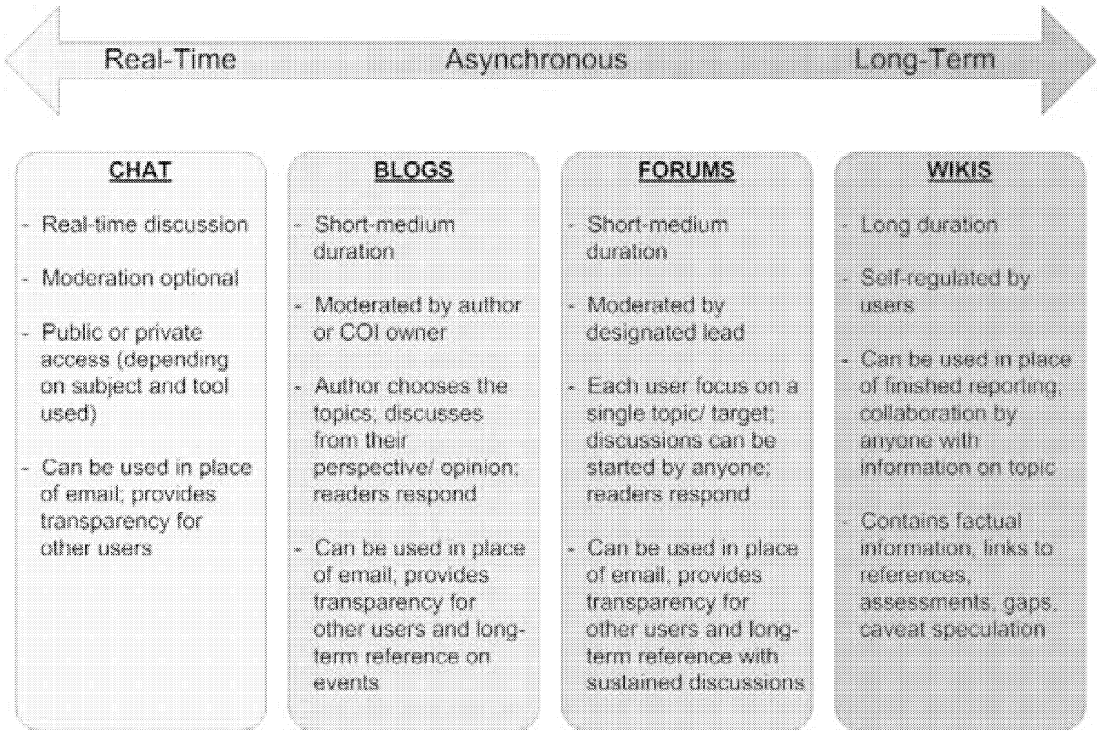


Figure 14.4

Each of the tools mentioned has its strengths and its limitations, and it is up to the user to decide which format is best to communicate the information. The decision to use a particular tool depends on the on the information a user wants to communicate, and the extent to which the information will be read and/or edited by other users/authors. There is no absolute right way to use Web 2.0 tools, and it should be noted that Web 2.0 is more defined by an attitude of sharing and collaborating than the technology.

For more information on Web 2.0 accesses, URLs, and other useful tips, please see the Appendix.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

chapter 15

Introduction to D2 and OPS-1 Policy

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

DISCUSSION QUESTIONS

1. Are Canadians anywhere in the world, or just in Canada, protected from being targeted by CSEC? Is that protection in place for corporations? What about Honorary Citizens?
2. If someone is trying to get a visa and is not currently in Canada, what is their official status? How does someone become a Permanent Resident?
3. Can we store information about non-Canadians in Canada? Can we store information on Canadians? Are there limits or rules about keeping these kinds of information?
4. IRRELEVANT
5. If the leader of a terrorist group that is planning an attack is thought to be [redacted] and then is found to be a Canadian, can CSEC target him? How do we treat dual citizens?
6. If CSEC can't target someone, can we ask a Second Party to do it?
7. Is a [redacted]
8. When a foreign target visits Canada, can the person continue to be targeted by CSEC? If not, when can this person be re-targeted?
9. When are Canadian Forces personnel bound by CSE's mandate? The Canadian Forces operate under 'Royal Prerogative' – what does that mean?
10. How are Canadian identities protected in Second Party reporting?

NOTES ON THE ONLINE OPS-1 BRIEFING

[redacted]

OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities, is the policy instrument that outlines the measures that must be in place to protect the privacy of Canadians and ensure lawfulness while CSEC carries out SIGINT and ITS activities, in accordance with CSEC legislation. This chapter will review:

- CSEC authorities and the policy framework;
- Ministerial Directives and Ministerial Authorizations;
- Key elements of the OPS-1 policy; and
- Two selected procedures within the Operational Policy suite of policy instruments.

OPS-1 can be found by navigating (on the internal, secured computer system) to the Operational Policy website from the CSEC homepage (begin by choosing DGPC from "Business Lines" at the top of the page and then follow the links to Operational Policy), or by going directly to the URL for Operational Policy instruments at: [redacted]

An overview of OPS-1 is mandatory for all staff working in SIGINT, since the document is essentially a "bible" for activities conducted under CSEC's mandate. CSEC must ensure all operational staff members understand and comply with OPS-1, since the measures it sets out serve as a means to ensure compliance with the law. CSEC's activities are subject to both internal and external review, and the CSEC Commissioner reports on its reviews of CSEC activities to the Attorney General and the Minister of National Defence.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

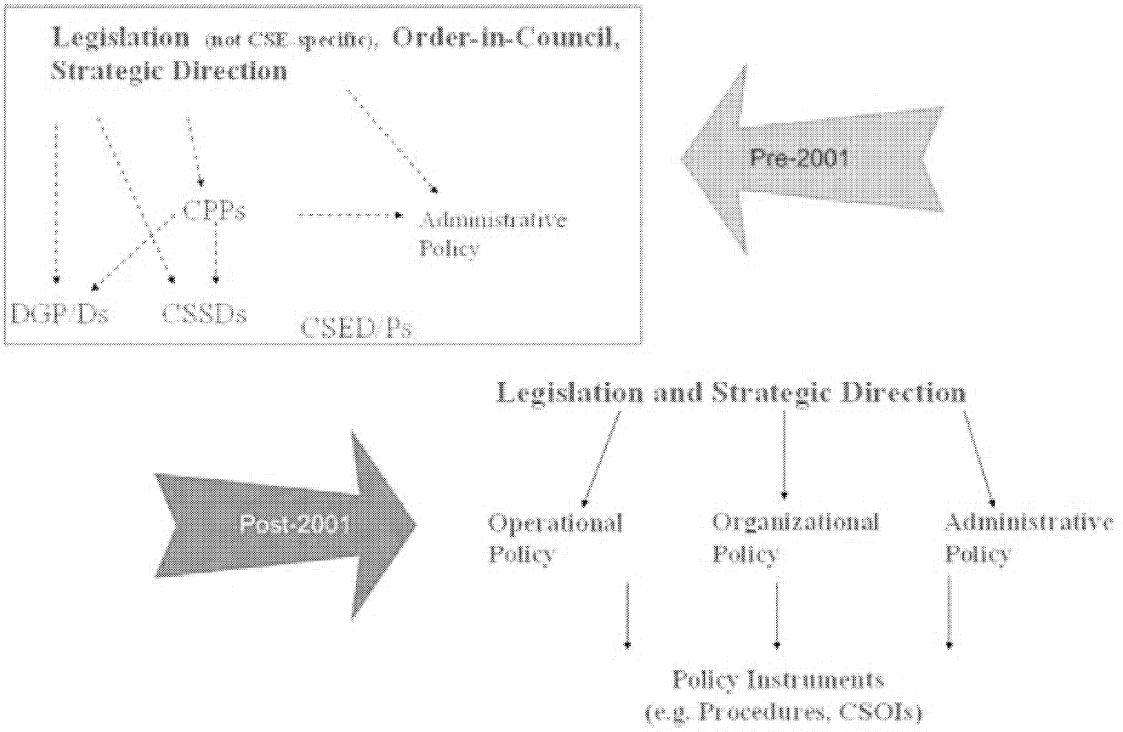


Figure 15.1

Figure 15.1 illustrates the SIGINT Policy framework as it existed prior to 2001 compared to the way it looks today. Because of the impact of 9/11, CSEC was able to acquire new authorities to conduct SIGINT activities to protect Canadian national security. With that increased responsibility, there arose a need for new accountability measures, and one of the things streamlining CSEC's policy framework does is to enable better compliance and a more straight-forward review of accountability.

THE CSEC MANDATE

To understand the relevance of OPS-1, first we will review the CSEC Mandate, as it is stipulated in the *National Defence Act* (NDA):

A) to acquire and use information from the Global Information Infrastructure for the purpose of providing foreign intelligence, in accordance with GC intelligence priorities;
B) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC; and
C) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

RESTRICTIONS ON MANDATE ACTIVITIES

While CSEC has the authority to carry out these activities, there are also key restrictions that are in place to ensure the privacy of Canadians and to ensure lawfulness in the conduct of CSEC activities:

GENERAL RESTRICTION (S.273.66 NDA)

CSEC may only undertake activities that are:

- Within its mandate;
- Consistent with any ministerial directives; and
- Consistent with ministerial authorization if required.

RESTRICTIONS ON ACTIVITIES CONDUCTED UNDER PARTS "A" AND "B" OF THE CSEC MANDATE:

- Activities shall not be directed at Canadians anywhere or at any person in Canada, and
- Activities are subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

(Note: we do not have to protect the privacy of non-Canadians in Canada. This means that in reports we can name people who are in Canada and who fall into certain categories like holding work or student visas, or who are illegal immigrants.)

IRRELEVANT

PRIVATE COMMUNICATIONS

In addition to the NDA, other pieces of legislation, like the *Privacy Act* and the Criminal Code, affect CSEC's activities. For example, the Criminal Code protects the private communications of Canadians. Private communications are defined in the Criminal Code as: 'any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada, and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it'. (Criminal Code, section 183) The test for private communications is based on GEOGRAPHY, not nationality. Below are some examples of private communications:

- Joe in Toronto calling his brother Jack in Montreal (because both parties are in Canada).
- [redacted] (because the recipient is in Canada).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Alternatively, there are non-private communications. The same rule regarding geography (mentioned above) applies. Below are some examples of non-private communications:

- [redacted]
- [redacted]

In the OPS-1 context, the examples in the last two bullets above are referred to as "Communications of Canadians outside Canada."

MINISTERIAL DIRECTIVES AND MINISTERIAL AUTHORIZATIONS

The NDA has paragraphs referring to Ministerial Directives (MDs) and Ministerial Authorizations (MAs). MDs are written direction to the Chief, CSEC respecting the implementation of CSEC's duties and functions. MAs are authorizations provided in writing by the Minister of National Defence to CSEC to ensure that CSEC is not in contravention of the law if, in the process of conducting certain foreign intelligence or IT Security activities, it should intercept private communications.

An MA may be for Foreign Intelligence or IT Security activities, but not both. They are valid for one year but may be renewed upon application by the Chief, CSEC to the Minister. MAs may apply to an activity (e.g. in IT Security), or a class of activities (e.g. the [redacted] Program in SIGINT).

If CSEC is bound by the provisions of the *Privacy Act* and the Criminal Code, but CSEC is also responsible for collecting and reporting on communications that may sometimes contain information related to Canadians, how are these two ideas reconciled? They are reconciled by having measures in place to protect the privacy of any information incidentally collected about Canadians.

The requirement to have measures in place to protect the privacy of Canadians has both legal and Ministerial origins. The legal requirement comes from the NDA, which states that activities under parts "A" and "B" of the CSEC mandate are subject to measures to protect the privacy of Canadians. The Ministerial requirement is found in both MDs and MAs. The MD on Privacy states that, "CSEC may retain and report information on or of Canadians subject to stringent criteria and appropriate measures in place for handling, retention and destruction of this information". In addition, a pre-condition for the granting of an MA is that, "… satisfactory measures are in place to protect the privacy of Canadians…".

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

DEFINITION – "CANADIAN"

While it may seem simple, on the surface, to distinguish Canadians from non-Canadians, there can be grey areas, but within the business of SIGINT, legal requirements stipulate that we must be able to clearly identify communications that are considered "Canadian" compared to those that are not. So, what exactly are "Canadian" entities? "Canadian" refers to the following:

- Canadian citizens;
- Permanent residents (as defined in the Immigration and *Refugee Protection Act*);
- Corporations incorporated under an *Act* of Parliament or of the legislature of a province; and
- Unincorporated organizations, which are granted the same protection as is given to incorporated organizations.

(Note: A corporation that is incorporated in another country is NOT Canadian, even if it is a subsidiary of a Canadian corporation).

If information about Canadians is included in SIGINT reports, naming conventions are put in place to conceal any personal information about a Canadian person (as described in the *Privacy Act*) or any information about a Canadian corporation or organization. Naming conventions will be covered later in this chapter.

DEFINITION – "FOREIGN INTELLIGENCE"

Another key to understanding OPS-1 is the meaning of "foreign intelligence", which is defined as, "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security." This does not include information where one of the communicants is a Canadian or Second Party[1] government entity. Below are two examples that show this difference:

- [redacted]
- [redacted]

OPS-1, PROTECTING THE PRIVACY OF CANADIANS AND ENSURING LEGAL COMPLIANCE IN THE CONDUCT OF CSEC ACTIVITIES

OPS-1 is the primary policy instrument implemented in response to the NDA and Ministerial Direction. The document reflects the CSEC statutory mandate and authorities and applies to both the SIGINT and IT Security activities of CSEC. The measures it details to ensure legal compliance and safeguard the privacy of Canadians in the use and retention of intercepted information must be applied by anyone conducting activities under CSEC authority.

1. i.e. US, UK, Australia or New Zealand

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

There are several specific key elements of OPS-1 that are of note to staff in SIGINT, outlined below:

KEY ELEMENT #1: LEGAL COMPLIANCE

- CSEC acts in strict compliance with all laws of Canada
- CSEC may only undertake activities that are
- Within its mandate;
- Consistent with ministerial direction; and
- If Ministerial Authorization is required, consistent with that authorization.
- If CSEC unintentionally or inadvertently collects or acquires private comms, communications of Canadians located outside Canada, or information about Canadians, it will use and retain this intercept according to OPS-1.

KEY ELEMENT #2: PRIVACY AND TARGETING

Under part "A" of the CSEC mandate

All selectors and methods used in collection and acquisition activities shall be:

- Directed at foreign entities* located outside Canada; and
- Consistent with GC intelligence priorities.

*Does not include US, UK, Australian or New Zealand entities

IRRELEVANT

KEY ELEMENT #3: PRIVACY AND ACQUISITION

Under part "A" of the CSEC mandate

Part I – In order for private communication or traffic containing information about a Canadian to be used, it must first meet the essentiality test. The essentiality test asks if the information is essential to international affairs, security or defence, and if it meets a GC intelligence requirement.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Part II – While scanning traffic, if CSEC SIGINT analysts identify a private communication, a communication of a Canadian located outside Canada, or observe a communication which contains information about Canadians, then the traffic must be destroyed (i.e. annotated for deletion), UNLESS it:

1) Is foreign intelligence as defined by the NDA;
2) Is essential to protect the lives or safety of individuals of any nationality, using criteria outlined in OPS-1, or
3) Contains information on serious criminal activity relating to the security or Canada, using criteria outlined in OPS-1.

IRRELEVANT

Canadian involvement in intercepted communications

If an analyst recognizes traffic where both the originator and the recipient are Canadians, both originator and recipient are in Canada, or one communicant is in Canada and the other is a Canadian abroad, THEN…

- Traffic must be annotated for deletion;
- All associated selectors must be reviewed; and
- SIGINT Programs, Oversight and Compliance (SPOC) should be notified for accountability.

If selectors continue to yield only these types of communications and they do not meet the essentiality test, then the analyst must notify SIGINT Programs, [redacted] to have the selector removed, or modify the targeting.

Very rarely, there are instances where a Canadian or a person inside Canada is inadvertently targeted. OPS-1 provides guidelines on how an analyst should handle these situations. The steps are to:

- De-target the selector;
- Annotate any existing traffic from the selector for destruction;
- Cancel any end-product reports based on the traffic; and
- Notify SPOC and Operational Policy (D2) so that these occurrences can be tracked.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Solicitor-client communications

There is one particular type of communication that needs further explanation and attention here: solicitor-client communications. Most people are aware that communications with one's legal representative are subject to confidentiality under the law. Canadian solicitor-client communications must be handled in particular ways when they are seen.

Under part "A" of the CSEC mandate

The following steps must be taken:

- The communication must be annotated for destruction unless it contains foreign intelligence;
- If it contains FI, it must be annotated and brought to the attention of analyst's Director;
- The Director obtains legal advice from the CSEC Department of Legal Services (DLS); and
- The reporting area must follow the legal advice as provided by DLS.

IRRELEVANT

KEY ELEMENT #4: PRIVACY AND FI REPORT FOCUS

CSEC SIGINT reports must focus on the activities, capabilities and intentions of foreign intelligence targets; information about Canadians should only be included in SIGINT reports if it meets one of the three criteria mentioned above:

- Is foreign intelligence as defined by the NDA;
- Is essential to protect the lives or safety of individuals of any nationality, using criteria outlined in OPS-1;
- Contains information on serious criminal activity relating to the security or Canada, using criteria outlined in OPS-1.

IRRELEVANT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

KEY ELEMENT #5: REPORT RELEASE AUTHORITY

Senior CSEC management must sign as the release authority for SIGINT reports based on a private communication, a communication of a Canadian outside Canada, or a communication containing information about Canadians IRRELEVANT IRRELEVANT

KEY ELEMENT #6: PRIVACY AND STORAGE

Intercept used in reports or retained as background information must be securely stored. Hard copies of such intercept should be kept to a minimum and must be stored in a locked container when not in use. Soft copies outside of traffic databases must be stored in electronic folders with limited access.

Other Operational Policy Instruments

An overview of the key elements of OPS-1 was presented in the above paragraphs. But in addition to this cornerstone policy, the Operational Policy suite of policy instruments includes OPS-1-7, SIGINT Naming Procedures, and OPS-1-1, Procedures for the Release of Suppressed Information from SIGINT Reports.

OPS-1-1, Procedures for the Release of Suppressed Information from SIGINT Reports, stipulates that

- information suppressed from SIGINT reports is stored securely (within [redacted], with limited access;
- suppressed information may only be released by Operational Policy to clients if a request meets specific criteria outlined in OPS-1-1; and
- senior management approval is required for the release of suppressed information to GC clients with law enforcement mandates, or to Second Parties.

OPS-1-7, SIGINT Naming Procedures, articulates the ways in which identities of Canadian, as well as Second Party, entities must be handled when their inclusion in SIGINT reports is essential. Identities of Canadian and Second Party entities must be replaced by generic terms (e.g. "named Canadian 1"). Identities may only be referenced in SIGINT reports if necessary to understand the foreign intelligence, so no gratuitous references should be made. Case-by-case naming exceptions are permitted (either for individual reports, or for specific operations), with Senior CSEC management approval (e.g. in threat-to-life situations). In certain circumstances, with the proper approvals, a blanket naming exemption for a series of reports is possible (contact Operational Policy for more information).

Other Operational Policy Series include:

- OPS-2 – Liaison and Cooperation
- OPS-3 – Sensitive Operations and Activities
- IRRELEVANT
- OPS-5 – Security/Control of SIGINT, and
- OPS-14 – TK Procedures.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

"Targeting" and "Naming"

Chapter 12, Introduction to [redacted] described the difference between targeting and tasking for the purposes of collection (vice analysis). Within the SIGINT policy framework, the terms "targeting" and "naming" must not be confused with one another. Targeting is determined by either nationality or location. We don't target Canadians anywhere, nor do we target anyone in Canada. Naming is determined by nationality only. We don't name Canadian or Second Party entities, but we can name some categories of non-Canadians in Canada. Below are some examples that show the difference between targeting and naming:

- [redacted]
  Named in SIGINT Reports? YES
  Targeted by CSEC under part A of the CSEC mandate? NO (only possible under CSIS authority)
- [redacted]
  Named in SIGINT Reports? YES
  Targeted by CSEC under part A of the CSEC mandate? NO (only possible under CSIS authority)

CONCLUSION

To conclude this introduction to OPS-1, it is important for all SIGINT staff to remember that:

- Under parts "A" and "B" of the CSEC mandate, CSEC cannot direct its activities against Canadians anywhere or against any person in Canada;
- IRRELEVANT
- By law, CSEC is obliged to protect the privacy of Canadians during the course of its activities, and
- It is important for CSEC staff to read OPS-1 annually, and always refer to the most up-to-date version.

Like any document, OPS-1 is subject to regular updates and amendments, which are designed to ensure that the policies in place align accurately with the law and Ministerial direction. The document, in its entirety, can be found at [redacted] All CSEC staff members are encouraged to become familiar with the key elements within OPS-1, and to especially note those sections that are most relevant to their work activities.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

appendix A

The World of SIGINT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

INTRODUCTION TO SIGINT

Earlier this morning, the various forms of SIGINT were discussed. Below is a review of the 3 forms of SIGINT:

- ELINT – Electronic Intelligence
- FISINT – Foreign Instrumentation Signals Intelligence
- COMINT – Communications Intelligence

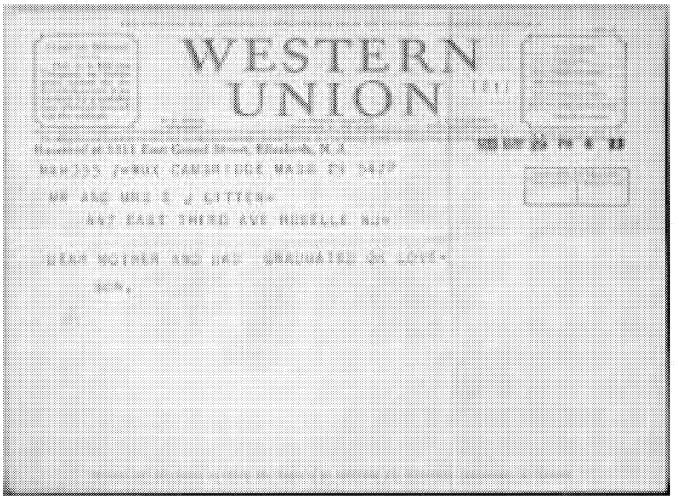
Officially, Signals Intelligence can be defined as: "the collection and analysis of intentional signals for both communication (i.e. telephone conversations) and non-communications (i.e. radar signals), and unintentional information (electromagnetic signals)". Some examples of SIGINT include intelligence derived from: phone calls, faxes, e-mails, [redacted] Other examples like beacons, telemetry (guiding systems on test rockets), and Morse code may not be things you encounter everyday.

HISTORY OF SIGINT

SIGINT is a modern phenomenon. Before signals, there was only COMINT (communications intelligence) because communications can only take place either by correspondence, or during face-to-face encounters. Once people started communicated with each other in ways and there were signals that carried the communications content from the sender to the receiver, there were signals to intercept, which is SIGINT.

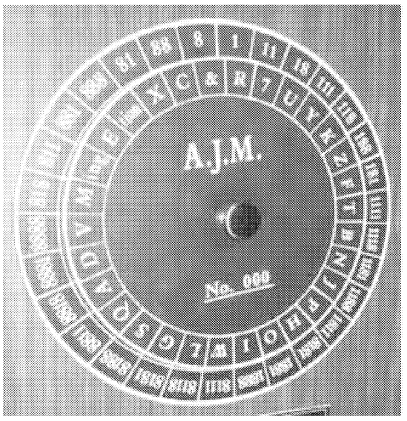
The invention of the electromagnet by William Sturgeon 1825 paved the way for the birth of signals. The telegraph and the Morse code (invented by Samuel F. B. Morse) allowed more scope for interception in the mid-19th century.

Below is a typical telegraph message that could be sent, using Morse code to transmit the actual content from point to point:



Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

One important aspect to the history of CSEC is that within signals intelligence, there is an element of coding involved. Just as Morse code had to be translated back into the alphabet, modern signals also require some processing. With those who security savvy, they would often use cryptography to mislead or hide the message that are sent and received.

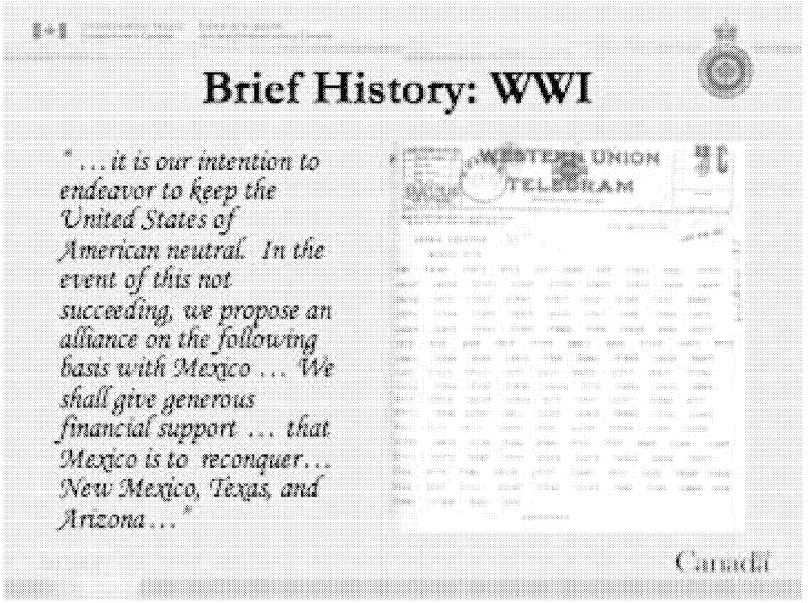


One example of this, prior to the digital revolution, is Union Maj. Gen. Butterfield's use of deceptive messages sent via telegraph to "throw off" the Confederates during the American Civil War. The ability to decipher Confederate messages allowed Butterfield to confirm that the false messages were received.

The Union began using cipher disc devices to improve the security of their messages, such as the one depicted here (on left).

By the First World War, the importance of signals intelligence became even more prominent. Among the most famous uses of SIGINT at the time was the Zimmerman Telegraph. The telegraph was a coded message sent by Foreign Secretary of German Empire to German ambassador in Washington, DC.

Pictured below with an excerpt of the deciphered text, intercepted by the Allies, this telegram became a key factor in the US's decision to enter the war.



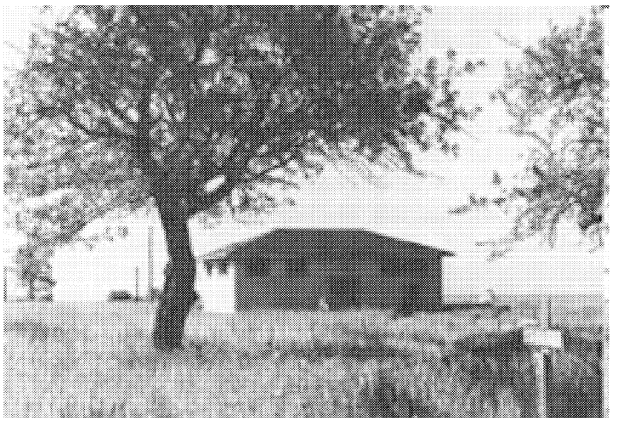
Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

While Canada had some participation in the intelligence war efforts, it was not until 1939 when the Royal Canadian Navy first established Signals Intelligence capabilities, most commonly known as the Y Section. The Army and Air Force would also establish their own branches to collect and analyse intelligence during the war to provide support to the troops and to the Allies. In 1943, the Canadian Forces combined their intelligence branches into a joint effort.

In 1941, a similar initiative to provide intelligence to the Government of Canada was created when Herbert Yardley was invited to Canada to help found the Examination Unit (XU) in 1941. The XU was an External Affairs (now Foreign Affairs) project, hosted by the National Research Council. Their focus was mostly on the Vichy government, as well as Japanese diplomatic reporting, as opposed to the military efforts directly targeted at winning the war.

1941 also saw the establishment of a training facility for secret agents of the British Special Operations Executive, who were inserted behind enemy lines. Affectionately (or more commonly) known as Camp X, this training facility outside Oshawa was the first of its kind in North America and shaped the spy schools for the US Office of Strategic Services (now CIA).

Below is a photo of what Camp X was like when it was first established:



Following the victory of the Allies over Germany, there was some doubt as to whether or not the Canadian SIGINT programs would survive in peacetime. There were prominent Canadian politicians and leaders on both sides of the debate. Proponents believed that a continued SIGINT effort will provide Canada with the necessary information advantage to prosper; while those who are opposed to the ideal believed in, and championed for a peaceful world without a need for espionage and spying.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

When Igor Gouzenko—a cipher clerk at the USSR Embassy in Ottawa—defected, he exposed the Soviet spy efforts operating in Canada. This incident served as a reminder to Canadian leaders that espionage was still being carried out after the Allies victory. Although Soviet Union was generally viewed as an ally during the war, the documents that Gouzenko surrendered indicated that they may be an adversary in the postwar environment.

In 1946, the military and civilian SIGINT organizations that had been operational during the Second World War were officially amalgamated into the Communications Branch of the National Research Council (CBNRC). With the NRC as host, the Communications Branch was administered by the External Affairs department. The CBNRC is CSEC's direct predecessor.

All of this changed in 1974, when the CBC program, The Fifth Estate, presented an episode called: "The Espionage Establishment" – clips of the Sir Leonard Tilley Building was shown on the television as the voice-over narration describe a spy agency working in Ottawa. In addition to the campus, the Fifth Estate also identified some key figures within the organization, and showed footage of employees entering and exiting the SLT. This attracted tremendous media attention, as government officials and Members of Parliament, previously oblivious to the existence of CBNRC demanded answers. In addition, the National Research Council suffered as their reputation as an impartial research and development institution came under question.

As a result, an Order in Council transferred CBNRC to the Department of National Defence, and the name of the agency was changed to the Communications Security Establishment (CSE):

Canadian SIGINT provided government leaders and our allies in the US and the UK with important information on Soviet activities during the Cold War. Tensions and threats of nuclear war dominated the reporting lines in Canada's SIGINT efforts, and it was not until the fall of the Berlin Wall in 1989, signifying the end of the Cold War, when SIGINT would face its next transformation.

Since SIGINT had been so focused on collecting information on the USSR, the conclusion of the Cold War and the collapse of the Soviet Union meant that Canadian SIGINT was once again in limbo. Priorities and focus shifted from Communist espionage and another world war to [redacted]

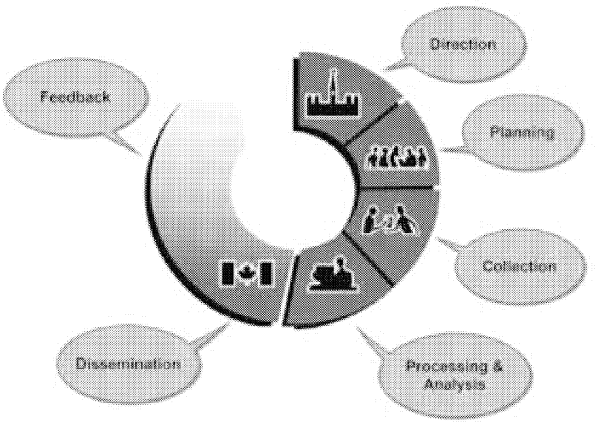
When the terrorist attacks on the World Trade Centre and the Pentagon occurred on 9/11, SIGINT in Canada had focused the majority of its resources on [redacted] In the aftermath of September 11, the Parliament passed the *Anti-Terrorism Act*, which amended the existing *National Defence Act*.

This legislation cemented CSEC's mandate into law, and allows CSEC to conduct our activities. With new authorities and legislation, CSEC grew in size to about double its pre-9/11 numbers.

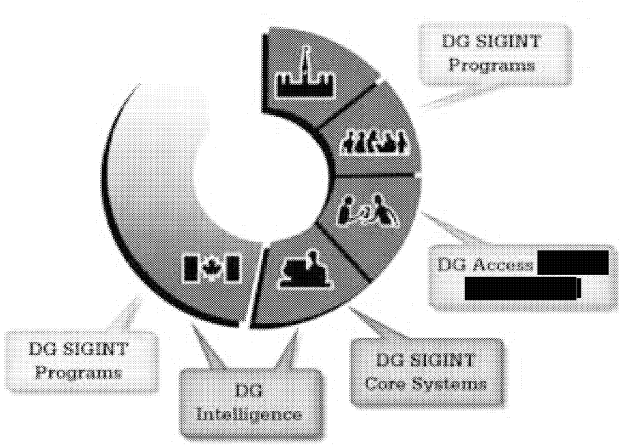
Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

INTELLIGENCE CYCLE

The various areas within the CSEC SIGINT Business Line correspond to the stages of the Intelligence Cycle. There are basically 6 different stages on the Intelligence Cycle, which can be used to understand the process through which intelligence requirement is gathered, collected, analysed, and disseminated. Below is an example of the Intelligence Cycle and the 6 stages:



And when the names of the stages are exchanged for the names of the various groups within CSEC, a clear picture of how SIGINT is conducted in CSEC emerges:



Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

Notice that the spots for Requirements and Dissemination are not populated with any directorate. Key to the understanding of the business of SIGINT is the reality that CSEC never dictates the requirements and priorities. CSEC acts on intelligence requirements from the Government of Canada, and specifically from various client departments like the Privy Council Office (PCO), the Department of National Defence (DND), and the Department of Foreign Affairs and International Trade (DFAIT).

REAL-WORLD SIGINT

To better understand how a requirement or event travels through the various stages of the Intelligence Cycle, one example is [redacted]

[redacted]

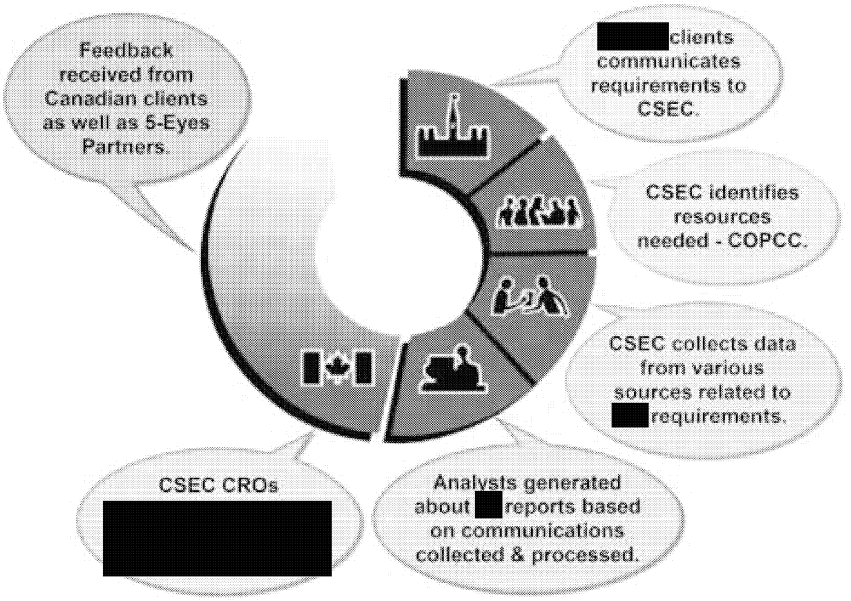
Since [redacted] approximately [redacted] end products directly related to [redacted] were issued, compared to only [redacted] end-products [redacted] All but six [redacted] %) received an Exceptional rating, mainly from [redacted] The Intelligence Branch [redacted] teams issued over [redacted] additional end-products related to [redacted]

Canadian clients [redacted] were impressed with the volume of valuable reporting coming from CSEC, commenting that the material was very useful. In particular, they were pleased with the quick turnaround time (a matter of a few hours in some cases) between levying a requirement and seeing the finished product. The CSEC product was also of high interest [redacted] – two CSEC reports got "tipped [redacted] and other reports were also getting "great play [redacted] sent their kudos and commented that "this is exactly what [redacted] is looking for".

As a result of this effort, CSEC has made use of the COPCC and the various resources identified for [redacted] to prepare and meet the intelligence requirements of Government clients for [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Using the narrative above, the various stages of the Intelligence Cycle can be easily identified, and when substituted into the Intelligence Cycle on Page 7, the image below illustrates how [redacted] requirement was handled by CSEC:



While [redacted] is one example with clearly identified steps of planning, coordination, and feedback, other requirements to which SIGINT responds follow a variation of the Intelligence Cycle. For urgent issues, such as the kidnapping of a Canadian, or when providing support to tactical military operations in Afghanistan, it may not be immediately obvious that the requirement can trace its steps through the Intelligence Cycle.

ADDITIONAL RESOURCES:

CSEC Time Capsule (Information on History):
[redacted]

CSEC [redacted] (Information on various areas within SIGINT):
[redacted]

Instructor:
[redacted]@cse-cst.gc.ca; [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

appendix B

Supplementary Information: History of SIGINT

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

As new employees to SIGINT[1], you are embarking on a career path with a long tradition and history of protecting Canada and safeguarding our national interests. Over sixty years ago, signals intelligence played a vital role in the victory of the Allies during World War II and today SIGINT continues to provide Canada's decision-makers with insight into what lies behind the [redacted] who threaten Canada's national interests.

SIGINT is and has been our government's primary source of secret information on the [redacted] The Canadian SIGINT program is the largest producer of foreign intelligence in Canada (about [redacted] SIGINT reports every year) and is by far the largest supplier of Allied foreign SIGINT.

Our government's insight into world events is informed, at least in part, by the foreign intelligence we produce.

Right now, the Canadian SIGINT program is at a pivotal time in its history. We can point with pride to the tremendous progress we have made since 9/11 in addressing the pressing security and technological challenges faced by this program. We are making a difference in the lives of Canadians, but we are also facing challenges that will demand the best of our efforts in the days to come.

Will our efforts be informed by a sound understanding of our business as shown in the lessons learned from our history? In order to move forward with assurance, we need to understand where we have come from.

The aim of this course is to acquaint you with the significant events and factors—both international and domestic—that shaped our history. By reflecting on what has happened, you will be able to see what has worked and what has not worked over the years, learn from these CSEC experiences, and build on them.

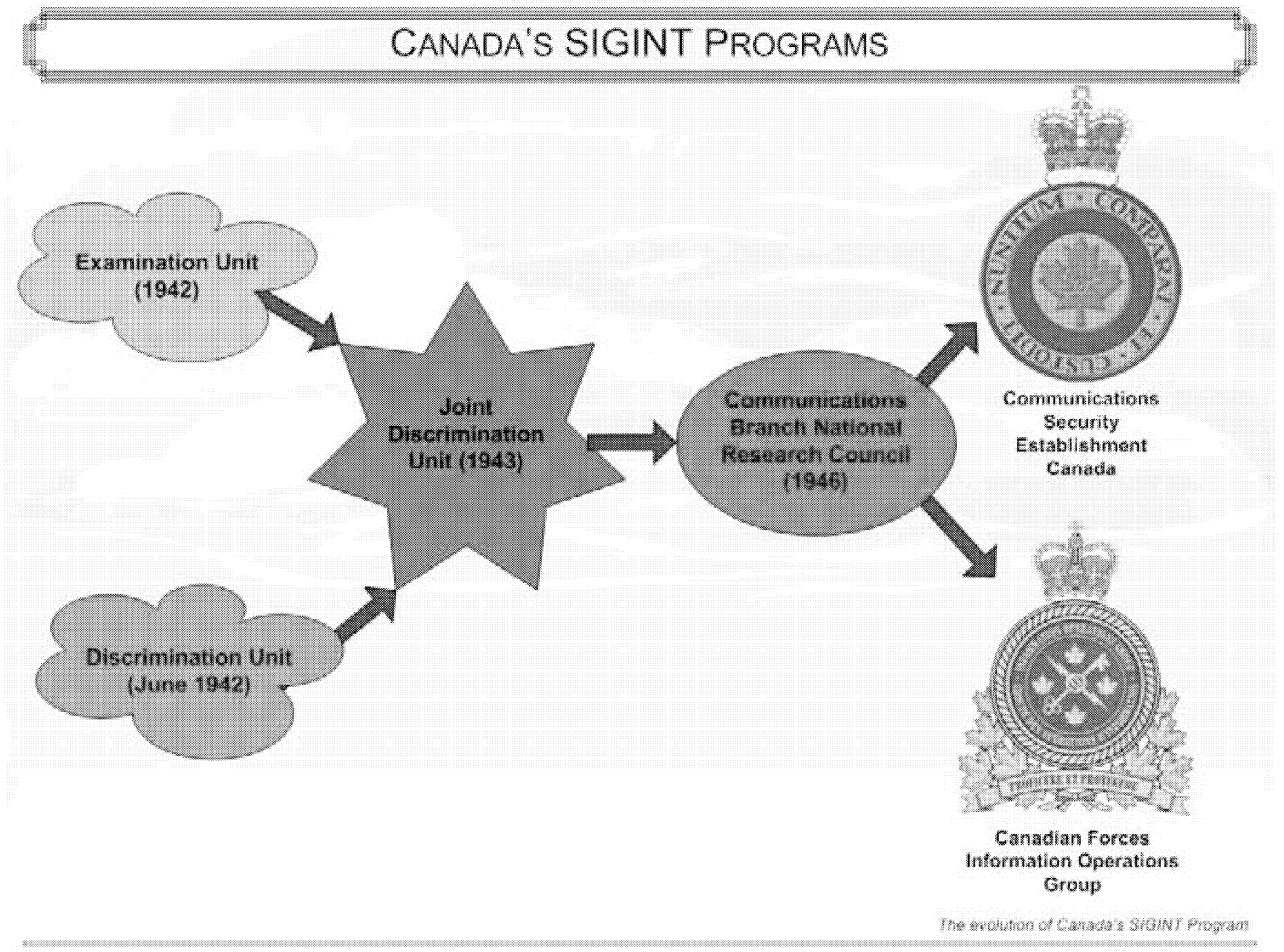
Along the way, you will learn about the critical domestic and international partnerships that have been, and still are, so vital to our continued success. You will develop a better appreciation of the foreign intelligence priorities of our Government over the years and how they drove SIGINT operations. You will also learn about the evolution of SIGINT authorities, resources, and capabilities, and how these impact on our ability to provide our Government with relevant and timely foreign intelligence. In order to fully understand the business of SIGINT, and the reasons for the Government's SIGINT priorities, it is important for us to look back on our history and examine how the business of SIGINT has evolved over time, and how CSEC has come to be the organization it is today.

1. For information on how the SIGINT Business Line is organized within CSEC, please refer to the "SIGINT Org Chart".

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

HISTORICAL OVERVIEW[2]:

The Canadian Government sanctioned intelligence activities in a few occasions in the decades following confederation, but as the Global Information Infrastructure (GII), as we know it today, did not exist, there was no real SIGINT. Most of the first intelligence efforts were done in cooperation with the UK and based on UK priorities. During WWI, Canada was involved in the interception of telegrams from the German government, but there was no comprehensive program for SIGINT. Intelligence work in Canada was chiefly performed by the Criminal Investigation Branch of the RCMP, and was directed against perceived threats from the left.



2. From: Granatstein, J.L., and Stafford, David: Spy Wars. Espionage and Canada from Gouzenko to Glasnost, (Toronto: Key Porter Books Limited).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

WWII[3]:

The Criminal Investigation Branch was too ill-equipped and insufficiently-trained to be adequate for Canada's intelligence needs following the outbreak of WWII, so an alternative solution was required.

Records show that the fist known Intercept Site (known as "Y" Site) was operational in 1939. The Army Headquarters Radio Station located at Rockcliffe Airport, Ottawa, was a logical place for army wireless activities. In June 1942, these activities were moved to Leitrim and the site was renamed as #1 Special Wireless Station. That same year, Special Wireless Stations #2 and #3 were established in Grande Prairie, Alberta, and Victoria, British Columbia, respectively.

In 1941, Herbert Osborn Yardley, a famous cryptologist of the 20s and 30s who helped break Japanese codes for Chinese Nationalist leader Chiang Kai-Shek, was recruited to help set up a Canadian cryptology program, which subsequently became the Examination Unit (XU). It was a very closely guarded program; Yardley even used an alias while working within the XU. Throughout the war, there was close Anglo-Canadian and US-Canadian cooperation in SIGINT. For example, a telekrypton link was established between the Examination Unit and the British Security Co-Ordination office in New York City. Canada's focus was on Abwehr agents in South American communicating with Hamburg. In this role, the Examination Unit was able to provide valuable intelligence to protect allied shipping. In addition, the XU intercepted and analysed the communications of Japense agents.

British and American agencies have collaborated with strong cryptologic ties throughout WWII; in 1942 the UK's Government Code and Cypher School (GCCS) – predecessor of the Government Communications Headquarters (GCHQ) – signed the "Holden" Agreement with the US Navy. This cooperation is followed by the signing of the GCCS-US Army Agreement in 1943.

Throughout the war Canada played a role chiefly as the Dominion of the UK, though the collaboration on the war effort had included representatives from Canada. Canada's partnership with the United States began in 1942, when Canada established war-time collaboration efforts with the US Army and Navy. In 1944, Lt Col Edward Drake represented the Canadian SIGINT Program when he attended the 2nd Japanese Army Cipher Conference.

3. Information courtesy of GCHQ Corporation Knowledge & Information Services.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

IRRELEVANT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

AGREEMENTS FOR SIGINT COOPERATION

[redacted]

Examples of documents sent between the 5-Eyes countries for cooperation & information-sharing

COLD WAR:

The Gouzenko Affair was the catalyst for Canada's participation in the Cold War and the continuation of a Canadian signals intelligence program in peacetime. In 1945, Igor Gouzenko, a cipher clerk at the Soviet embassy in Ottawa, approached the police with a sheath of documents taken from the embassy, which revealed the extent of the Soviet espionage efforts in Ottawa. Although not everyone believed him at first, Gouzenko was eventually taken seriously and the information he provided led to the arrest of many Soviet spies.

The defection of Gouzenko was eye-opening for most Canadians, who saw the USSR as an ally critical in victory over the German forces in WWII. The incident prompted the Canadian government to continue developing the SIGINT program it had begun during the War, and to maintain the close cooperation on SIGINT that had been forged between Canada, the UK, and the US.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

To continue with the partnership and collaboration after the war, the Commonwealth Conference was held in March 1946, where it was agreed by those in attendance that Canada needs to work directly with Washington for mutual benefit and defence. The British-US (BRUSA) Agreement was signed between the two countries' intelligence agencies. This provided a division of effort and a commitment to collaboration for the post-war SIGINT.

That same year, the responsibilities previously under the Examination Unit were transferred to the Communications Branch National Research Council (CBNRC). The Department of External Affairs would drive the policy and priorities of the CBNRC, with the National Research Council (NRC) as the host of the civilian SIGINT program. In 1947, a bi-lateral agreement was drafted between Canada and the US, based on the BRUSA/UKUSA text. This document, the Can-US Agreement, was subsequently signed on 29 June 1949.

While Canada had been mentioned in the BRUSA (later the UKUSA) Agreement, Canada did not independently establish ties with the US until, in 1949, Canada and the US signed the CANUSA Agreement, which paved the way for liaison exchanges between the two countries in 1954, when the Special US Liaison Office in Ottawa (SUSLO) and the Canadian Special Liaison Office Washington (CANSLO/W) were established.

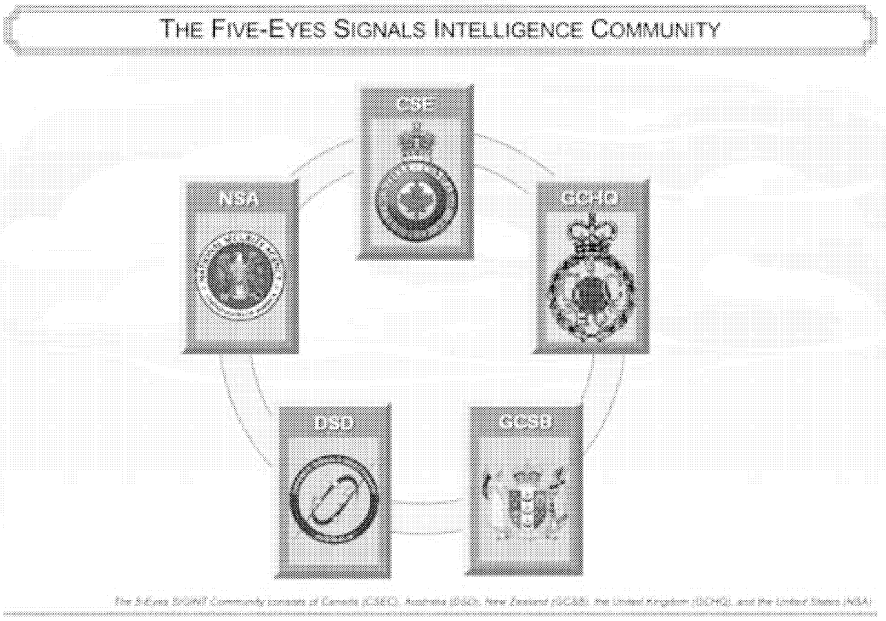
While stories of spies were popular during the Cold War, SIGINT was another "battlefield". The threat from the USSR and its allies was very real. For example, in the 1980s, the USSR's Main Intelligence Directorate (Glavnoje Razvedyvatel'noje Upravlenije, or GRU) had [redacted] signals regiments and ran SIGINT from over [redacted] ships and over [redacted] aircrafts. [redacted] were carried out from all Soviet foreign posts. The USSR at one point employed approximately [redacted] people to carry out SIGINT.

In 1975, the Fifth Estate, a program produced by the Canadian Broadcasting Corporation (CBC), featured a story on the espionage activities being conducted by the CBNRC at Sir Leonard Tilley Building in Ottawa. This created tremendous unease within the House of Commons, as Members of Parliament learned of the previously-unknown agency through the television. The NRC also suffered from the publicity and high profile of the program. As a result, the CBNRC was renamed the Communications Security Establishment and would be hosted by the Department of National Defence (DND).

Although the Cold War still dominated Canada's intelligence priorities throughout the 1980s, there was also an awareness of the threat posed by international terrorism. On 23 June 1985, Air India Flight 182 was bombed in what was the deadliest terrorist attack involving an aircraft until 11 September 2001. The attack was planned by Sikh separatist organizations, and the incident led CSIS and the RCMP to shift their focus towards counter-terrorism.

While this shift may have provided the Canadian SIGINT program with new direction, the recent history of Canadian SIGINT is not without some obstacles and setbacks. In 1982, the Canadian Charter of Rights and Freedoms came into effect, guaranteeing the rights of people in Canada. From SIGINT's point of view, the Charter posed a dilemma; since all communications of Canadians are now protected, and supporting legislations did not exist to allow CSEC to carry out operations on communications that are routed within or through Canada, the SIGINT program was threatened by the legal protection of communications. The Canadian SIGINT program, as a result, lost much of its ability to intercept and track communications of entities of interest to the Government.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés



1990'S AND BEYOND:

Following perestroika and the collapse of the Soviet Union, SIGINT efforts took on less importance in Canada and, indeed, some questioned whether the existence of CSEC was even necessary through the 1990s. In 2001, however, all of that changed with the 11 September attacks on the World Trade Centre in New York City and the Pentagon in Arlington, Virginia. The incident highlighted the danger posed by international terrorist groups, and in the years following the attack, CSEC grew in number as many new analysts were hired.

In 1991, the Canadian Forces Supplementary Radio System (CFSRS) – established in 1938 and was the branch chiefly responsible for coordinating military SIGINT – was renamed the Canadian Forces Information Operations Group (CFIOG).

Another important milestone for Canadian SIGINT came in December 2001 with the passing and Royal Assent of the *Anti-Terrorism Act* (Bill C-36). Among other clauses, the legislation amended the *National Defence Act*, and cemented CSEC's mandate into law. The legislation also established clear rules within which CSEC must operate[4]. With the Canadian Forces' participation in the mission in Afghanistan, SIGINT has established much stronger ties with the military in support of Canadian [redacted] troops in-theatre to ensure their safety, and the success of their mission. In recent years, cyber security threats also required CSEC to devote resources in response to the various GC requirements on [redacted] around the world. As technologies change, and as different threats emerge to threaten the national security and interests of the Government of Canada, CSEC SIGINT will continue to evolve in order to respond, and in this way, to remain a valuable source of information, and to provide leaders in the Government with vital information to further Canadian interests.

4. For more information on CSEC's legislation, please see Chapter 3: SIGINT's Legal Framework.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT TIMELINES

The two following fold-out pages show the important historical events that had an impact on CSEC since 1940, and CSEC SIGINT targets of interest for the same period of time.

A simple way to identify and understand SIGINT priorities is to ask: Why would the Government of Canada (GC) be interested in this event? What information would be of interest to the Government of Canada?

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

A-2017-00017--01952

CANADIAN SIGINT TIMELINE

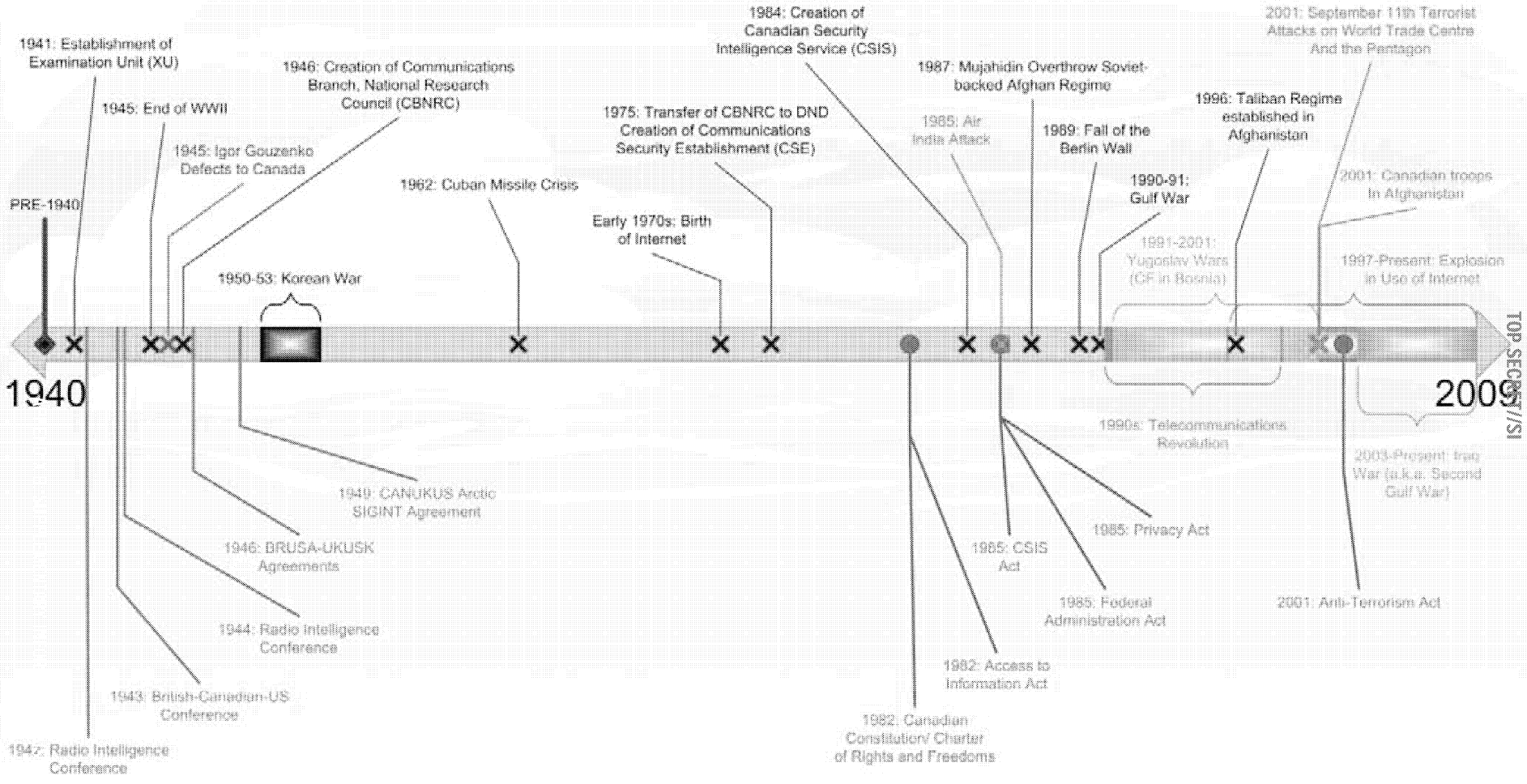


Figure 2.4 – Significant Events in the History of Canadian SIGINT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

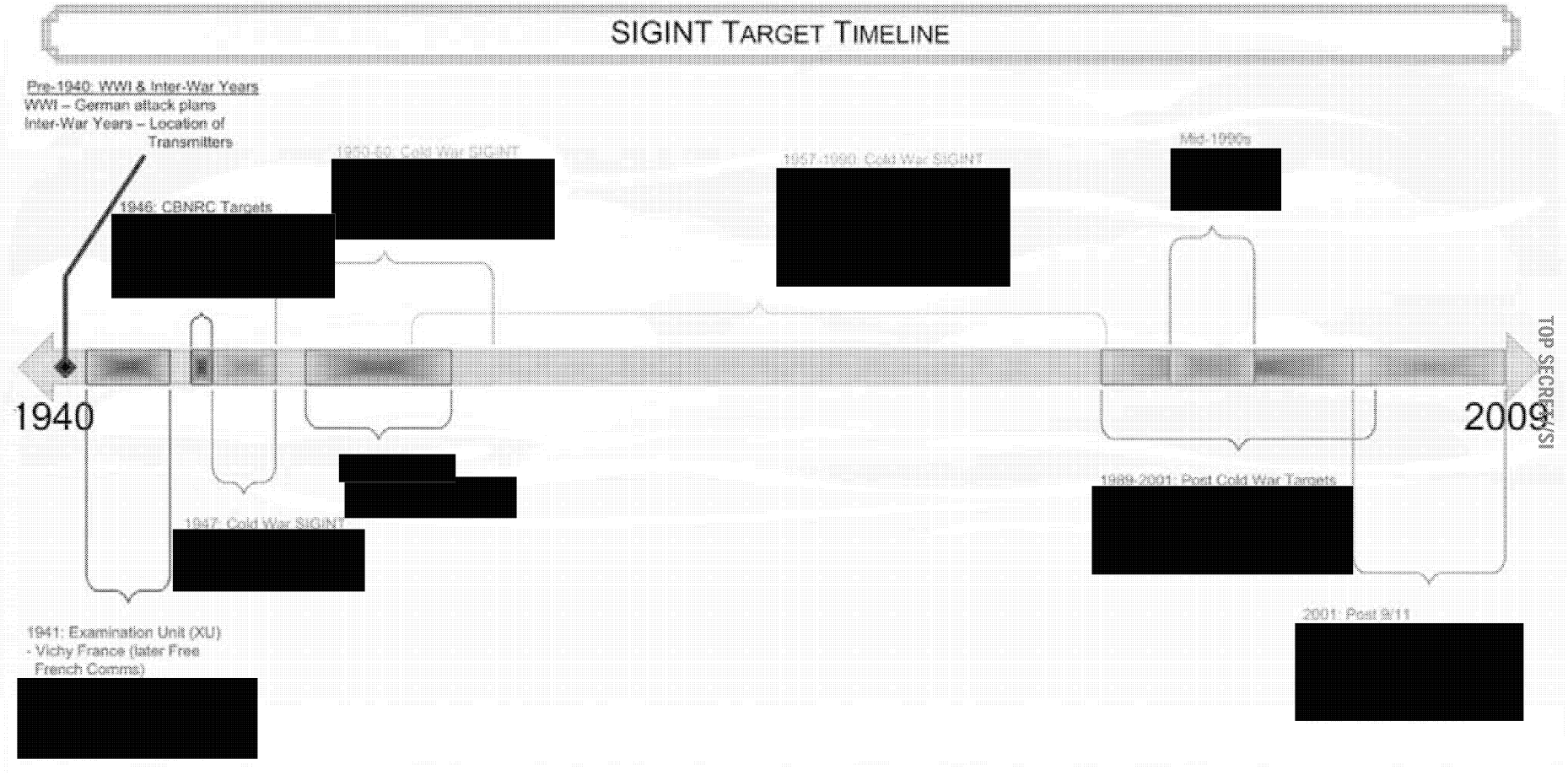


Figure 2.X – Targets of Interest through the History of Canadian SIGINT

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT "HALL OF FAME": QUOTABLE QUOTES:

"When our contribution was nil, we received nothing… When, in agreement with them [US/UK], our contribution became substantial, we received ample return – a seat in their counsels and a regular budget of valuable intelligence. If we contributed to the pool we shall draw from it in the form of finished products; if we fail to contribute, we shall receive nothing."

"Cryptanalysis is a short, straight road into the opponent's mind."

– Col. William W. Murray

"One supreme value of signals intelligence is that it is a short road into the mind of others… One reads what the originator actually says and what… he is transmitting to others. Experience in War has demonstrated that wireless information is one of the most important sources of secret information."

– Gen. Charles F. Foulkes, Dec 1945

"Through the Unit… Canada has been led to a window on world diplomacy which otherwise she may never have looked through. Whatever is decided concerning this office, most countries of the world will continue doing cryptography work after the war is over and I cannot agree that Canada will improve her position in the world affairs by renouncing all activity in this work… This is not to foresee another war, but the world will be a troubled place for a long time to come and there will undoubtedly be countries whose activities we will be particularly interested."

– Gilbert Robinson, MBE (Professor and Mathematician)

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

PEOPLE OF NOTE:

Edward M. Drake was an Officer in the Reserve Army at the outbreak of the Second World War. He was commissioned in the Royal Canadian Corps of Signals (RCCS) as a Lieutenant. His outfit, the Experimental Station at Rockcliffe air force base in Ottawa, intercepted German and Italian communications. By June 1942, Drake had become a Captain and was attached to National Defence Headquarters (NDHQ) in charge of MI2 within the Directorate of Military Intelligence. He was made responsible for leading the Discrimination Unit that processed messages. Eventually, Lieutenant Colonel Drake managed the Joint Discrimination Unit, which combined those of Army, Air Force, and Navy into one consolidated organization. He was the first Chief of CSE. The Edward Drake Building, located at 1500 Bronson Avenue, was named after Drake to commemorate his contribution to CSEC.

Igor Gouzenko was a cipher clerk at the Soviet Embassy in Ottawa who defected from the Soviet Union on 5 September 1945. Gouzenko revealed a vast network of Soviet spies in Canada, the US, and Great Britain. The inquest that followed led to 39 arrests in Canada and the exposure of spies, including Klaus Fuchs – the German communist physicist who stole atomic secrets after moving to Britain and gave them to the Soviets, and Julius and Ethel Rosenberg. Gouzenko's defection and the information he provided strengthened the case for maintaining a SIGINT capability in Canada when critics questioned the relevance and need for peacetime SIGINT.[5]

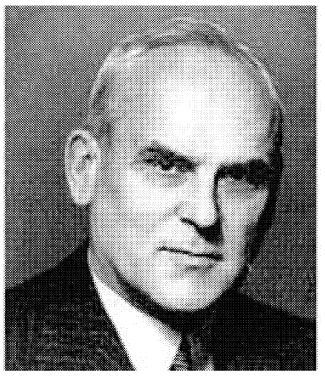
Clarence D. Howe was the Minister of Munitions and Supply during WWII. He was responsible for signing the Order in Council for the creation of the Communications Branch of the National Research Council (CBNRC), the predecessor of Communications Security Establishment Canada (CSEC).

Kevin O'Neill was the second Director of CBNRC, from 1971 to 1980. He was recruited by Edward Drake from UK's Government Code and Cipher School (GCCS). The Kevin O'Neill Boardroom (KON), located on the second floor of the SLT building, commemorates his contribution to Canadian SIGINT.

Herbert Yardley taught Canada the esoteric profession of code-breaking and thereby gave Canadians a SIGINT capability. He established a firm foundation for Canada's Examination Unit (XU) in 1941. Yardley was considered one of the world's greatest cryptanalyst. In 1999, the National Security Agency (NSA) inducted Yardley into its Hall of Honour. He was also a member of the Military Intelligence Hall of Fame.

Edward M. Drake

Igor Gouzenko



Clarence D. Howe

Herbert Yardley

5. Efforts to identify Soviet spies included the VENONA project, collaboration between the US and the UK intelligence agencies, provided information that contributed to the identification and exposure of agents such as the Cambridge Five – Donald MacLean, Guy Burgess, Kim Philby, Anthony Blunt, and John Cairncross, as well as many others.

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

SIGINT ESTABLISHMENT OVER THE YEARS:

HYDRA, located at Camp X outside Oshawa ON – used to communicate with undercover agents in Nazi-occupied Europe. This building was used as communications link for SIGINT agencies in the US, the UK, and Canada after WWII.

Leitrim, in the "early" days

Canadian Forces Station, Alert, 1957

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

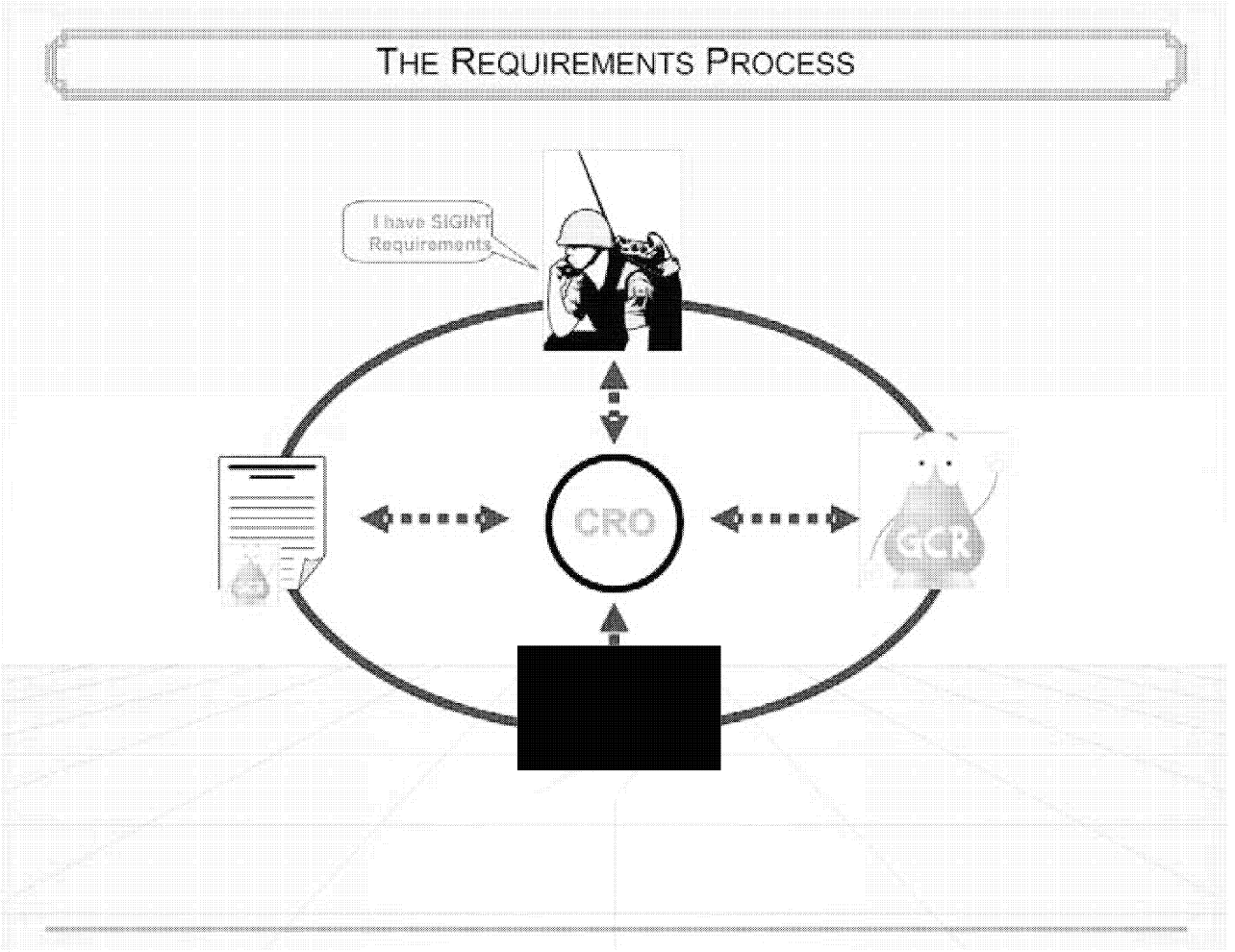
Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

appendix C

Supplementary Information: Government of Canada Requirements

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

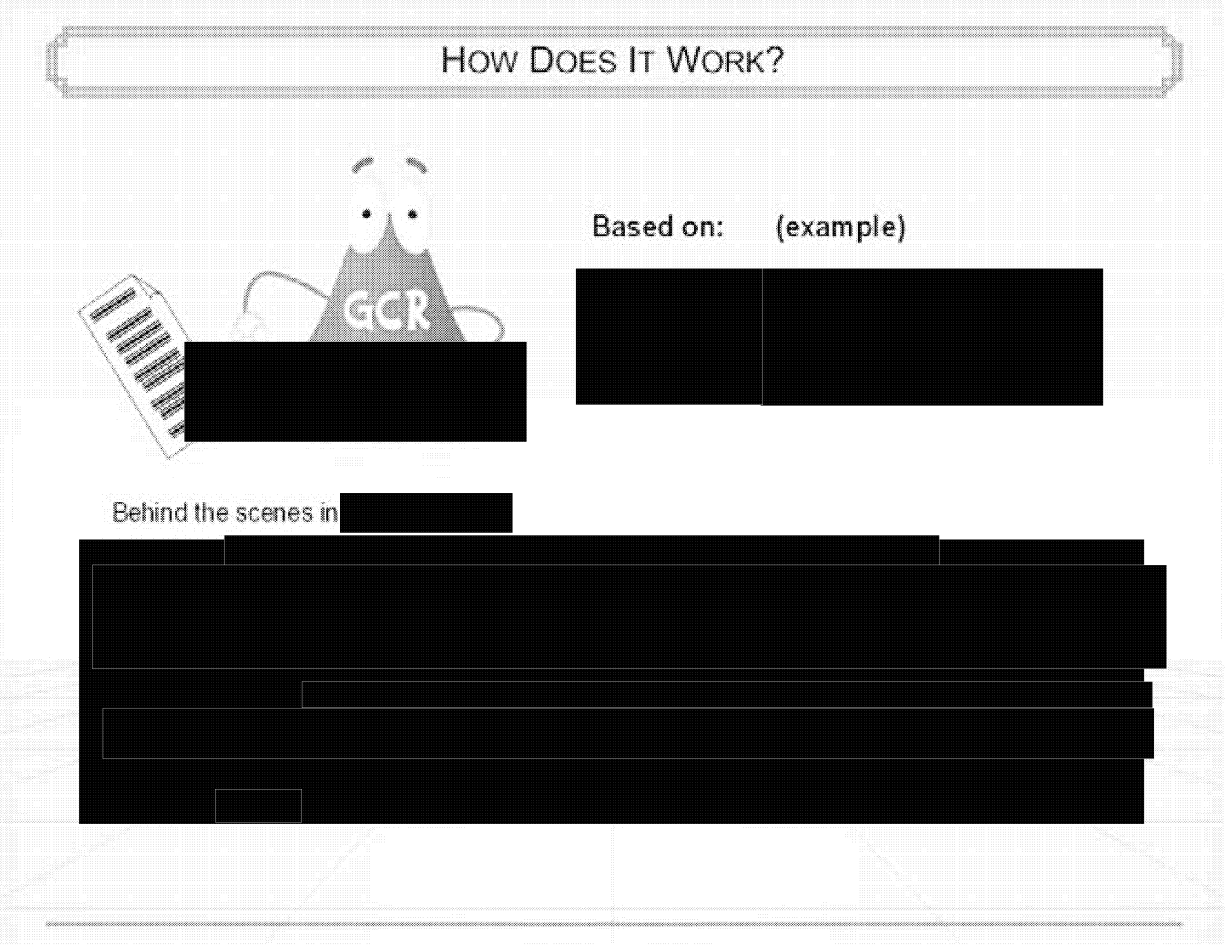
The Government of Canada Requirements (GCRs) were created to facilitate end-to-end tracking of client requirements and CSEC's efforts against those requirements. There are many stakeholders who utilize GCRs. They include Government of Canada (GC) clients, Client Relations Officers (CROs), [redacted] and CSEC and CFIOG SIGINT analysts. [redacted] is the software application that allows client requirements to be entered against GCRs. CSEC manages these GCRs, and SIGINT analysts' reports are automatically assigned GCRs to enable CSEC's clients to find the SIGINT report they need in [redacted]



Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

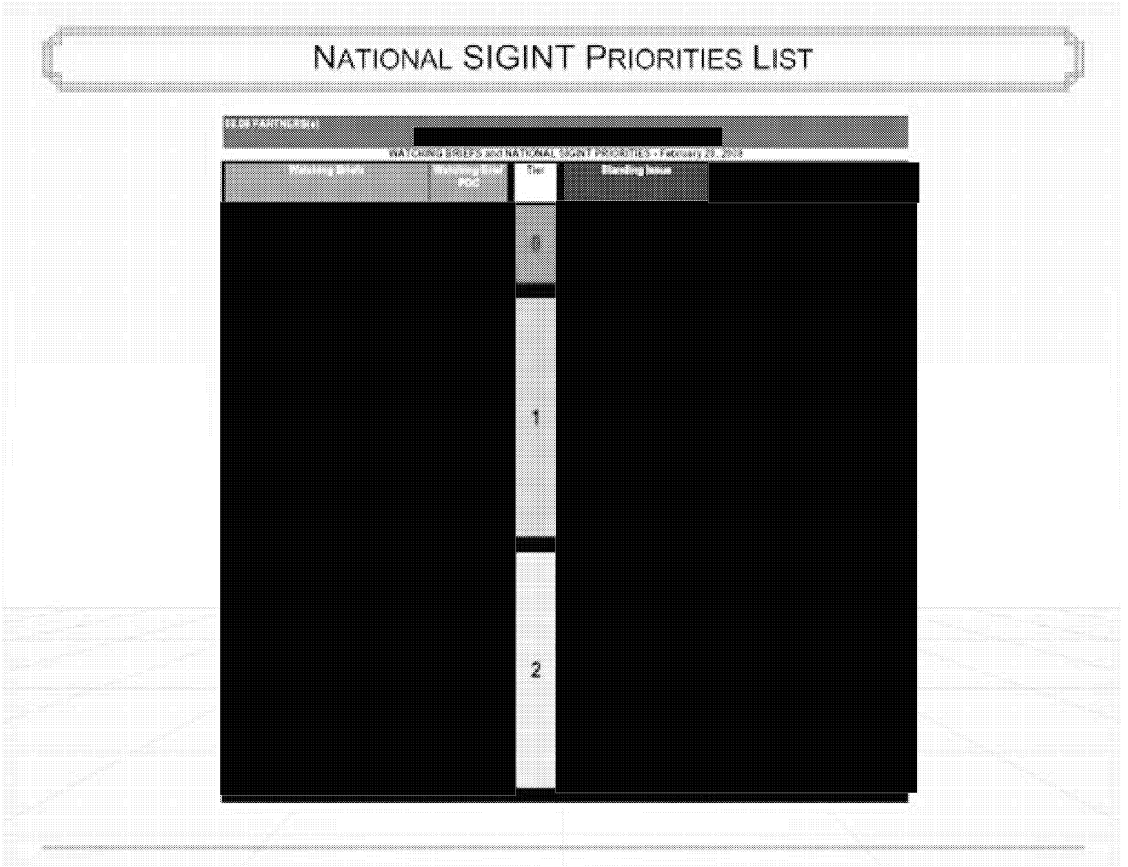
SIGINT reports generated by CSEC must correspond to GCRs. When a client has requirement for SIGINT information, a GCR is matched to their specific request based on their topic of interest. A GCR can be shared by many clients, and each client can have more than one GCR in his/her profile. A client can have different GCRs to meet their needs, but these GCRs must be prioritized and subscribed in [redacted] in order to facilitate automatic dissemination and provide CSEC with an understanding of the client's requirements.

The GCR is composed of [redacted] different sets of numerical digits. The [redacted] numbers represent the [redacted] Each [redacted] has a related search in [redacted] based on a series of keywords, and once the GCR is subscribed, the software searches the database for all reports with the keywords as outlined by the GCR. The graphic below provides an example of a GCR in its [redacted] and what the search keyword string would look like in [redacted]



Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

The National SIGINT Priorities List (NSPL) sets out the overall priorities of the Government of Canada, with Tier 0 being the [redacted] and Tier 4 the [redacted] The list includes issues relating to a [redacted] rather than the [redacted] As such, a [redacted] may appear in several Tiers. The NSPL is separated into Standing Issues [redacted] on the right of the Tier number, and Watching Briefs and their points of contact on the left of the Tier. Both Standing Issues and Watching Briefs have appropriate GCRs mapped to them in order to facilitate tracking production and client satisfaction. Below is an example of the NSPL.



Understanding GCRs and NSPL:

GCRS	NSPL
[redacted]	Standing Issue
	Standing Issue further refined
	[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

appendix D

Supplementary Information: Access Fundamentals for SIGINT

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

REVIEW OF EXERCISE #1: [redacted]

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

REVIEW OF EXERCISE #2: [redacted]

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

BASIC ACCESS [redacted] SUMMARY TABLE

Access	[redacted]
Pros	[redacted]
Cons	[redacted]
Risk	[redacted]
Authorities	[redacted]
Knowledge/ Information Required	[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

REVIEW OF EXERCISE #3: TARGETING CONCEPTS

- Phone, Facsimile [redacted]
  - » [redacted]
  - »
  - »
  - »
  - »
  - »
  - »
  - »
  - »
  - »

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

- [redacted]
- [redacted]

[redacted]

REVIEW OF SUCCESS STORY: [redacted]

[redacted]

2. [redacted]
3. For more information on DNI and DNR, refer to Chapter 12

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

appendix E

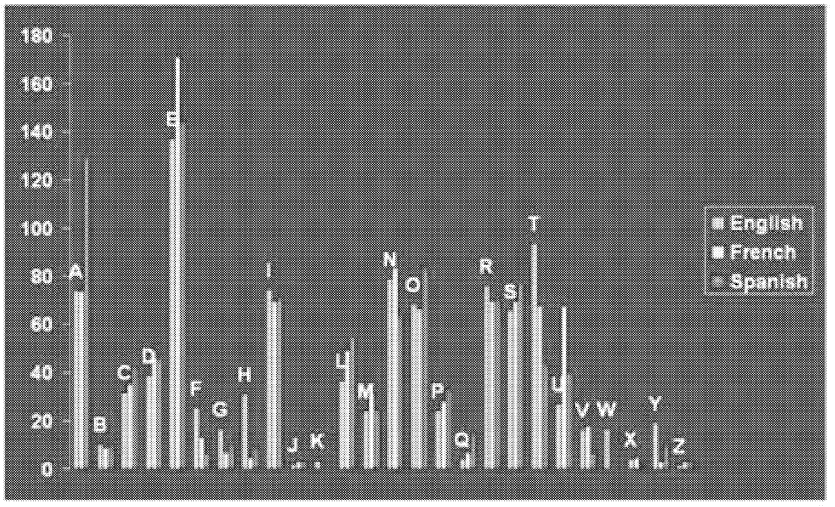
Supplementary Information: Access Fundamentals for SIGINT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Simple encryption methods can be detected if one has a basic understanding of the English language. There are certain properties of plaintext that would help to break an encryption, especially one based on substitution:

- Identity
  - » the alphabet used in the plaintext
  - » ex. A B C D E . . .
- Roughness
  - » frequency with which the letters within the alphabet are used
  - » ex. "SENORITA" – this word contains the most commonly-used letters in the English alphabet
- Cohesion
  - » certain consonants or letters appear together
  - » ex. QU, TH, SS, . . .
- Pattern
  - » distinguish words that have a particular pattern (like anagrams)
  - » ex. MADAM (pattern = a b c b a), ASSESS (pattern = a b b c b b)
- Repetition
  - » words or groups of letters that are frequently used together
  - » ex. THE, -MENT, -TION, . . .

The image below shows a statistical layout of the most frequently-used letters in English, French, and Spanish:



(Out of 1000 Characters)

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

HOW CAN ANALYSTS HELP DO CRYPTANALYSIS

Analysts can help cryptanalysts perform their jobs in a variety of ways, which would not take much time. First of all, cryptanalysts need cipher to analyse and they need as much as possible. One sample of the cipher is usually not enough for cryptanalysis. So do not be surprised if cryptanalysts ask for what seems to be excessive amounts of cipher examples. The cipher must also look exactly like cipher produced by the encryption system. In other words, they must be able to peel overlying layers of the onion without corrupting the cipher.

Metadata is also very important for cryptanalysis. Cryptanalysts will always appreciate [redacted] Examples of items of interest to cryptanalysts are:

- [redacted]

Plaintext properties are also of great use. Analysts could help cryptanalysts to learn these properties by providing:

- [redacted]

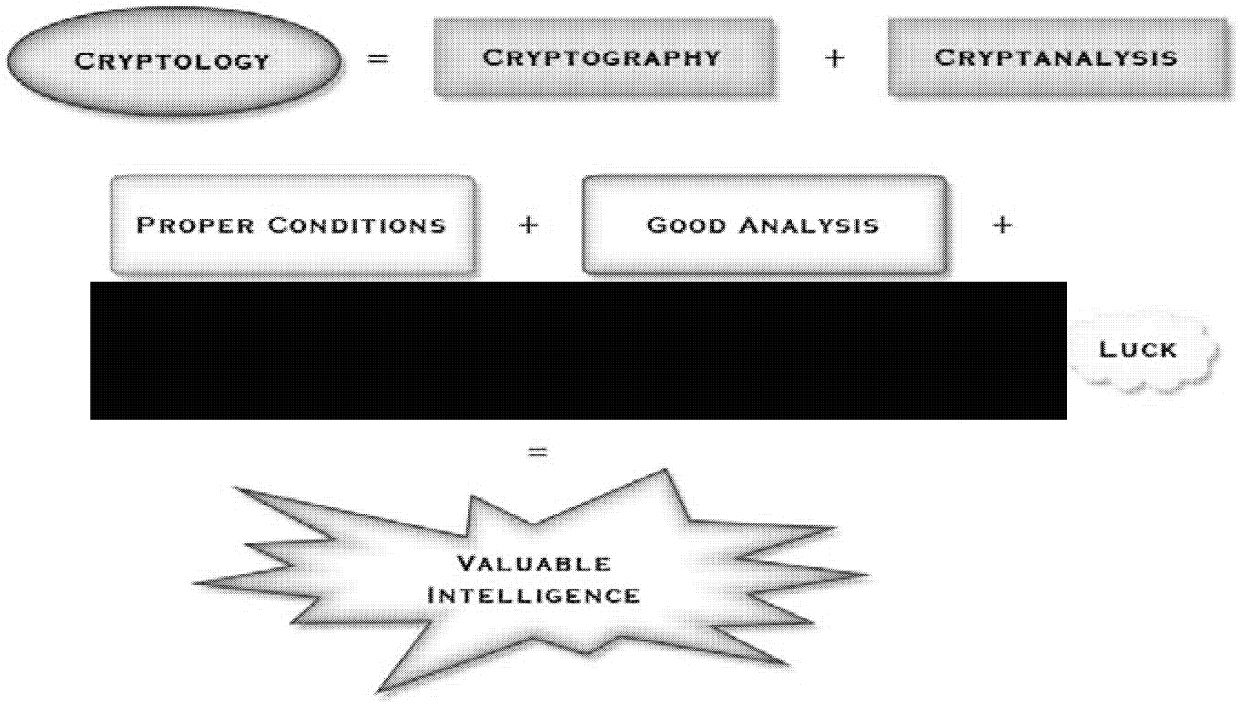
Since cryptanalytic work can take a long time (sometimes on the order to years), it is always important for the cryptanalysis areas to have as much information as possible in order to determine crypt investment. For the same reason, as much lead time as possible with respect to a requirement will always be appreciated. In other words, [redacted]

Because of the challenge in breaking cryptography, cryptanalysts are always looking for ways to combine approaches in order to find the easiest solution possible. An example would be [redacted] facilitating cryptanalysis and vice versa.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Finally, optimism is a great asset in cryptanalysis. While the initial prognosis for success may not be high, cryptanalysis have often been able to tackle and identify vulnerabilities in encryption.

While Data Analysis and Enrichment tackles various challenges posed by cryptanalysis, they also rely heavily on Intelligence Branch analysts and other members within SIGINT to provide plaintext for analysis (to study the language and type of text), information from [redacted], and samples of ciphertext. In the end, Cryptology can be summed up as:



Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Appendix ? – Data Analysis and Enrichment: Encryption/ Decryption Examples

I. Substitution: "Snow Difference"

```
NMGUDMTQGZ HTMHGTJZI NJZUMT KFTMSGAU AHJOOA SFTTMSUJFZ KOLJW
FZ QGH, HTFQLUJZI TMHFTU FK ZMGT NDJUMFLU SFZWJUJFZA.
```

By counting the frequency with which each letter appears in the encrypted text, the data compiled would look like this:

T 11	H 7	O 3
F 10	G 6	Q 3
J 9	A 4	D 2
M 9	S 4	I 2
U 9	K 3	L 2
Z 9	N 3	W 2

Aside from counting the repetition of letters, picking out patterns of letters would also be useful. In this case, the data would show:

UJFZ	X2
JZI	X2
TMH	X2
TMS	X2

Repeated groups of letters aid in attacking the encrypted message:

NMGUDMTQGZ HTMHGTJZI NJZUMT KFTMSGAU AHJOOA SFTTMSUJFZ KOLJW FZ QGH, HTFQLUJZI TMHFTUFKZMGT NDJUMFLU SFZWJUJFZA.

A very common four-letter ending for a long word is TION. Let's crib that into the text:

```
   T      N        IN    INT     O      T   I      O     TION
NMGUDMTQGZ HTMHGTJZI NJZUMT KFTMSGAU AHJOOA SFTTMSUJFZ

   ID ON     ,    O    IN      O    O  N       IT O T
KOLJW FZ QGH, HTFQLUJZI TMHFTU FK ZMGT NDJUMFLU

 ON ITION .
SFZWJUJFZA.
```

So this looks pretty good. Perhaps the last letter of the last word is S. Let's add that in:

```
   T      N        IN    INT     O     ST S I  S CO    CTION
NMGUDMTQGZ HTMHGTJZI NJZUMT KFTMSGAU AHJOOA SFTTMSUJFZ

   ID ON     ,    O    IN      O    O  N       IT O T
KOLJW FZ QGH, HTFQLUJZI TMHFTU FK ZMGT NDJUMFLU

 ON ITIONS.
SFZWJUJFZA.
```

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

The last word looks like CONDITIONS. We can now fill in the C and D.

```
   T     N       IN   INT    O    ST S I  S CO   CTION
NMGUDMTQGZ HTMHGTJZI NJZUMT KFTMSGAU AHJOOA SFTTMSUJFZ

   ID ON    ,   O   IN     OR  O  N      IT O T
KOLJW FZ QGH, HTFQLUJZI TMHFTU FK ZMGT NDJUMFLU

CONDITIONS.
SFZWJUJFZA.
```

ETC… and finally:

```
WEATHERMAN PREPARING WINTER FORECAST SPILLS CORRECTION
FLUID ON MAP, PRODUCING REPORT OF NEAR WHITEOUT CONDITIONS.
```

Cipher Alphabet: **ADFGHIJKLMNOQSTUWZ**
Plain Alphabet: **SHOAPGIFUEWLMCRTDN**

Tools to help you get started:

- Three-letter words in English are likely to be: THE or AND
- One-letter words in English are either: A or I
- For long words, try TION or ING at the end of the word
- Look for two consecutive letters in the cipher (i.e. QQ), this could represent: SS, TT, LL, NN, etc.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

II. Transposition: "Tomatoes for Launch"

```
AHSWM DUETI LNNYO ATRKE ANIED TMRYS NWIAG DTATB EIDSS MOANO
SRTNL LRBMT HHISI AAFEO WTTDI ENWTM EISAV USISW THTOW SNISW
YMTON EEHCI KIOAO UENOT TIIIR HECOB DT
```

Frequencies:

T 16	D 6	L 3
I 15	H 6	U 3
E 12	M 6	Y 3
A 10	W 6	K 2
N 10	R 5	F 1
O 10	B 3	G 1
S 10	C 3	V 1

INFORMATION GIVE:

Matrix: 11X12
Key: 4 9 12 8 1 5 10 7 6 11 3 2

Reconstructing the Matrix:
Divide cipher into chunks of row size (11)and label the chunks from 1 to column size (12):

1	2	3
AHSWM DUETI L	NNYO ATRKE AN	IED TMRYS NWI
4	**5**	**6**
AG DTATB EIDS	S MOANO SRTNL	LRBMT HHISI A
7	**8**	**9**
AFEO WTTDI EN	WTM EISAV USI	SW THTOW SNIS
10	**11**	**12**
W YMTON EEHCI	KIOAO UENOT T	IIIR HECOB DT

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Draw a blank 11X12 matrix and place the key at the top:

4	9	12	8	1	5	10	7	6	11	3	2

Place the first chunk of letters in the column labelled "1":

1	2	3
AHSWM DUETI L	NNYO ATRKE AN	IED TMRYS NWI
4	5	6
AG DTATB EIDS	S MOANO SRTNL	LRBMT HHISI A
7	8	9
AFEO WTTDI EN	WTM EISAV USI	SW THTOW SNIS
10	11	12
W YMTON EEHCI	KIOAO UENOT T	IIIR HECOB DT

4	9	12	8	1	5	10	7	6	11	3	2
				A							
				H							
				S							
				W							
				M							
				D							
				U							
				E							
				T							
				I							
				L							

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Please the second chunk in the column labelled "2":

1	**2**	3
AHSWM DUETI L	**NNYO ATRKE AN**	IED TMRYS NWI
4	5	6
AG DTATB EIDS	S MOANO SRTNL	LRBMT HHISI A
7	8	9
AFEO WTTDI EN	WTM EISAV USI	SW THTOW SNIS
10	11	12
W YMTON EEHCI	KIOAO UENOT T	IIIR HECOB DT

4	9 12 8			1	5 10 7			6 11 3			2
				A							N
				H							N
				S							Y
				W							O
				M							A
				D							T
				U							R
				E							K
				T							E
				I							A
				L							N

Continue filling in the columns according to the numbers until:

4	9 12 8			1	5 10 7			6 11 3			2
A S		I	W	A S		W	A	L	K	I	N
G W		I	T	H	M	Y	F	R	I	E	N
D	T	I M		S O		M	E B		O	D	Y
T H		R	E	W	A	T O		M	A	T O	
A	T	H	I	M N		O	W	T	O	M A	
T	O	E	S	D O	N		T	H U		R	T
B	E	C A	U		S	E	T H	E		Y R	
E C		O	V	E R		E D		I	N	S	K
I	N B		U T		T	H	I	S	O	N E	
D I	D		S	I N		C	E	I	T	W	A
S S		T	I	L	L	I N		A	T	I N	

In Plain Text: (Note: Punctuation was added to ease readability.)

AS I WAS WALKING WITH MY FRIEND TIM, SOMEBODY THREW A TOMATO AT HIM. NOW TOMATOES DON'T HURT BECAUSE THEY'RE COVERED IN SKIN, BUT THIS ONE DID SINCE IT WAS STILL IN A TIN!

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

appendix F

Supplementary Information: SIGINT Collaboration using Web 2.0

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

A FICTIONAL ACCOUNT OF HOW WEB 2.0 TECHNOLOGIES COULD BE IMPLEMENTED.

Corporal Jones had seen it happen – he was the driver of the rear vehicle when the explosion occurred. This time there had been no Canadian casualties and he smiled, knowing that he had personally been involved in the success. Unfortunately, this was not the case. A mere three weeks ago; a similar roadside bomb had caused one death and several injuries. Corporal Jones had been driving just behind the lead vehicle and had seen the events unfold. Immediately following, he recorded his recollections into his personal digital assistant (PDA), taking care to describe the events that happened. He also used the camera function in the PDA to take pictures of the scene. Inside the wire that night, he updated his blog and downloaded the pictures. He carefully tagged his entries, knowing that they would be used by others to learn about the incident.

Indeed, over the next couple of days, many members accessed his blog and pictures. The rapid training team in theatre used Jones' account, along with others' experiences, to update the "ambush stimulation game" used to train drivers in theatre. This update was instantly available on the network and was now being used at the training school back in Canada. Many of his fellow soldiers and officers had also accessed his blog.

In fact, his account had been voted by his peers as "highly relevant and useful" and now appeared on the top of the wiki-based lessons-learned page. After being scanned, the page was fed (via RSS) to nearly 80% of the Canadian Forces (CF). So when the lead driver had recognized the potential danger and took evasive action – there was no luck involved. The vast network and social production tools available to DND/CF had ensured that Jones' knowledge was quickly and effectively shared.[1]

HOW YOU CAN CONTRIBUTE

Blogs – brainstorm, comment on conversation threads
- Start or reply to discussion threads in [redacted]

Wikis – store group knowledge, collaboratively work on documents
- Edit, create a wiki page or provide comments on the discussion page in the [redacted]

Social bookmarking – tool for sharing/indexing web/wiki pages
- Tag your favourite web or wiki pages in [redacted]

Mashups – visual tools that allows users to connect with multiple forms of digital information
- Search for language information in [redacted] and when released, for OSINT material in [redacted]

1. Verson, John, LCdr Bruce Forrester, Leesa Tanner Transformation in the CF: Understanding the Impact of Network Technologies on the Design of Work – Social and Peer Production, April 2007.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

WEB 2.0 LINKS

CEO [redacted]	[redacted]	Canadian citizens only
[redacted]	[redacted]	[redacted]
CSEC Blog	[redacted]	
CSEC [redacted]		[redacted]
CSEC SIGINT Tradecraft		
Analyst Forum	[redacted]	
CSEC Tweets (micro blog)		
CSEC [redacted]		
[redacted]		
Mandrake [redacted]	[redacted]	(requires Mandrake account)
[redacted]		

FULL ACCESS		
[redacted]	[redacted] (CSEC)	[redacted]
[redacted]	[redacted]	
	GC [redacted]	Mandrake [redacted]
NO ACCESS		
[redacted]		

2. CSEC employees can use their LDAP log-in after creating an account.

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

appendix G

Supplementary Information: Part V.1 of the National Defence Act

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Below is Part V.1 of the *National Defence Act*. For more information on CSEC's legislations and legal requirements please direct your inquiries to your immediate supervisor for clarifications.

***NATIONAL DEFENCE ACT*—PART V.1: COMMUNICATIONS SECURITY ESTABLISHMENT**

Definitions: 273.61 The following definitions apply in this Part.

"CANADIAN"

"Canadian" means a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act* or a body corporate incorporated and continued under the laws of Canada or a province.

"ENTITY"

"entity" means a person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state.

"FOREIGN INTELLIGENCE"

"foreign intelligence" means information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.

"GLOBAL INFORMATION INFRASTRUCTURE"

"global information infrastructure" includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or networks.

"MINISTER"

"Minister" means the Minister of National Defence or such other member of the Queen's Privy Council as may be designated by the Governor in Council to be responsible for the Communications Security Establishment.

"PRIVATE COMMUNICATION"

"private communication" has the same meaning as in section 183 of the Criminal Code.

2001, c. 41, ss. 102, 128.

COMMUNICATIONS SECURITY ESTABLISHMENT CONTINUED

273.62 (1) The part of the federal public administration known as the Communications Security Establishment is hereby continued.

CHIEF

(2) The Chief of the Communications Security Establishment, under the direction of the Minister or any person designated by the Minister, has the management and control of the Establishment and all matters relating to it.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

DIRECTIONS BY MINISTER

(3) The Minister may issue written directions to the Chief respecting the carrying out of the Chief's duties and functions.

DIRECTIONS NOT STATUTORY INSTRUMENTS

(4) Directions issued under subsection (3) are not statutory instruments within the meaning of the *Statutory Instruments Act*.

2001, c. 41, s. 102; 2003, c. 22, s. 224(E).

APPOINTMENT OF COMMISSIONER

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

DUTIES

(2) The duties of the Commissioner are

c. to review the activities of the Establishment to ensure that they are in compliance with the law;
d. in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
e. to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

ANNUAL REPORT

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

POWERS OF INVESTIGATION

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

EMPLOYMENT OF LEGAL COUNSEL, ADVISERS, ETC.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

DIRECTIONS

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other *Act* of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

TRANSITIONAL

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

2001, c. 41, s. 102.

MANDATE

273.64 (1) The mandate of the Communications Security Establishment is

a. to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
b. to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
c. to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

PROTECTION OF CANADIANS

(2) Activities carried out under paragraphs (1)(a) and (b)

a. shall not be directed at Canadians or any person in Canada; and
b. shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

LIMITATIONS IMPOSED BY LAW

(3) Activities carried out under paragraph (1)(c) are subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties.

2001, c. 41, s. 102.

MINISTERIAL AUTHORIZATION

273.65 (1) The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

CONDITIONS FOR AUTHORIZATION

(2) The Minister may only issue an authorization under subsection (1) if satisfied that

a. the interception will be directed at foreign entities located outside Canada;
b. the information to be obtained could not reasonably be obtained by other means;
c. the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
d. satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

MINISTERIAL AUTHORIZATION

(3) The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the Criminal Code, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

CONDITIONS FOR AUTHORIZATION

(4) The Minister may only issue an authorization under subsection (3) if satisfied that

a. the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks;
b. the information to be obtained could not reasonably be obtained by other means;
c. the consent of persons whose private communications may be intercepted cannot reasonably be obtained;
d. satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and
e. satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.

MINISTERIAL CONDITIONS

(5) An authorization made under this section may contain any conditions that the Minister considers advisable to protect the privacy of Canadians, including additional measures to restrict the use and retention of, the access to, and the form and manner of disclosure of, information derived from the private communications.

CANADIAN FORCES

(6) The Minister of National Defence may issue directions for the Canadian Forces to support the Establishment in carrying out activities authorized under this section.

DIRECTIONS NOT STATUTORY INSTRUMENTS

(7) Authorizations issued under subsections (1) and (3) and directions issued under subsection (6) are not statutory instruments within the meaning of the *Statutory Instruments Act*.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

REVIEW OF AUTHORIZATIONS
(8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

MEANING OF "GOVERNMENT OF CANADA"
(9) In this section, "Government of Canada" means a federal institution, as defined in subsection 3(1) of the *Official Languages Act*.

2001, c. 41, s. 102.

LIMITS ON ACTIVITIES
273.66 The Communications Security Establishment may only undertake activities that are within its mandate, consistent with ministerial direction and, if an authorization is required under section 273.65, consistent with the authorization.

2001, c. 41, s. 102.

PROTECTION OF PERSONS
273.67 Notwithstanding any other law, every person or class of persons that is authorized to give effect to an authorization under section 273.65 or any person who assists such a person is justified in taking any reasonable action necessary to give effect to the authorization.

2001, c. 41, s. 102.

EFFECTIVE PERIOD OF AUTHORIZATION
273.68 (1) An authorization is valid for the period specified in it, and may be renewed for any period specified in the renewal. No authorization or renewal may be for a period longer than one year.

VARIANCE OR CANCELLATION OF AUTHORIZATION
(2) An authorization may be varied or cancelled in writing at any time.

2001, c. 41, s. 102.

EXCLUSION OF PART VI OF CRIMINAL CODE
273.69 Part VI of the Criminal Code does not apply in relation to an interception of a communication under the authority of an authorization issued under this Part or in relation to a communication so intercepted.

2001, c. 41, s. 102.

CROWN LIABILITY AND PROCEEDINGS ACT
273.7 No action lies under section 18 of the *Crown Liability and Proceedings Act* in respect of

a. the use or disclosure under this Part of any communication intercepted under the authority of a Ministerial authorization under section 273.65; or
b. the disclosure under this Part of the existence of such a communication.

2001, c. 41, s. 102.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT 101

Acronyms and Glossary

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

ACRONYM	EXPANSION
[redacted]	[redacted]
[redacted]	[redacted] Business Development – part of SIGINT Programs
ADM	Associate Deputy Minister
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
AO	Administrative Officer
[redacted]	[redacted]
ATIP	*Access to Information Act* and *Privacy Act*
BN	Briefing Note
BRLO	British Liaison Office, located in [redacted]
[redacted]	[redacted]
CANSLO	Canadian Special Liaison Office or Canadian Senior Liaison Officer
CANSLO(W)/CANSLO(L)/CANSLO(C)	NSA (Washington, DC, USA)/GCHQ (London, United Kingdom)/DSD (Canberra, Australia)
CAP	Counselling Advisory Program, located in [redacted]
CBSA	Canada Border Services Agency
[redacted]	[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

CCIRM	Collection and Coordination Intelligence Requirements Management. A DND/CF requirement process
CDI	Chief of Defence Intelligence – DND (formerly DGINT)
CDS	Chief of Defence Staff
CEO	Canadian Eyes Only
CF	Canadian Forces
CFB	Canadian Forces Base
CFIA	Canadian Food Inspection Agency
CFIOG	Canadian Forces Information Operations Group
CFS	Canadian Forces Station
CFSOC	Canadian Forces SIGINT Operations Centre
[redacted]	[redacted]
CIA	Central Intelligence Agency (USA)
CIO	Chief Information Officer
Ciphertext	The unintelligible information
[redacted]	[redacted]
CND	Computer Network Defence
[redacted]	[redacted]
COB	Close of Business
COI	Community of Interest

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

COMINT	Communications Intelligence
Comms	Communications
[redacted]	[redacted]
COMSEC	Communications Security
COPCC	Canadian Operational Production and Coordination Centre
[redacted]	[redacted]
CPP	Canada Post Place
[redacted]	[redacted]
CRI	Content Related Information or Cryptologic Research Institute/Cryptologic Research Institute.
CRO	Client Relations Officer
Cryptanalysis	The art and science of breaking the unintelligible information
Cryptologic	Anything pertaining to the mandate and activities of CSEC, including SIGINT or ITS
Cryptology	The branch of mathematics embodying both cryptography & cryptanalysis
Cryptography	The art and science of rendering information unintelligible to outsiders
Cryptosystem or Cipher System	A method or process for transforming properties of the plaintext in order to conceal its meaning
Cryptovariable	Component which is shared between the sender and receiver of the information (this may vary for each encryption)
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
CSOI	Canadian SIGINT Operations Instruction
CT	Counter Terrorism
CVAN	CSEC Visitor Access Notification

IRRELEVANT

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

D2	Operational Policy
D3	External Review & Policy Compliance
DC SIGINT	Deputy Chief SIGINT
DD	Distribution Designator
Decryption	The process of transforming ciphertext into plaintext
DFAIT	Department of Foreign Affairs and International Trade
DFO	Department of Fisheries and Oceans
DG	Director General
DGA	Directorate or Director General Access
DGI	Directorate or Director General Intelligence
DGMS	Director General Military SIGINT (within CSEC)
DGP	Directorate or Director General SIGINT Programs
DGPC	Directorate or Director General Policy and Communications
DLS	Directorate of Legal Services
DM	Deputy Minister
DND	Department of National Defence
DNI	Digital Network Intelligence
DNR	Dialled Number Recognition
DRDC	Defence Research and Development Canada
[redacted]	[redacted]
DSD	Defence Signals Directorate (Australia)
[redacted]	[redacted]
EA	External Affairs or Executive Assistant

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

ECI	Exceptionally Controlled Information
EDB	Edward Drake Building
ELINT	Electronic Intelligence
EM	Electromagnetic
Encryption	The process of transforming plaintext into ciphertext
EPR	End Product Reports
[redacted]	[redacted]
EXCOM	Executive Committee
FBI	Federal Bureau of Investigation
FI	Foreign Intelligence
FISINT	Foreign Instrumentation Signals Intelligence
[redacted]	[redacted]
FTE	Full-Time Employee
FTP	File Transfer Protocol
FY	Fiscal Year; the Government of Canada fiscal year starts on 1 April
GC	Government of Canada. Also known as GoC
GCHQ	Government Communications Headquarters (United Kingdom)
GCR	Government of Canada Requirement
GCSB	Government Communications Security Bureau (New Zealand)
GII	Global Information Infrastructure
[redacted]	[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]	[redacted]
HRA	*Human Rights Act* (UK)
HRMS	Human Resources Management System
HUMINT	Human Intelligence
IB	Insurance Building
IC	Industry Canada
ICOM	Integrated Communications Security (Integrated COMSEC)
[redacted]	[redacted]
IM	Information Management
[redacted]	[redacted]
IO	Information Operations (used in CSEC to refer to an area of SIGINT) or Intelligence Officer (used mainly by CSIS)
IP	Internet Protocol
IR	Information Repository
[redacted]	[redacted]
ISAF	International Security Assistance Force
ISOM	Integrated SIGINT Operational Model

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

ISP	Internet Service Provider
IT	Information Technology
ITAC	Integrated Threat Assessment Centre
JFT	Joint Task Force
JRO	Joint Research Office
[redacted]	[redacted]
KON	Kevin O'Neil Boardroom, located in SLT/B268
LA	Linguist Analyst
LDAP	Lightweight Directory Access Protocol
LTA	Long-Term Accommodation
MA	Ministerial Authorization
[redacted]	[redacted]
MD	Ministerial Directive
MDD	Multiple Distribution Designators
[redacted]	[redacted]
MND	Minister of National Defence
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
[redacted]	[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

MTA	Mid-Term Accommodation
[redacted]	[redacted]
NATO	North Atlantic Treaty Organization
NCS	National Cryptologic School, NSA
NDA	*National Defence Act*
NDHQ	National Defence Headquarters
[redacted]	[redacted]
NGO	Non-Governmental Organization
NSA	National Security Agency (USA) or National Security Advisor
NSPL	National SIGINT Priorities List
[redacted]	[redacted]
OCS	Office of Cryptologic Studies
[redacted]	[redacted]
OCT	Office of Counter Terrorism
[redacted]	[redacted] (Source [redacted] Glossary) [redacted]
OPELINT	Operational ELINT
OPS	Operational Policy
OPSEC	Operational Security
OSI	Open Source Information
OSINT	Open Source Intelligence
OSN	Online Social Networks, also known as social networking sites

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

OSN	On Line Social Networks, also known as social networking sites
[redacted]	[redacted]
PA, PB, PC	Protected A, Protected B, Protected C
[redacted]	[redacted]
PCO	Privy Council Office
PCO IAS	Privy Council Office – Intelligence Assessment Secretariat
PCS	Personal Communications Services
[redacted]	[redacted]
PLM	Product Line Manager or Prime Minister
[redacted]	[redacted]
PIQ	Position Information Questionnaire
PKI	Public Key Infrastructure
Plaintext	The original information
PM	Production Manager or Prime Minister
PMO	Prime Minister's Office
POC	Point of Contact
PPR	Performance Planning and Review
PRI	Personal Record Identifier
[redacted]	[redacted]
PSAC	Public Service Alliance of Canada
[redacted]	[redacted]
RCMP	Royal Canadian Mounted Police

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

RDIMS	Records, Document and Information Management System
[redacted]	[redacted]
RFI	Request for Information
RSS	Really Simple Syndication or Rich Site Summary
ROPI	Responsible Office of Primary Interest
S & I	Security & Intelligence
SA	Special Access
[redacted]	[redacted]
[redacted]	[redacted]
SD	SIGINT Development
SDF	Support to Deployed Forces
[redacted]	[redacted]
SIGDEV	SIGINT Development
SIGINT	Signals Intelligence
SLA	Support to Lawful Access or Service Level Agreement
SLE	Support to Law Enforcement or Second Language Evaluation
SLT	Sir Leonard Tilley building
SME	Subject Matter Expert
SMF	SIGINT Management Forum
SMF	SIGINT Management Forum

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SMO	Support to Military Operations
SMT	Senior Management Team
[redacted]	[redacted]
SOP	Standard Operating Procedure
[redacted]	[redacted]
SPR	SIGINT Programs Requirements
[redacted]	[redacted]
SPOC	SIGINT Programs Oversight & Compliance OR SIGINT Programs Operational Coordination
SPOR	SIGINT Programs Operational Requirements
[redacted]	[redacted]
[redacted]	[redacted]
SSD	SIGINT Systems Development
[redacted]	[redacted]
STU	Secure Telephone Unit
SUSLO	Special US Liaison Office
[redacted]	[redacted]
TBA	To be Announced
TBD	To be Determined
TBS	Treasury Board of Canada Secretariat

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

TK	Talent-Keyhole
TL	Team Leader
[redacted]	[redacted]
TPI	Two Person Integrity
TS	Top Secret
TSSA	Top Secret Special Access
[redacted]	[redacted]
VTC	Video Teleconferencing
[redacted]	[redacted]
WTR	Write-to-Release

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT 101 GLOSSARY

5 EYES

The Quinquepartite SIGINT relationship between the Australia (DSD), Canada (CSEC), New Zealand (GCSB), the United States (NSA), and the United Kingdom (GCHQ). NSA uses "FVEY" as a short-form for Five-Eyes.

[redacted] ANALYST

An analyst using one of any combination of tools/ tradecraft to [redacted] a SIGINT target's [redacted] Proficient in metadata, this analyst uses a variety of analytic techniques in order to identify [redacted]

Within the Intelligence Branch of CSEC SIGINT, the [redacted] Analyst position is classified at the UNI-08 level, and linguist analysts and intelligence analysts must complete a competency framework and be approved by a selection board in order to be designated as an [redacted] Analyst.

ACCESS TO INFORMATION ACT

The purpose of the *Access to Information Act* is to provide a right of access to information in records under the control of a Government of Canada (GC) institution in accordance with the principle that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government. The *Act* provides for exceptions to the disclosure of information that are relevant to CSEC, such as section 15(1) regarding information on international affairs and defence.

ACTION-ON

Any action, or decision to act, taken on the basis of COMINT information, which might jeopardize the COMINT source. Action-on usually involves a sanitization. (Source: OPS-1-1).

[redacted] SIGINT COLLECTION

[redacted]

ACTIVITY

1. The volume and type of [redacted] communications.
2. A unit, organization, or installation performing a function or mission. (Source: [redacted]

ACTIVITY AUTHORIZATION REQUEST (AAR)

[redacted]
(Source: [redacted] Glossary).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

ANALYSIS

The process of reviewing and collating essential elements of information (EEIs) to reach a reasoned conclusion. (Source: [redacted]

ANNOTATION

An explanatory note which may provide information about the content of the information. In the case of SIGINT traffic, to annotate a document would consist of adding the appropriate privacy annotation concerning the traffic content (i.e. one-end Canadian, etc…).

[redacted] (Source: [redacted] Glossary.)

[redacted] (Source: [redacted] Glossary).

[redacted] (Source: [redacted] Glossary).

BLOGS

Online journal (weblog) which can be organized by an individual or community of interest. Entries are usually displayed in reverse chronological order. (Reference: Wikipedia). The term blog can also be used as a verb, in the context of maintaining or adding content to a blog. CSEC 2.0 includes a corporate blogging service. The corporate blogging service [redacted]

[redacted] (Source: [redacted] Glossary).

CANADIAN

Canadian refers to: a Canadian citizen, a person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act* (IRPA), and who has not subsequently lost that status under that *Act*, or, a corporation incorporated under an *Act* of Parliament or of the legislature of a province. Canadian organizations are accorded the same protection as Canadian citizens and corporations. (Source: OPS-1).

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

CANADIAN EYES ONLY
Control markings that indicate that the reports contain intelligence information that is of a sensitive nature either to Canada or to a Second Party country; therefore, such reports are limited to a Canadian readership and must not be released to Second Parties. (Source: SIGINT Report Writing Basics Course, S121).

CANADIAN EYES ONLY REPORT
Reports containing intelligence information that is of a sensitive nature either to Canada or to a Second Party country; therefore, such reports are limited to a Canadian readership and must not be released to Second Parties. (Source: SIGINT Report Writing Basics Course, S121).

CANADIAN SECURITY AND INTELLIGENCE COMMUNITY
See Security and Intelligence Community.

CANADIAN SECURITY INTELLIGENCE SERVICE
Canadian agency whose role is "to investigate threats, analyze information and produce intelligence; it then reports to, and advises, the Government of Canada, so as to protect the country and its citizens". (Source: CSIS website).

CANADIAN OPERATIONAL PRODUCTION AND COORDINATION CENTRE
CSEC's 24/7 point of contact to the 5-eyes community as well as all Government of Canada departments and military personnel within Canada and abroad.

[redacted] (Source: [redacted]

[redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

CATEGORY

[redacted] (Source: [redacted] Glossary; Guide to Tasking, Targeting and Dataflow Terminology).

CAVEAT

Indicator of additional handling or dissemination restrictions or procedures restrictions on information or services (other than classification) that must be enforced.

CERRID

CSEC's Records, Document and Information Management System (RDIMS) software solution.

[redacted]

CLASSIFICATION/ CLASSIFIED INFORMATION

Information that if compromised would affect the national interest or the national security of Canada.

[redacted] (Source: [redacted] Glossary).

CLIENT

Any authorized Canadian Government official or organization that receives SIGINT. (Source: [redacted].

COMPUTER NETWORK DEFENCE

Any activities taken to enhance CSEC's capability to analyze, detect, predict and prevent computer network attacks against Government of Canada networks. (Source: CSEC OPS-1-14 Procedures for CND activities).

[redacted]

COLLECTION

The act of obtaining traffic by SIGINT for the purpose of producing intelligence. Collection involves the acquiring, recording and monitoring of target signals. (Source: [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

COMMUNICATIONS

The aggregate either of several means of conveying information or of the information thus conveyed. It is a plural noun, not an adjective. The adjectival form has no terminal "s", e.g. communication plan. (Source: [redacted]

COMMUNICATIONS INTELLIGENCE (COMINT)

Technical and intelligence information derived from foreign communications [redacted] by those other than the intended recipients. The intelligence is focused on several different sources, primarily foreign [redacted] sources. (Source: SIGINT Report Writing Basics Course, S121).

COMMUNICATIONS SECURITY

Protective measures designed to deny unauthorized persons information of value which might be derived from the possession or study of telecommunications, and to ensure the authenticity of communications. Such protection includes the application of crypto security, emission security, and transmission security measures to electrical systems that generate, process, or handle national-security related information. It also includes the application of physical security to communications security information or materials. (Source: [redacted]

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

Canada's National Cryptologic Agency and a member of the Canadian Security and Intelligence (S&I) community. CSEC is responsible to the Minister of National Defence, and is a member of the quinquepartite agreement (See 5-Eyes).

[redacted] (Source: [redacted]

CONFIDENTIAL

A specific end product series that includes only plain-language raw traffic communications that may be disseminated outside COMINT channels.

A classification that refers to information that, if compromised, may potentially cause "injury to the national interest".

[redacted] (Source: [redacted]

[redacted] (Source: [redacted] Glossary).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

IRRELEVANT

COVERNAME
A name used to represent or conceal the identity of a person, place or thing. (Source: [redacted]

COVERTERM
A word, number, letter or combination thereof, used to represent or conceal the identity of a person, place or thing. (Source: [redacted]

CRYPTANALYSIS
The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plaintext without prior knowledge of the system or key. (Source: [redacted]

CRYPTOGRAPHY
The art and science of rendering information unintelligible to outsiders.

CRYPTOLOGIC
(adjective) Anything pertaining to the business of either SIGINT or ITS. (noun) Algorithm which encrypts/decrypts data.

CRYPTOLOGY
The branch of mathematics embodying both cryptography and cryptanalysis. (Source: [redacted]

CRYPTOVARIABLE
Component in a cryptosystem which is shared between the sender and receiver of the information. The cryptovariable is generally the sole element of the cryptosystem which needs to be kept secret.

CSE 2010/ CSEC 2010
Vision and strategy document published in 2006 to describe CSEC's direction until 2010.

CSEC 2.0
Also known as the CSEC Web Modernization Project. The CSEC 2.0 intranet will include social media tools such as corporate blogging and microblogging (Tweets), fora, video sharing service [redacted] and wiki [redacted]

CSEC COMMISSIONER
A supernumerary or a retired judge of a superior court who reviews CSEC activities to ensure they are in compliance with the law; in response to a complaint, undertakes any investigation that he considers necessary, and informs the Minister of National Defence and Attorney General of any activity not in compliance with the law. The Commissioner is responsible for an annual report to Minister which is tabled in Parliament. (Source: section 273.63 of the *National Defence Act*).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

CSEC MANDATE A

Pursuant to Part V.1 of the *National Defence Act* (NDA), CSEC has three mandates. Mandate A: To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities.

CSEC MANDATE B

Pursuant to Part V.1 of the *National Defence Act* (NDA), CSEC has three mandates. Mandate B: To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructure of importance to the Government of Canada.

IRRELEVANT

CSEC MANDATE RESTRICTIONS

For CSEC's Mandate A and B:

1. activities will not be directed at Canadians or anybody in Canada;
2. and are subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

IRRELEVANT

CSIS ACT

An *Act* to establish the Canadian Security Intelligence Service. The *Act* sets out CSIS's mandates, as well as its roles and responsibilities in the execution of its mandates.

[redacted]

[redacted] Target Development/SIGINT Development [redacted]

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

DIALLED NUMBER RECOGNITION (DNR)
The use of phone numbers (selectors) [redacted] to intercept [redacted] Fax [redacted] communications over the Global Information Infrastructure (GII). (Source: [redacted] Glossary; Guide to Tasking, Targeting and Dataflow Terminology).

DIGITAL NETWORK INTELLIGENCE (DNI)
The use of keywords (selectors) to intercept [redacted] communication over the Global Network. (Source [redacted] Glossary).

[redacted] (Source: [redacted] Glossary).

DISTRIBUTION DESIGNATOR
A listing of offices which will receive information. (Source: [redacted] Glossary).

[redacted] (Source: [redacted] Glossary).

E-LEARNING
Learning using online electronic media.

ELECTRONIC INTELLIGENCE
A discipline aimed primarily at the analysis of the non-communications electromagnetic radiations, particularly of radars towards gaining technical and operational intelligence. (Source: [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

END-PRODUCT REPORTS
Foreign intelligence information, derived from SIGINT processes that is made available in readable form to authorized recipients in response to a Government of Canada Requirement. (Source: [redacted]

[redacted] (Source: [redacted] Glossary).

FIVE-EYES
See 5 Eyes.

FOLKSONOMY
Also called social tagging. Folksonomies are a user-generated taxonomy which have been created by online communities to categorize and share web content such as blogs, photographs, etc. The activity of contributing to a folsonomies is known as tagging as the labels used to describe the content are know as tags. See: Social bookmarking. (Reference: [redacted]

FOREIGN INSTRUMENTATION SIGNALS INTELLIGENCE
A discipline aimed primarily at the analysis of electromagnetic emissions associated with testing, and deployment of aerospace, surface, and subsurface systems. It includes, but is not limited to, signals from telemetry, beaconing, [redacted]

FOREIGN INTELLIGENCE
Information or intelligence about the capabilities, intentions, or activities of a foreign individual, state, organization, or terrorist group, as they relate to international affairs, defence or security. (Source: *National Defence Act*, section 273.61).

Within the Canadian context, its purposes is to protect Canada's interests, to facilitate the policy process, and to provide advantage in the pursuit of overall government policy objectives. In general, FI deals with events outside Canada, including foreign reaction to developments within Canada. CSEC provides FI to Canadian partners and allies.

FORUMS
A forum is a web version of a bulletin board allowing people to post messages (known as posts). Posts found under a topic show up in a threaded fashion. Forums allow for the creation of communities of people who share a common interest. For example, CSEC has a SIGINT tradecraft forum for information sharing. The LTA forum has also been a place of much discussion and clarifying of information and questions. This is how forums are useful in the workplace in sharing and clarifying information. [redacted] (Source: Social Media Student Guide).

[redacted] (Source: [redacted] Glossary).

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

GAMMA

A sub-control system of the COMINT control system that provides additional protection for very sensitive COMINT reports and related material.

[redacted] (Source: [redacted] Glossary).

[redacted]

GLOBAL INFORMATION INFRASTRUCTURE

Refers to ectromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions systems and networks. (Source: section 2.73.61 of the *National Defence Act*).

[redacted] (Source: [redacted] Foundations of SIGINT).

[redacted] (Source: [redacted] Glossary).

GOVERNMENT OF CANADA REQUIREMENTS

Numeric values that reflect the Canadian Government's ongoing intelligence requirements. GCRs are made up of the following components: [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

HUMAN INTELLIGENCE

Clandestine and overt collection techniques used mainly by the Canadian Security Intelligence Services (CSIS), Department of Foreign Affairs and International Trade (DFAIT), Royal Canadian Mounted Policy (RCMP), the United States' Central Intelligence Agency (CIA), Departments of State, Department of Defence, and the Federal Bureau of Intelligence (FBI). [redacted] (Source: SIGINT Baseline Program, Introduction to Intelligence; [redacted] Foundations of SIGINT).

[redacted]

INTELLIGENCE

The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign powers. (Source: [redacted] Foundations of SIGINT).

INTELLIGENCE CYCLE

The steps by which information is converted into intelligence and made available to users. The steps of the cycle are: planning and direction; collection; processing; analysis and production, and dissemination. (Source: [redacted] Foundations of SIGINT).

[redacted]

INTERCEPT

The collection of the electromagnetic emissions of others without obtaining the consent of the originator and ordinarily without delaying or preventing the reception of those emissions by the intended addresses. SIGINT involves intercepting foreign communications as they transit the Global Information Infrastructure. Intercept differs from collection as entities are not tasked. (Source: [redacted]

[redacted] (Source: [redacted] Glossary).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] (Source: [redacted] Glossary).

INTERNET SERVICE PROVIDER

A vendor that provides access for customers (companies and private individuals) to the Internet. Users typically reach an ISP by either dialling up through their own computer or over a dedicated line installed by their phone company. Internet access. Internet Service Provider (ISP) provides customers with access to the Internet.

[redacted] (Source: [redacted] Glossary).

[redacted] DNI collection. (Source: [redacted]

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

Used as the CSEC corporate directory.

[redacted] (Source: [redacted] Glossary).

MANDRAKE

CSEC's secure online link with the Government of Canada (GC) partners in the security and intelligence (S&I) community. Users are able to access the extranet site of each department, and are thus able to access open source and classified information. MANDRAKE also includes a directory on the main page where users can search for contact in the other departments. (Source: SIGINT Report Writing Basics Course, S121).

MASHUPS

Web applications that combines data from more than one source into a new integrated tool such as [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

METADATA

Information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content. (Source: OPS 1-6 [redacted] Procedures).

MICROBLOGGING

A form of blogging that allows users to write brief updates (usually 140 characters) exchange of quick, frequent answers to short questions or micromedia such as photo or audio clips. These messages can be usually submitted by a variety of methods such as text messaging, instant messaging, email or the web. (Reference: Wikipediia). For example: Internet website Twitter, CSEC's Tweets or [redacted]

MINISTERIAL DIRECTIVES

Written directions issued by the Minister of National Defence to the Chief of CSEC in respect of the carrying out of the Chief's duties. MDs may be operational or administrative in nature.

[redacted]

An area within SIGINT Programs that provides CSEC with a cross-organization perspective on all Canadian [redacted] SIGINT collection programs, and works with internal and external organizations to determine the best solution for each specific requirement. This area tracks the [redacted] also monitors tasking and targeting for compliance with CSEC policy and Canadian laws.

MULTIPLE DISTRIBUTION DESIGNATORS

[redacted] DNR selector, [redacted] (Source: [redacted] Glossary).

MY TOOLBAR

Navigation toolbar on CSEC 2.0 containing important information and bookmarks (similar to bookmarks of IE or Firefox). (Source: Social Media Student Guide).

NEED-TO-KNOW

The principle that individuals that are granted information have a valid security clearance and have a legitimate reason to receive classified or protected information to perform their job. Employees are expected to limit their requests to information for which they have a valid need-to-know. (Source: OPS-5-15).

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted] (Source: [redacted] (Source: [redacted]

[redacted] (Source: [redacted] Glossary). [redacted]

ONLINE SOCIAL NETWORKS
British acronym for Online Social Networks, also known as social networking sites.

OPEN SOURCE INFORMATION
Open Source Information (OSI) is comprised of the raw unclassified data that can be put together, generally by an editorial process that provides some filtering and validation. Newspapers, books, broadcasts and general daily reports are part of the OSI world. See: Open Source Intelligence (OSINT) (Source: NATO Open Source Intelligence Handbook).

OPEN SOURCE INTELLIGENCE
OSINT as compared to Open Source Information is intelligence that is produced from unclassified publicly available information collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. OSINT can be used in a variety of different ways including, [redacted] finding background information related to a target, and supporting and verifying SIGINT.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

OPEN SOURCE INTELLIGENCE

Any unclassified, publicly available information that can be found in a variety of different sources including print, television, radio, and the internet. OSINT can be used in a variety of different ways including, [redacted] finding background information related to a target, and supporting and verifying SIGINT.

OPERATIONAL ELINT

The technique whereby COMINT emitters and their characteristics can be identified and geolocated from ELINT satellites.

OPS-1

Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities – Document is one of CSEC's Operational Policy Instruments.

PART V.1 OF THE NATIONAL DEFENCE ACT

CSEC's enabling legislation, enacted as part of the *Anti-Terrorism Act* in November 2001. Provides CSEC with its mandates and establishes CSEC's roles and responsibilities in the execution of its mandates.

[redacted] COLLECTION

[redacted]

PEOPLESOFT

A Human Resources Management System that allows for the seamless integration of data in a collaborative network, while giving end users immediate access to information and services. Using PeopleSoft allows CSEC to manage and optimize the human resources with built-in features that align the human resources strategies with the corporate objectives.

[redacted] allows for the targeting of DNI, DNR [redacted] (Source: [redacted] Glossary).

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

PRIORITY

Method for prioritizing targeting requests. The following guidelines should be adhered to:

- [redacted]
- [redacted]
- [redacted]

(Source: [redacted] Glossary).

PRIVACY ACT

A legislation that protects the privacy of individuals with respect to personal information about themselves held by a government institution, and to provide individuals with a right of access to that information.

PRIVACY ANNOTATION

A private communication, a communication of a Canadian located outside Canada, or a communication which contains information about Canadians must be annotated. Section 2.8 of OPS-1 prescribes that intercept from CSEC collection or acquisition from Second Parties (Mandate A) must be annotated for destruction unless it is foreign intelligence, is essential to protect lives, or contains information on serious criminal activity relating to the security of Canada.

PRIVATE COMMUNICATION

Any oral communication or telecommunication that is made by an originator who is in Canada or is intended by the originator to be received by a person which is in Canada and that is made under circumstance in which is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it. (Source: section 273.61 of the *National Defence Act*).

It is based on geography, and not nationality; neither the originator nor the recipient has to be a Canadian. [redacted]

[redacted] **DIGRAPH**

[redacted] (Source: [redacted] Glossary).

PROTECTED A

Information is of low sensitivity and at limited risk. If compromised, could cause embarrassment or injury to an individual or organization.

PROTECTED B

Information is particularly sensitive. If compromised, certain to cause an invasion of privacy, loss of reputation or competitive advantage.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

PROTECTED C
Information is extremely sensitive and requires special safeguards to protect it. If compromised, could result in serious consequences for an individual or organization, possibly even loss of life.

PROTECTED INFORMATION
Information that if compromised would affect private and non-national interests. Protected Information is classified either as Protected A, Protected B, or Protected C.

[redacted]

RECORDS, DOCUMENT AND INFORMATION MANAGEMENT SYSTEM
RDIMS is a shared systems initiative of the Chief Information Officer (CIO) Branch of the Treasury Board Secretariat. It currently supports a community of over 44,000 users across the Government of Canada.

RESPONSIBLE OFFICE OF PRIMARY INTEREST
For the purpose of the [redacted] database, this is the office which first enters a number into the database. (Source: [redacted] Glossary).

Often used as acronym in place of POC to indicate the area/individuals who are key players or stakeholders.

[redacted] TERMINAL
A CSEC provided computer terminal with access to the World Wide Web (internet). The classification of the terminal is UNCLASSIFIED; no classified information should be created, saved, shared, or transferred on the [redacted] terminal.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SANITIZATION

The process of editing or otherwise disguising COMINT to protect sensitive intelligence sources, methods, techniques or other sensitive characteristics of the data, [redacted] The aim of sanitization is to permit wider dissemination outside of COMINT channels. (Source: OPS-5.9)

SECOND-PARTY

CSEC's SIGINT counterparts and includes: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB). (Source: OPS-1-1).

SECRET

Information that would cause serious injury to the national interest if compromised. Would likely damage relations with friendly governments, raise international tension, or cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.

IRRELEVANT

SECURITY AND INTELLIGENCE COMMUNITY

A large and diverse grouping of Federal Departments and Agencies. All authority ultimately derives from Parliament. Individuals in Cabinet responsible for the Security and Intelligence community include the Prime Minister, Minister of Foreign Affairs, Minister of National Defence, Minister of Public Safety and Emergency Preparedness, Minister of Justice, Minister of Immigration, and the Minister of Transportation. The Privy Council Office coordinates the S & I community. (Source: SIGINT Baseline Program, Introduction to Intelligence).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SELECTOR

Unique identifier of a target within the Global Information Infrastructure (GII). [redacted] that has been designated to select data of interest from [redacted] or that is used as a search criterion in the context of analysing [redacted] (Source: [redacted]

[redacted] (Source: [redacted] Glossary).

SIGINT DEVELOPMENT (SIGDEV/ SD)

A set of multidisciplinary discovery activities performed to anticipate and/or enhance [redacted] current and emerging foreign communications and non-communications systems.

SIGDEV is the art of defining (through analysis [redacted] a comprehensive and definitive description of foreign targets' [redacted] SIGDEV applies to [redacted] SIGDEV underpins SIGINT [redacted] activities and improves the ability to acquire the desired communications to satisfy client's information needs. SIGDEV work can be a full time occupation or simply an aspect of an analyst's overall duties. All SIGDEV efforts must, ultimately, be measured by how they directly improve the SIGINT system's ability to acquire the desired communications to satisfy customers' information needs.

[redacted]

SIGINT REQUIREMENT

A client requirement for signals intelligence. In the CSEC context, this may be expressed in the form of a Government of Canada Requirement (GCR) or a Client Request (CR).

SIGINT TARGET [redacted] PROGRAM

A training program offered to experienced SIGINT analysis to further develop their tradecraft and SIGINT development skills. The [redacted] coordinates this program regularly.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted]

SIGNALS INTELLIGENCE (SIGINT)
Intelligence acquired through the collection of electromagnetic signals. Its challenge is creating intelligence from signals and requirements. It can be broken down into three categories: COMINT; ELINT; FISINT.

[redacted]
An end-product reporting and viewing tool, also used for transcription, and for Client Requests and Feedback. [redacted] contains all end-product reports that CSEC produces or receives from Second Parties, and collateral reports published by [redacted]

SOCIAL BOOKMARKING
Method for Internet/Intranet users to store, organize, search and manage bookmarks with the use of metadata, typically in the form of tags that collectively become a folksonomy (Reference: Wikipedia). Examples include [redacted] Delicious.

SOCIAL NETWORKING SITES
Web-based services that allow individuals to create a public or semi-public profile within a bounded system with the intention of allowing users to connect to each other. Examples include [redacted]

[redacted]
CSEC's [redacted] populated with target information by analysts; the means to target selectors. (Source: [redacted] Glossary).

STATIC IP ADDRESS
Permanently assigned IP address. (Source: [redacted] Glossary).

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

STRONG SELECTOR

A unique identity of a target within the Global Information Infrastructure. Examples of Strong Selectors include such things as [redacted] A strong selector does not include [redacted] The strong selector philosophy is the [redacted] (Source: [redacted] Glossary).

[redacted]
(Source: [redacted] Glossary).

[redacted]

SUPPRESSED INFORMATION

Information excluded from a SIGINT end-product or technical report or an IT Security report because it may reveal the identity of a Canadian or Second Party entity. This information is stored in a limited-access database or system and is replaced in the report by a generic term. Suppressed information includes, but is not limited to, personal identifiers such as names, passport information, [redacted] email addresses, phone numbers, and IP addresses, [redacted] (Source: OPS-1-1).

TACTICAL INTELLIGENCE

Intelligence that is required to plan and conduct tactical operations, specifically battles and engagements to accomplish assigned objectives.

TAGGING

A Web 2.0/social software concept that allows users to add keywords to entries in the system so that similar entries are grouped by this keyword. This increases discoverability of related topics in the system. (Reference: [redacted]

TALENT-KEYHOLE

A control system for information related to, or derived from, satellite reconnaissance systems and products collected by foreign intelligence organizations in collaborating countries.

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

TARGET
A specific entity whose activities are of interest to SIGINT; the people, entities, and organizations [redacted] (Source: [redacted]

TARGET DEVELOPMENT
See SIGINT Development.

TASK
A directive to acquire, record, and monitor a communication link carrying target signals. (Source: [redacted]

A directive to analyze or report intelligence information; the activity deriving therefrom. (Source: [redacted]

In IT, a directive to produce, modify, enhance, or support hardware, software, or documentation. (Source: [redacted]

A request by analysts for [redacted] (Source: [redacted] Glossary).

TASKING
In SIGINT collection, designating a link to [redacted] (Source: [redacted]

Analyst "tasks" a [redacted] This entails work by [redacted] (Source: [redacted] Glossary; Guide to Tasking, Targeting and [redacted] Terminology).

[redacted] (Source: [redacted] Glossary).

THE FLOOR
See Canadian Operational Production and Coordination Centre.

THEATRE
A geographically defined area of military operations.

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

TOP SECRET
Information which, if compromised, would likely cause exceptionally grave injury to the national interest; threaten the internal stability of Canada or allied nations, cause widespread loss of life, cause severe long-term damage to relations with friendly nations, or severely damage the Canadian economy.

TOPIC
[redacted] (Source: [redacted] Glossary).

TRADECRAFT
The development of methods, techniques, [redacted] and processes in order to generate intelligence, and developing the ability to apply this knowledge either manually or through automation. Tradecraft is developed from experience, research, intuition and by the reapplication and redefinition of existing techniques.

TRAFFIC
1. Communications intercepted for SIGINT purposes.
2. The signals transmitted over a communication channel. (Source: [redacted]

[redacted] using the Strong Selection principal. (Source: [redacted] Glossary).

TWEETS
CSEC 2.0 allows for microblogging. A tweet is a short entry used for quick updates or feedback as well as latest news or reminders. (Source: social Media Student Guide).

[redacted] (Source: [redacted] Glossary).

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

[redacted]

CSEC's video sharing website. This web site allows users to upload, share and view videos. The name comes from the use of the letters [redacted] on communiqués sent from CSEC to the 5-eyes partners, to inform all other parties that the communication came from CSEC. (Source: Social Media Student Guide).

VULNERABILITIES

Encompasses evaluation of customer networks, network services, cryptography and its implementation, the search for vulnerabilities in facilities, and the necessary infrastructure to support this effort.

[redacted]

IRRELEVANT

[redacted] (Source: [redacted] Glossary).

WEB 2.0

Also known as social software. Social software enables people to connect or collaborate through computer-mediated communication and to form online communities. The most prominent Web 2.0 tools are blogs, wikis, podcasts, RRS, social networking and content tagging.

WIKI

Web-based tool that allows multiple users to create, modify and organize web page content in a collaborative manner. Wikis are online knowledge-sharing tools. An example is Wikipedia.org, the collaborative encyclopaedia. CSEC's wiki is known as [redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la loi LAI - renseignements non classifiés

[redacted]

WRITE-TO-RELEASE

The SIGINT principle that requires intelligence producers to "write for the consumer", that is, to prepare reports and products at the lowest possible classification level. WTR is proactive sanitization. (Source: [redacted]

[redacted] (Source: [redacted] Glossary).

OTHER RESOURCES

[redacted]

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT 101

Orientation Program

[redacted]