Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC
technologyscientechnologie

The National Critical Infrastructure Interdependency Model—Volume VII

Characterizing the Information and Communications Technology Sector

Paul Chouinard
DRDC – Ottawa Research Centre

Doug Hales
D Hales Consulting Inc.

The body of this CAN UNCLASSIFIED document does not contain the required security banners according to DND security standards. However, it must be treated as CAN UNCLASSIFIED and protected appropriately based on the terms and conditions specified on the covering page.

Defence Research and Development Canada
Reference Document
DRDC-RDDC-2020-D046
April 2020

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Disclaimer: This publication was prepared by Defence Research and Development Canada an agency of the Department of National Defence. The information contained in this publication has been derived and determined through best practice and adherence to the highest standards of responsible conduct of scientific research. This information is intended for the use of the Department of National Defence, the Canadian Armed Forces ("Canada") and Public Safety partners and, as permitted, may be shared with academia, industry, Canada's allies, and the public ("Third Parties"). Any use by, or any reliance on or decisions made based on this publication by Third Parties, are done at their own risk and responsibility. Canada does not assume any liability for any damages or losses which may arise from any use of, or reliance on, the publication.

Endorsement statement: This publication has been published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

© Her Majesty the Queen in Right of Canada (Department of National Defence), 2020

© Sa Majesté la Reine en droit du Canada (Ministère de la Défense nationale), 2020

Abstract

In an increasingly connected and uncertain world, it is important to broaden horizons and appreciate what partners bring to the table and the challenges they face. A National Critical Infrastructure Interdependency Model (NCIM) was developed to assist Public Safety Canada (PS) and Critical Infrastructure (CI) owners and operators identify dependency relationships and recognize imported risk with a view to informing and enhancing resiliency. Characterization of the 10 CI sectors was an important first step. Functional decompositions and logic models were developed to describe each sector as a prelude to developing a relational database and an integrated model. Subsequently a software application (*RiskOutLook*®) was employed to calculate cumulative/cascading risk. This report describes how the *Information and Communications Technology* (ICT) sector was characterized.

Significance to Defence and Security

This work has significant import for Public Safety. Structural seams and organizational handoffs present risks, opportunities for misunderstandings. Ordering dependencies and understanding the nature and significance of imported risks can be used to inform contingency and investment plans. The NCIM was developed in response to a request from the National Cross Sector Forum, and the requirement for a model was noted in the *2014–2017 National Critical Infrastructure Action Plan*. The characterization and logic models describing sectors will help shape internal and external stakeholders' appreciation of functional dependencies and can be used to stimulate dialogue and align assumptions.

The *ICT* sector provides goods and services that are integral to functioning of all other sectors and the Canadian economy. In addition to changing social behaviour, the convergence of computers and communications enabling users to share information in "real-time" has revolutionized business processes facilitating vertical and horizontal integration underwriting globalization and enabling tightly coupled supply chains. Consequently it has introduced new dependencies and potential vulnerabilities. Reliance on telecommunications and the movement of data within and between sectors has become an essential enabler; it has been described as the nervous system that binds CI sectors and through which risk can be transferred. Any substantial disruption of ICT services and/or loss of confidence in the ICT would have significant direct and downstream consequences. Advancing an understanding of functional dependencies and vulnerabilities is a key first step to enhancing resiliency.

Résumé

Dans un monde de plus en plus interconnecté et incertain, il est important d'élargir ses horizons et de comprendre ce que nos partenaires nous apportent, de même que les difficultés auxquelles ils font face. On a élaboré un modèle d'interdépendances des infrastructures essentielles nationales (MIIEN) pour aider Sécurité publique Canada (SPC), de même que les propriétaires et exploitants d'infrastructures essentielles (IE) à déterminer les relations de dépendance et à reconnaître les risques importés en vue de favoriser et d'accroître la résilience. La caractérisation des dix secteurs d'IE représentait une première étape importante dans ce but. On a également élaboré des décompositions fonctionnelles et des modèles logiques pour décrire chaque secteur comme premier pas vers la création d'une base de données relationnelles et d'un modèle intégré. Par la suite, on s'est servi d'une application logicielle (*RiskOutLook*®) pour calculer les risques cumulatifs ou en cascade. Le présent rapport fournit une description de la méthode de caractérisation du secteur des *technologies de l'information et des communications* (TIC).

Importance pour la défense et la sécurité

Ces travaux revêtent une grande importance pour Sécurité publique Canada. Les liens structurels et les transferts organisationnels présentent des risques et peuvent occasionner des malentendus. L'ordonnancement des dépendances et la reconnaissance de la nature et de l'importance des risques importés pour une organisation peuvent être utilisés pour orienter les plans d'urgence et d'investissement. On a élaboré le MIIEN a en réponse à une demande du Forum national intersectoriel, puis on a évoqué la nécessité d'un modèle dans le Plan d'action national 2014–2017 sur les infrastructures essentielles. La caractérisation et les modèles logiques qui servent à décrire les secteurs aidera les intervenants internes et externes à affiner leur compréhension des dépendances fonctionnelles et permettra de faciliter le dialogue et de coordonner les hypothèses.

Le secteur des TIC fournit des biens et services qui font partie intégrante du fonctionnement de tous les autres secteurs et de l'économie canadienne. En plus de modifier les comportements sociaux, la convergence de l'informatique et des communications, qui permet aux utilisateurs de partager de l'information en temps réel, a révolutionné les processus opérationnels en facilitant l'intégration verticale et horizontale qui sous-tend la mondialisation et a permis des chaînes d'approvisionnement étroitement liées. Elle a aussi entraîné de nouvelles dépendances et de possibles vulnérabilités. La dépendance aux télécommunications et à la circulation intrasectorielle et intersectorielle des données est devenue un facteur essentiel; on l'a décrit comme le système nerveux central qui unit les secteurs des IE et permet le transfert de risque. Toute perturbation importante de services de TIC ou de perte de confiance en ceux-ci aurait de graves conséquences directes ou en aval. Les avancées dans la compréhension des dépendances et des vulnérabilités fonctionnelles constituent un premier pas important pour accroître la résilience.

Table of Contents

Abstract . . . i
Significance to Defence and Security . . . i
Résumé . . . ii
Importance pour la défense et la sécurité . . . ii
Table of Contents . . . iii
List of Figures . . . v
List of Tables . . . vi
Acknowledgements . . . vii
1 Introduction . . . 1
1.1 Project Background . . . 1
1.2 Objective . . . 1
1.3 Document Structure . . . 1
2 Modelling Approach . . . 3
2.1 Focusing On Functions . . . 4
2.2 The North American Industry Classification System . . . 5
2.3 Adopting the Approach . . . 6
3 The Information and Communications Technology Sector . . . 8
3.1 Introduction . . . 8
3.2 Partitioning . . . 9
3.3 Characterizing . . . 11
3.3.1 Transmission Means . . . 11
3.3.2 Roles . . . 18
3.4 Telecommunications Sub-Model . . . 21
3.4.1 Radio and Television Broadcasting . . . 23
3.4.2 Internet . . . 24
3.5 Information Services Sub-Model . . . 24
3.6 Generic Models . . . 26
3.7 RiskOutLook Representation . . . 28
4 Trends and Vulnerabilities . . . 31
5 Conclusion . . . 32
5.1 Way Ahead . . . 32
References . . . 33
Annex A Key Stakeholders . . . 36
Annex B Information and Communications Technology NCIM Functions . . . 38
Bibliography . . . 41
List of Symbols/Abbreviations/Acronyms/Initialisms . . . 42

List of Figures

Figure 1: Modelling approach. 4
Figure 2: Scenarios, functions and assets. 5
Figure 3: Canada's ICT companies by sub-sector. 8
Figure 4: Communications sector architecture. 12
Figure 5: Cable access architecture. 13
Figure 6: Wireless communications architecture. 14
Figure 7: Satellite communications architecture. 15
Figure 8: Illustrative mesh network. 16
Figure 9: Broadcast architecture.. 17
Figure 10: Characterizing telecommunications CI by transmission means. 18
Figure 11: Illustrative single and multi-exchange networks. 18
Figure 12: Illustrative telecommunications network. 19
Figure 13: Management and Control Planes for ICT Operations. 20
Figure 14: Characterizing telecommunications services by transmission means and component role. 21
Figure 15: Telecommunications—network maintenance and repair. 22
Figure 16: Telecommunications sub-model—network operations. 23
Figure 17: Information services sub-model. 25
Figure 18: Generic core facilities model. 26
Figure 19: Generic management model. 27
Figure 20: Generic maintenance and repair model. 27
Figure 21: Wireless services.. 29
Figure 22: Telecommunications intra-sector dependencies. 30

List of Tables

Table 1: NAICS extract.. 6
Table 2: National CI sector and sub-models.. 6
Table 3: NAICS to NCIM Mapping for the ICT Sector. 10
Table B.1: Telecommunications NCIM functions. 38
Table B.2: Information services NCIM functions. 40
Table B.3: Radio wave NCIM functions. 40

Acknowledgements

The authors would like to acknowledge the contributions of Public Safety Canada. Team composition has changed over life of the project; their commitment to advise and advance the characterization of CI sectors has not.

1 Introduction

1.1 Project Background

CI is at risk from natural, intentional and accidental hazards, and risks can be propagated and exacerbated by the complex system of interdependencies leading to cascading effects between sectors and across borders. This interdependence and increasing societal reliance on connectivity, services and just-in-time supplies chains pose concerns and challenges and place a premium on communications, collaboration and coordination i.e., a *whole of society* response to major emergencies/disasters.

In 2009 the Federal Government, the Provinces and Territories agreed on a *National Strategy for Critical Infrastructure* (Public Safety Canada, 2009) and subsequently on an *Action Plan for Critical Infrastructure* (Public Safety Canada, 2014). The intent of the Strategy was to strengthen resilience through building partnerships, applying an all hazards risk management approach and promoting the timely sharing and protection of information. The Action Plan outlined a number of initiatives supporting implementation of the National Strategy, one of which was the creation of Sector networks and establishment of a cross sector forum as the basis for collaborative work and information sharing. Note was taken of a previous CI interdependency modeling effort led by Emergency Management Ontario (EMO), using *RiskOutLook*® software. It foretold the benefits and underscored the requirement for an equivalent national model. At the 2012 National Cross-Sector Forum (NCSF) meeting, it was proposed that this methodology be exported, extended and exploited, and that Sector models and an integrated national model be developed to support an analysis of CI interdependencies within and between sectors. It was agreed that Public Safety Canada (PS) and the Centre for Security Science (CSS) would partner and lead the project.

Neither the National Strategy nor Action Plan offered a detailed description of CI Sectors, although an earlier Government of Canada Position Paper did describe illustrative "sample sub-sectors" (Public Safety and Emergency Preparedness Canada, 2004). One of the immediate challenges faced was to describe Sectors in sufficient detail to support modelling efforts. The methodology which emerged and was adopted is outlined below (Figure 1). The first step involved orientation and scoping—studying and structuring the problem space (e.g., identifying potential utility of the model, developing a basic understanding of each Sector and choosing an integrating framework suitable for all sectors). Open source literature research followed. Characterizations for each CI Sector were generated with logic models describing key functions and relationships.

1.2 Objective

The objective of this Reference Document is to describe characterization of *the Information and Communications Technology (ICT)* sector—functions, upstream and downstream dependencies and vulnerabilities.

1.3 Document Structure

This Document consists of a number of discreet sections:

- Section One outlines the project objective and scope;

- Section Two discusses the modelling approach adopted and the key concepts which informed and framed development of the model;
- Section Three provides an overview of the ICT sector; and
- Section Five summarizes the conclusions reached relating to both the methodology and the model, and notes the proposed Way Ahead.

2 Modelling Approach

Critical infrastructure refers to "the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government." The NCIM aspires to develop a more fulsome appreciation of the relationships between the 10 CI Sectors which Canada recognises (listed below):

1. Energy and Utilities;
2. Finance;
3. Food;
4. Government;
5. Health;
6. Information and Communications Technology (ICT);
7. Manufacturing;
8. Safety;
9. Transportation; and
10. Water.

The approach adopted in developing Sector Characterizations is outlined below (Figure 1). The first step involved orientation and scoping—studying and structuring the problem space. An open source literature research followed. Sector characterizations were generated following development of logic models for each CI sector describing key functions and relationships. Federal Lead Departments were consulted and, in some cases, Subject Matter Experts (SMEs) were contracted to review the logic models. Functional decompositions and dependent relationships were captured in a Microsoft Access database. A list of key Federal Government stakeholders can be found at Annex A.

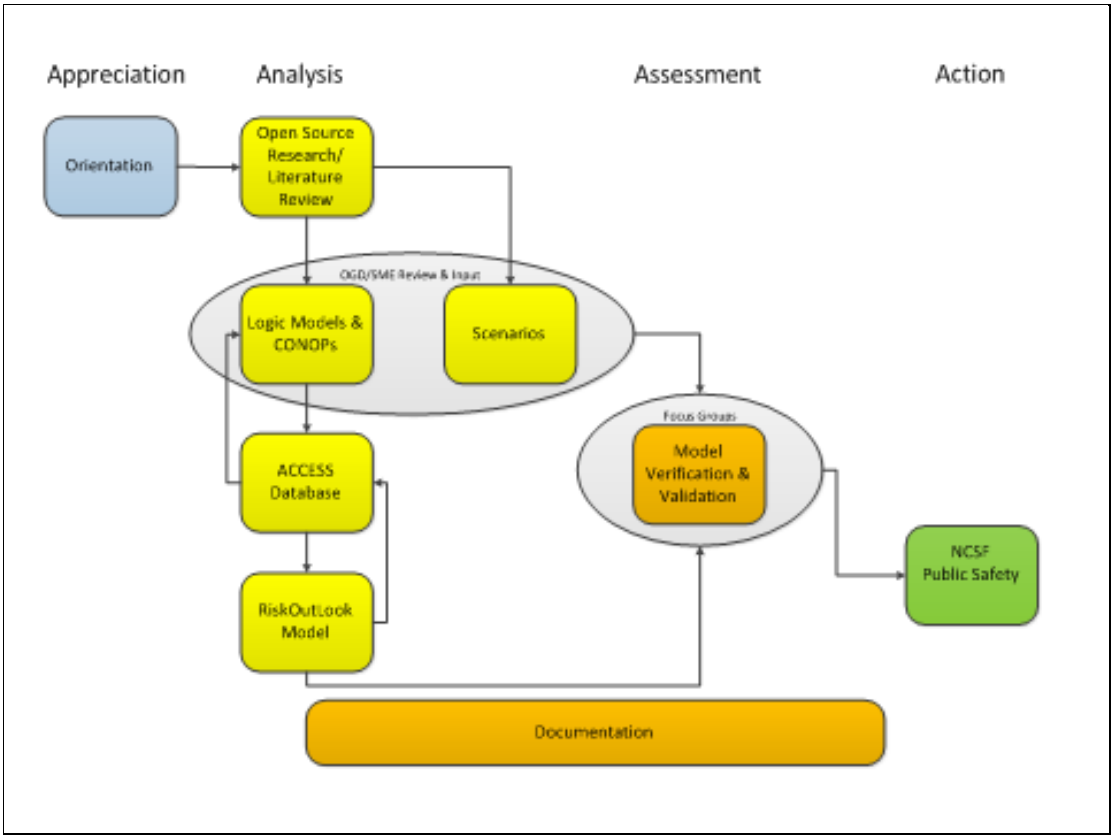

Figure 1: *Modelling approach.*

2.1 Focusing On Functions

Intuition, research and discussions with U.S. Department of Homeland Security (DHS) staff confirmed that past efforts which adopted an asset-based approach found that many CI owners and operators were reluctant to disclose (what they considered) proprietary details e.g., inventory, location and network structure—underlying their operations. Maintaining currency proved an additional challenge; significant staff effort would be required to keep a national asset inventory up to date. Further, an awareness of assets alone is insufficient to understand the full impact on critical infrastructure lying downstream. Complementary knowledge of the business operations (i.e., processes or functions) which the assets support is required. Lastly, it was suspected that there might be a temptation to exploit such a model to provide (near) real time situational awareness decision support. Developing this type of decision-support tool would involve satisfying an additional set of requirements given that liabilities could be incurred if plans were based on outdated and incorrect information or processing delays. Hence it was decided to adopt a functional approach in lieu.

Figure 2 illustrates the relationship between scenarios, assets and functions. Scenarios invoke functional requirements—most of which can be described in terms of services. Employing functional requirements as ends introduces a level of abstraction which avoids a premature focus on ways and means. An integrating framework promotes semantic interoperability and provides an organizing or ordering structure. It also enables decomposition and analysis and aggregation and synthesis. There is a

requirement to relate conceptual to physical models to assess if and how well physical, human and virtual assets satisfy functional requirements. Representative risk scenarios are used; they establish context, bound the scope and define functional requirements. Assets are the third leg in the stool. The scenario situates (ad restricts) the data collection requirements and the functional framework provides a schema for organizing and structuring information. This approach offers several advantages, notably adaptability and scalability.

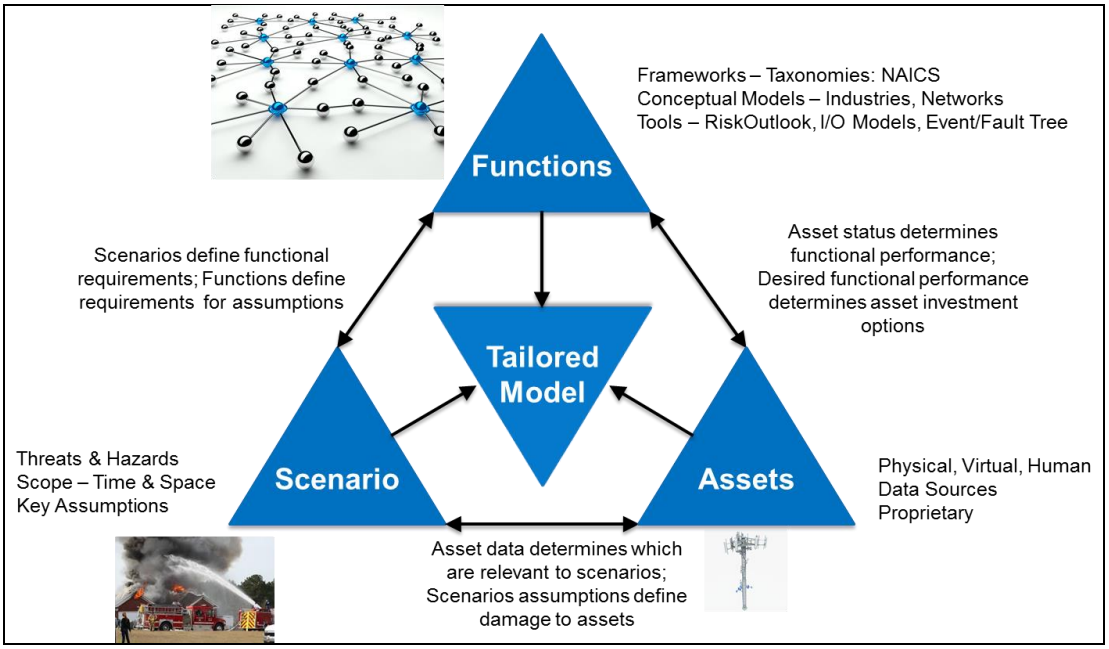

Figure 2: *Scenarios, functions and assets.*

2.2 The North American Industry Classification System

The North American Industry Classification System (NAICS) was adopted and adapted to provide an integrating framework (Statistics Canada, 2017). It provides an exhaustive and authoritative characterization of national economic activities. Adoption involved tweaking the NAICS to establish a service oriented perspective and extending the NAICS to covered activities, particularly those invoked in the Safety Sector, which are not a significant part of routine economic activities and included. Nonetheless the NAICS provided the departure point for developing an integrating framework. It offered an established organizational structure a basis for cataloguing and relating CI functions ad a comprehensive set of agreed definitions. Two other key advantages are worth noting: 1) the hierarchical structure of the NAICS (Table 1) helped to ensure a consistent level of resolution when defining functions/model entities, 2) the NAICS is used by Statistics Canada and the associated data bank provides a sound basis for assessing the economic impact of a risk.

Table 1: *NAICS extract.*

	NAICS Code	NAICS Title
Sector	51	Information and Cultural Industries
Sub-sector	515	Broadcasting (except Internet)
Group	5151	Radio and Television Broadcasting
Industry	51511	Radio Broadcasting

The NAICS taxonomy was only a starting point for the development of a CI functional taxonomy. Extension of the NAICS was anticipated and was required for some sectors such as the Water and Safety sectors.

2.3 Adopting the Approach

Using, insofar as possible NAICS units as the building blocks, logic models and characterizations/concepts of operations (CONOPs) describing key functions and relationships were generated for each of the 10 national CI sectors.[1] In many cases sub-models were required e.g., Electricity, Petroleum and Natural Gas models to characterize the Energy Sector; Watershed Management, Drinking Water and Waste Water to characterize the Water Sector. Sector and sub-models are shown below (Table 2). In some cases, sub-model (e.g., Insurance) were not developed fully, but could be if a requirement to do so was identified.

Table 2: *National CI sector and sub-models.*

National CI Sector	NCI Sub-models
Energy	Electricity
	Natural Gas
	Petroleum
Finance	Banking
	Securities
	Insurance
	Brokerage
Food	Agri-Supply
	Crop Production
	Animal Production
	Aquaculture and Fishing
	Food Processing and Distribution
Government	International
	Federal
	Provincial/Territorial
	Aboriginal
	Municipal

[1] The US has 16 CI sectors. The model (10 CI sectors) proposed but Public Safety has not been adopted nationally. For example, Ontario considers Food & Water one sector, distinguishes Electricity from Oil & gas and does not recognize Manufacturing as a CI sector. In the Ontario model, Government is identified as Continuity of Government (Emergency Management Ontario, 2016).

National CI Sector	NCI Sub-models
Health	Primary Health (e.g., ambulatory patients)
	Secondary Health (e.g., Hospitals Nursing and Residential Homes)
	Nursing and Residential Care
	Medical Support Services (e.g., laboratories, blood/organ banks)
ICT	Telecommunications
	Information Services
Manufacturing	Basic Materials
	Chemical
	Equipment and Machinery
	Technology
	Transportation
	Pharmaceuticals
Safety	Environment
	Incident Response
	Community Resilience
	Professional Services
	Protective Services
Transport	Air
	Marine
	Rail
	Road
	Trucking
	Urban
Water	Watershed Management/Flood Control
	Potable Water
	Wastewater

In order to develop an integrated interdependency model, it was necessary to both bound and expand the descriptions of the individual Sectors. In some cases, e.g., *Manufacturing*, the NAICS offered a comprehensive and well-organized listing of entities. In others, e.g., Water, the NAICS had to be substantially extended, sub models (*Watershed Management, Potable Water* and *Wastewater*) introduced and the NAICS list of *industry groups* expanded to differentiate and singularize depict key functions. In some cases an *industry* group was reallocated e.g., *Pipelines* were moved from *Transportation* to *Energy* sectors to provide an end-to-end profile of the sector. The NAICS categorizes *Government* organizationally e.g., Federal, Provincial/Territorial, Aboriginal and Municipal. The NCIM has incorporated these *industries* into a *Public Administration and Regulation* sub-model. The NAICS does not distinguish a *Safety* sector; fire and police services are included under *Government* in the NAICS but under *Safety* in the NCIM.

3 The Information and Communications Technology Sector

3.1 Introduction

The Information and Communications Technology (ICT) sector provides goods and services that are integral to functioning of all other sectors and the Canadian economy. In addition to changing social behaviour, the convergence of computers and communications enabling users to share information in "real-time" has revolutionized business processes facilitating vertical and horizontal integration, accelerating globalization and fostering tightly coupled supply chains. Consequently, it has introduced new dependencies and potential vulnerabilities. Reliance on telecommunications and the movement of data within and between sectors has become an essential enabler; it has been described as the nervous system that binds CI sectors and through which risk can be transferred.[2]

The ICT sector is a diverse and growing segment of the Canadian economy. The ICT sector employed 1,450.3000 professionals and contributed $74.7 billion dollars to Canada's GDP in 2017 (The Information and Communications Technology Council, 2017). It consists of over 33,500 (mainly small) with the majority in the Software and Computer Services industry (Figure 3). ICT service industries are domestically oriented. Conversely ICT goods industries rely heavily on export markets; about 80% of ICT-related manufactured products were exported in 2016 (Innovation, Science and Economic Development Canada, 2016).

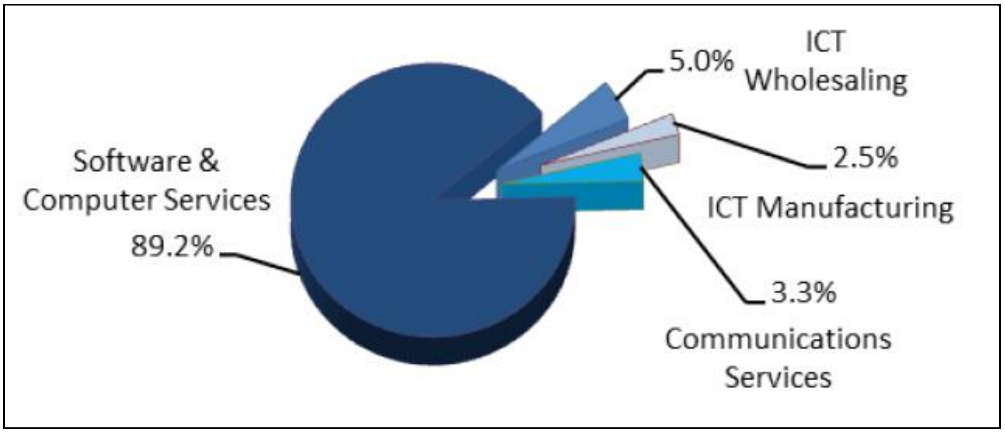

Figure 3: *Canada's ICT companies by sub-sector.*[3]
With the permission of Industry, Science and Economic Development Canada (ISEDC).

[2] For example, the breach which cost *Target* millions was traced to network credentials stolen from a third party (refrigeration, heating and air conditioning subcontractor. The challenge for many companies is more related to recognizing risks than to managing risk.
[3] Innovation, Science and Economic Development Canada. Canadian ICT Sector Profile 2016, page 3, https://www.ic.gc.ca/eic/site/ict-tic.nsf/eng/h_it07229.html accessed 9 April 2019.

3.2 Partitioning

In March 2013, Industry Canada[4] aligned with Statistics Canada and adopted the Organization for Economic Co-operation and Development (OECD)'s definition:

> *ICT goods are those that are either intended to fulfil the function of information processing and communication by electronic means, including transmission and display, OR which use electronic processing to detect, measure and/or record physical phenomena, or to control a physical process (OECD, 2019).*[5]

Bounding the *ICT* Sector—determining what is "in" and what is "out"—and identifying and isolating functions poses modelling challenge. The sector is rapidly evolving, epitomized by the convergence of voice and data networks and the institutionalization of cloud based services. In addition, as ICT has become pervasively ingrained in other sectors, they have, in many cases, developed dedicated internal infrastructures and infostructures blurring differentiation between internal an external services.[6]

The NAICS did provide a departure point for distinguishing functional entities and modelling relationships in and with *ICT* sector. For its part, Industry Canada's Sector Profile identifies four distinct sub-sectors—ICT Manufacturing, ICT Wholesaling, Software and Computer Services and Communication Services.[7] These can be mapped to the NAICS e.g., *Computer and Electronic Product Manufacturing* is considered a subsector under *Manufacturing*, *Telecommunications* a subsector under *Information and Cultural Industries* and *Computers and Communications Equipmen*t and *Supplies Merchant Wholesalers* is considered an industry group falling under *Wholesale Trade*. Table 2 outlines the NAICS codes which are being used as functional entities in the CI Interdependency model. As a general rule, in applying the NAICS, preference has given to aggregation but in many cases, as shown, reversion to industry group or industries is required in order to provide sufficient granularity to identify dependencies and assess risks.

---

[4] In 2015 Industry Canada was restructured/retitled becoming Innovation, Science and Economic Development Canada (ISED).

[5] OECD Glossary of Statistical Terms, http://stats.oecd.org/glossary/detail.asp?ID=6274 accessed 14 October 2014.

[6] Infostructure is the virtual equivalent of infrastructure. It refers to the engineered ordering, processes and tools for accessing and exploiting information; for example, Health Canada makes reference to a national "health infostructure" http://www.hc-sc.gc.ca/hcs-sss/ehealth-esante/infostructure/index-eng.php accessed 15 October 2015.

[7] The US IT Sector Specific Plan (U.S. Department of Homeland Security, 2016a) notes that the sector assets include both physical and virtual systems and networks. It identifies 6 critical functions required to maintain "high assurance IT products and services" for other sectors. These include:

- Provide IT products and services;
- Provide incident management capabilities;
- Provide domain name resolution services;
- Provide identity management and associated trust support services;
- Provide Internet-based content , information and communications services; and
- Provide Internet routing, access, and connection services.

Table 3: *NAICS to NCIM Mapping for the ICT Sector.*

		NAICS	
Sector	**Sub-Sector**	**Industry Groups**	**Industries**
33 Manufacturing	**334 Computer and Electronic Product Manufacturing**	3341 Computer and Peripheral Equipment Manufacturing	
		3342 Communications Equipment Manufacturing	
		3343 Audio and Video Equipment Manufacturing	
		3344 Semiconductor and other Electronic Component Manufacturing	
		3345 Navigational, Measuring, Medical and Control Instruments Manufacturing	
		3346 Manufacturing and Reproducing Magnetic and Optical Media	
	335 Electrical Equipment, Appliance and Component Manufacturing	3351 Electrical Lighting Equipment Manufacturing	
		3352 Household Appliance Manufacturing	
		3353 Electrical Equipment Manufacturing	
		3359 Other Electrical Equipment and Component Manufacturing	
41 Wholesale Trade	417 Machinery, Equipment and Supplies Merchant Wholesalers	**4173 Computer and Communications Equipment and Supplies Merchant Wholesalers**	
44-45 Retail Trade	443 Electronics and Appliance Stores	4431 Electronics and Appliance Stores	443143 Electronics and Appliance Stores
			443144 Computer and Software Stores
			44145 Camera and Photographic Stores
			44146 Audio and Video Recordings Stores
51 Information and Cultural Industries	511 Publishing Industries	5111 Newspaper, Periodical, Book and Directory Publishers	**N51114 Directory and Mailing List Publishers**
		5112 Software Publishers	
	512 Motion Picture and Sound Recording Industries		
	515 Broadcasting	5151 Radio and Television Broadcasting	
	517 Telecommunications	**5171 Wired Telecommunications Carriers**	
		5172 Wireless Telecommunications Carriers (except Satellite)	
		5174 Satellite Telecommunications	
		5179 Other Telecommunications	
	518 Data Processing, Hosting and Related Services		
	519 Other Information Services	5191 Other Information Services	51911 News Syndicates
			51912 Libraries and Archives
			51913 Internet Publishing and Broadcasting and Web Search Portals
			51919 All Other Information Services
54 Professional, Scientific and Technical Services	541 Professional, Scientific and Technical Services	**5415 Computer Systems Design and Related Services**	
81 Repair and Maintenance	811 Repair and Maintenance	8111 Automotive Repair and Maintenance	
		8112 Electronic and Precision Equipment Repair and Maintenance	
		8113 Commercial and Industrial Machinery (except Automotive and Electronic) Repair and Maintenance	
		8114 Personal and Household Goods Repair and Maintenance	
Legend			
ICT Sector: Telecommunications			
ICT Sector: Information Services			
ICT Sector: Public Communications			
Other CI Sectors: Manufacturing			

DRAFT

The NAICS codes in blue are deemed (for modelling purposes) to be in the ICT Sector; those in orange are deemed to be more appropriately considered an integral part of another sector or sub-model. For example, the production of electronic components and control instruments is generally considered a Manufacturing process and a Technology and Electronics Supply Chain sub-model has been developed in characterizing the Manufacturing sector. Many if not most stakeholders in other CI sectors procure electronic and hardware components directly through merchant wholesalers. These are considered an integral part of the Technology and Electronics sub-model. Capturing dependencies on product and parts and repair services is more critical than sector placement.

3.3 Characterizing

The ICT sector can be characterized through several lenses.

3.3.1 Transmission Means

The 2010 US Telecommunications Sector Specific Plan characterized the communications sector in terms of five components:

- **Wireline** consists primarily of the Public Switched Telephone Network (PSTN) and includes cable networks and enterprise networks. Wireline networks are being redefined by Next Generation Networks (NGNs), which are high-speed, converged circuit-switched and packet switched networks capable of transporting and routing a multitude of services, including voice, data, video, and other multimedia, across various platforms. The wireline component also includes the Internet infrastructure and submarine cable infrastructure.
- **Cable** communications systems are wireline networks that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service. They use a mixture of fiber and coaxial cable that provide two-way signal paths to the customer.
- **Wireless** consists primarily of cellular telephone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services, including numerous law enforce-ment, public safety, and land mobile radio systems**.**
- **Satellite** communications deliver data, voice, and video services. Satellite services exist in several forms: fixed, transportable, on the move, and handheld. The technology can deliver two-way point-to-point or mesh converged access and/or backbone services (voice, data, and video), as well as multicast (video and/or data for distribution of content to large audiences).
- **Broadcasting** systems consist of free, over-the-air radio and television stations that offer analog and digital audio and video programming services and data services. Traditionally broadcasting has been the principal means of providing emergency alert services to the public. The recent transition to digital television (DTV) and the ongoing transition to digital radio both provide broadcast stations with enhanced capabilities, including the ability to multicast multiple programs on a single channel (US Department of Homeland Security, 2010).

Each of these components has distinctive physical footprint and infrastructure architectures. Examples are shown below and have been included as they are useful in both situating assets and segments, and in illustrating the inherent complexity of the current and emergent telecommunications ecosystem.

Wireline infrastructure has evolved from development of the electrical telegraph in the mid-19th century which was followed by the laying of submarine cables mid-century through Alexander Graham Bell's discovery of the telephone in the1870s and establishment of Public Switched Telephone Networks to today's infrastructure. Initially the supporting infrastructure was—and remains—predominantly corporeal, and includes fiber optic, coaxial cable and copper wire elements with landlines running underground, above ground (on poles) and undersea. Wireline communications supports both local exchange telecommunications networks and long-haul transport providing the fixed "backbone" sustaining "core" networks (Figure 4).

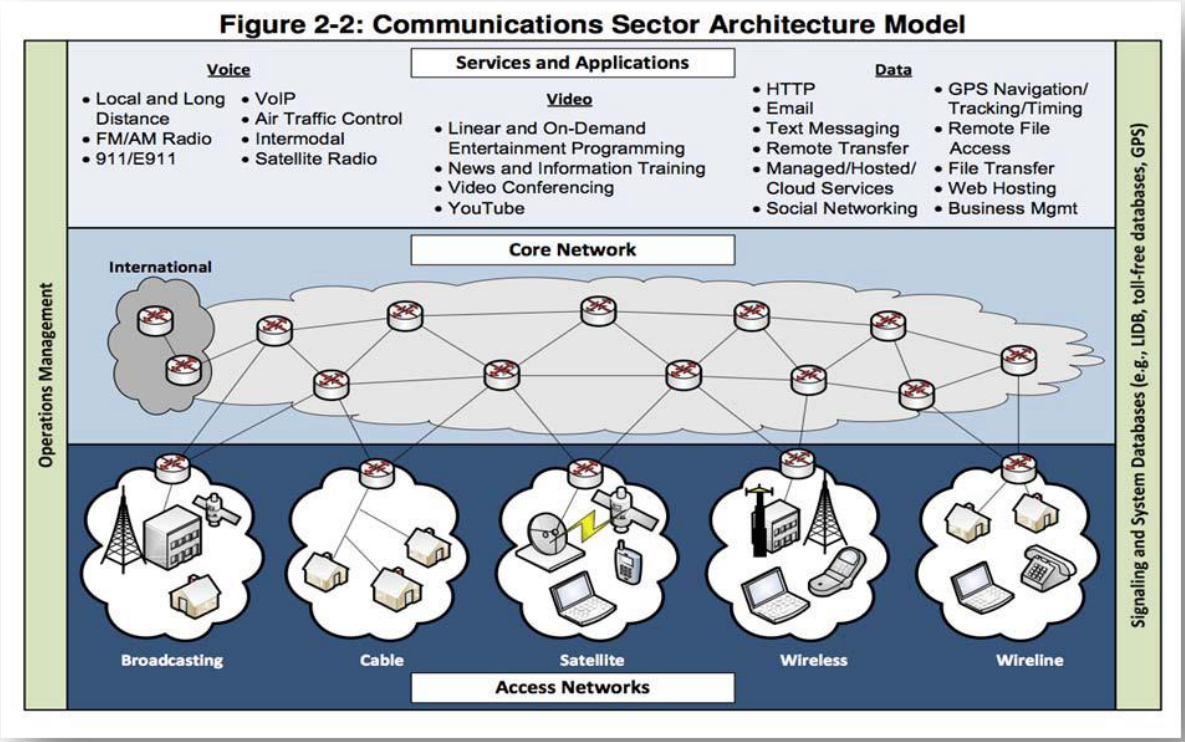

Figure 4: *Communications sector architecture.* [8]
With the permission of the US Department of Homeland Security (DHS).

Cable networks represent a specific instantiation of wireline communications. They employ fiber and coaxial cables to provide bi-directional signal paths to customers employing a Service Delivery Network (SDN) integrating access and transport functions. As shown (Figure 5), a typical hybrid fiber/coaxial (HFC) network includes headends, distribution hubs and multiple fibre nodes. Headends provide connectivity to core voice and data communications networks, distribution hubs serve as intermediate waypoints, and fiber nodes convert optical to radio frequency (RF) signals for "last mile distribution." Outside Plant Equipment refers to small vaults/huts located in neighbourhoods which house supporting equipment including power to fiber nodes and RF amplifiers.

[8] Page 39, Communications Security, Reliability and Interoperability Council (2015).

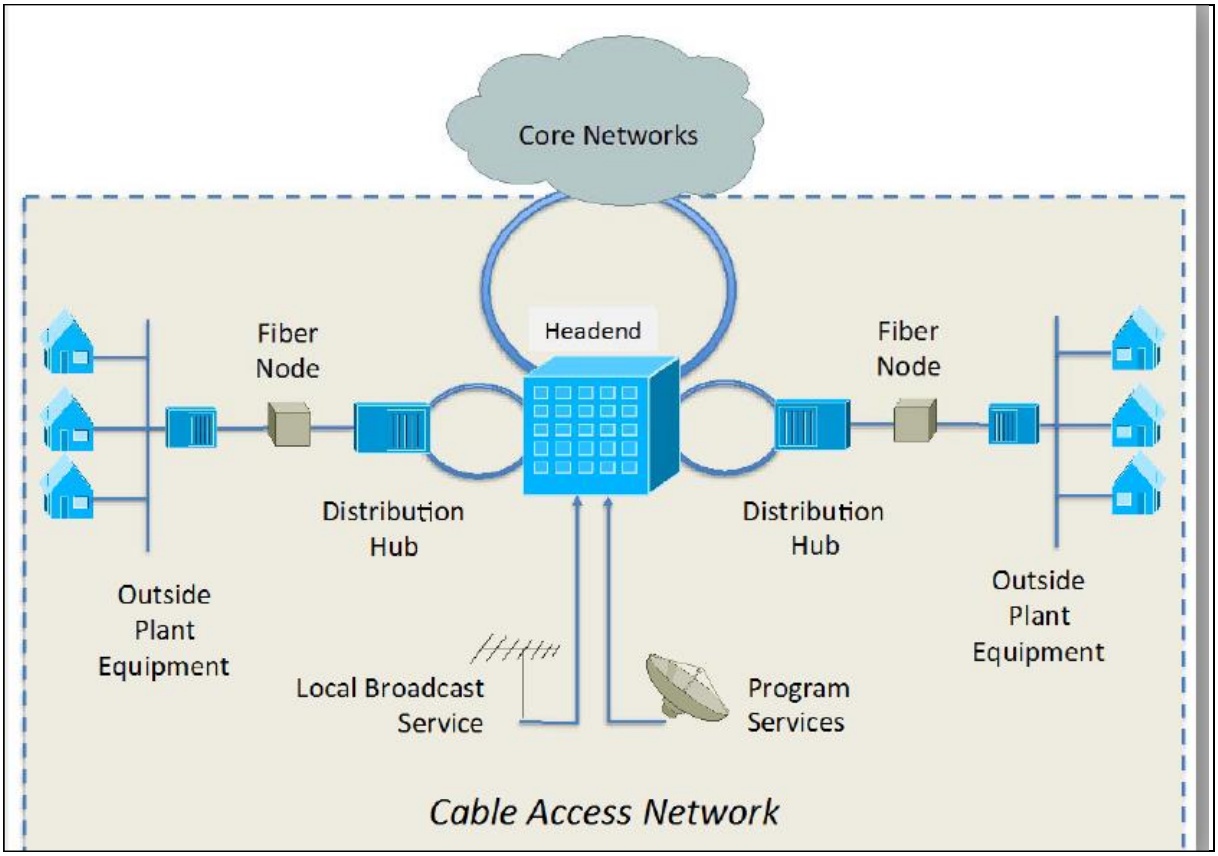

Figure 5: *Cable access architecture.*[9]
With the permission of the US Department of Homeland Security (DHS).

Rapid technological advancements have changed the way people communication, pushing wirelines to the background. Nonetheless wireline communications are fitted in many, if not most, buildings and many CI functions continue to rely on wirelines. For modelling purposes Cable Services have not been distinguished but wireline services have been recognized as a distinct function.

Wireless communications use electromagnetic transmissions most commonly radio waves in lieu of electrical impulses. It enables a variety of electronic devices to link to existing wired infrastructure (through network elements) and to access information and services beyond the immediate transmitter range. Supporting infrastructure includes cell towers and base stations and base transmitters. Detached and mobile connectivity offer significant advantage. The shift from analogue to digital data has also contributed to this revolution in the ITC sector. One of the inherent challenges—reflecting the pace of change—is that the architecture must accommodate both legacy and emergent protocols.[10] Transmission

[9] Page 170, Communications Security, Reliability and Interoperability Council (2015).
[10] The "G" refers to generation. The first—1G—networks were analog and designed for voice. Digital 2G circuit-switched data networks introduced in the early 1990s offered better security, sound quality and capacity—a way to repurpose voice-centric networks for data. They are now virtually obsolete. Packet-switching represented yet another increase in data throughput speed and International Telecommunication Union (ITU)-specified 3G technology entered service in 2004. Further advances in technology (defined by Advanced International Mobile Telecommunications (IMT) standards) re incorporated in 4G which became the norm in 2011.

speeds continue to increase reducing latency times and allowing more data to transferred. This continuing evolution is reflected in generational sets of standards i.e., 4G.captured

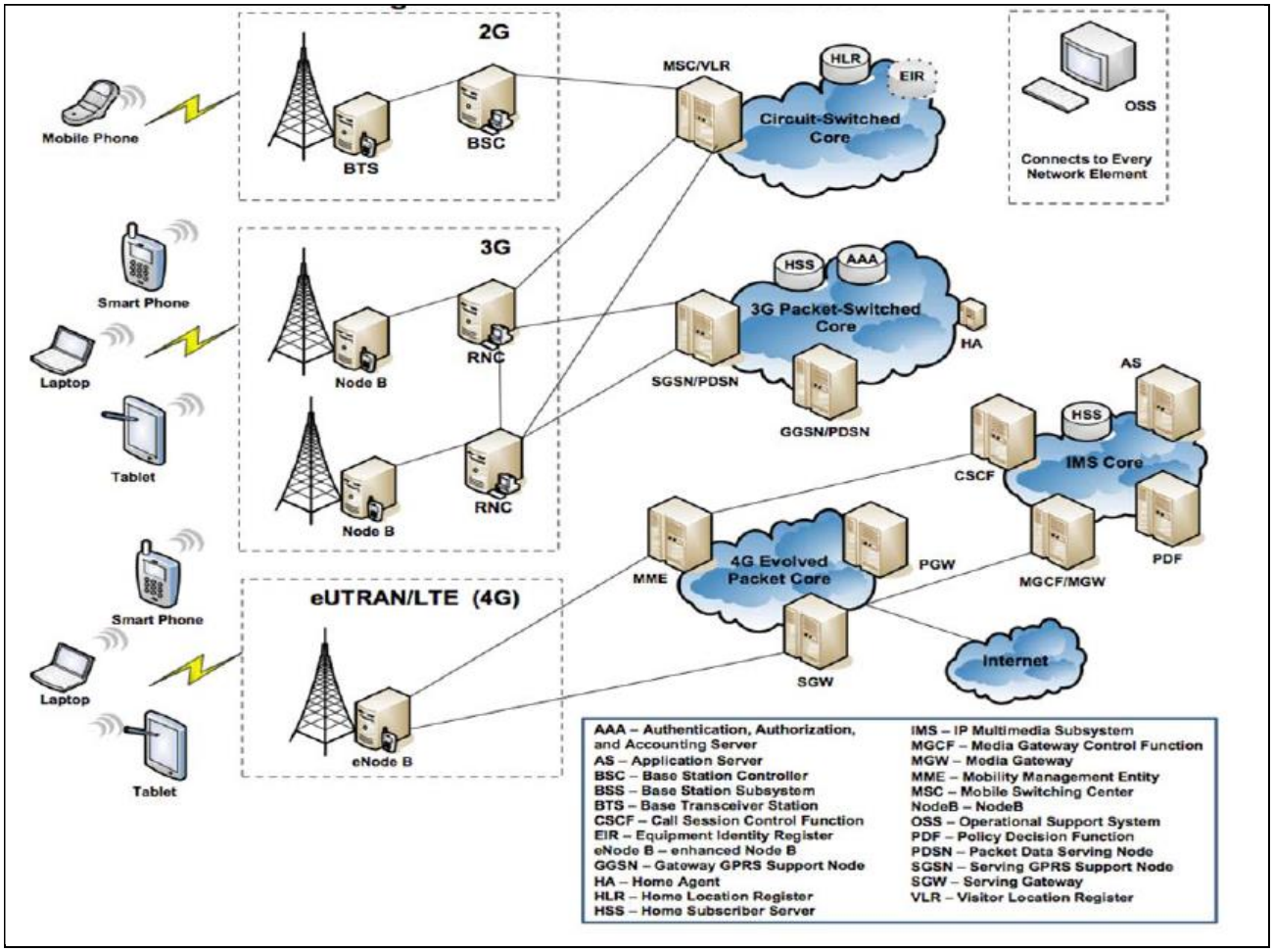

Figure 6: *Wireless communications architecture.*[11]
With the permission of the US Department of Homeland Security (DHS).

The prime focus of the NCIM is on inter-sectorial dependencies rather than detailed architectures. The key "take-away" is that critical infrastructure supporting wireless communications, albeit an extension of wired communications, is sufficiently different to warrant being treated separately i.e., modelled as a discrete function.

Satellites provide a means to relay and amplify radio signals. An illustrative satellite communications architecture is depicted below (Figure 7). Noteworthy critical infrastructure elements include space-based satellites and ground-based satellite control stations and communications stations. (TT and C refers to telemetry, tracking and command. A Very Small Aperture Terminal (VSAT) uses small dish antenna to transmit and receive narrow band data e.g., Point of Sales transactions, Radio Frequency Identification (RFID) data.)

[11] The Page 160, Communications Security, Reliability and Interoperability Council (2015).

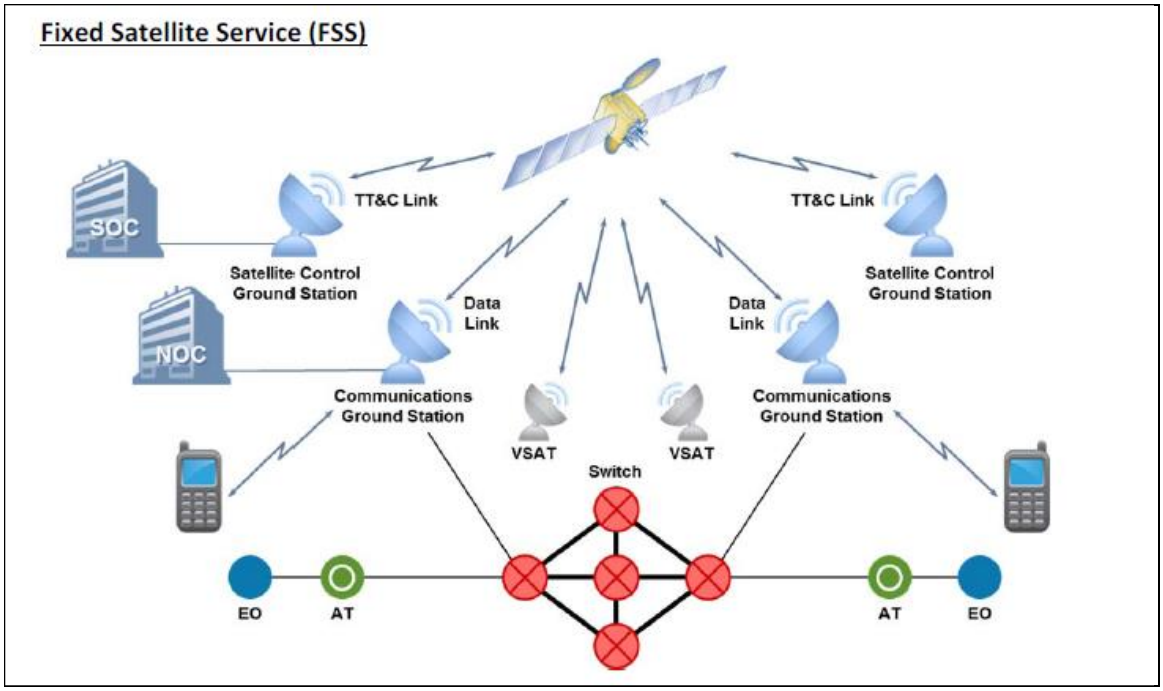

Figure 7: *Satellite communications architecture.*[12]
With the permission of the US Department of Homeland Security (DHS).

As note in the recent Defence Review, in addition to supporting the operation of cell phones and televisions, "satellites underpin an increasing range of daily activities, including by providing the time stamp function for ATMs and stock exchanges, coordinating air traffic control and 'just in time' delivery of goods" Department of National Defence, 2017). The CI associated with satellite communications is considered sufficiently discreet to warrant consideration as a separate NCIM function.

A mesh network embodies progression from point to point communications and a limited number of access points to network topologies. In a mesh network infrastructure, connection points are widely dispersed and nodes interact directly and dynamically and non-hierarchically with other nodes providing alternative transmission channels (Figure 8). This "rich" connectivity increases speed and resiliency, and flexibility i.e., in a wireless mesh network, only one node needs to be physically wired to a network connection.

[12] Page 98, Communications Security, Reliability and Interoperability Council (2015).

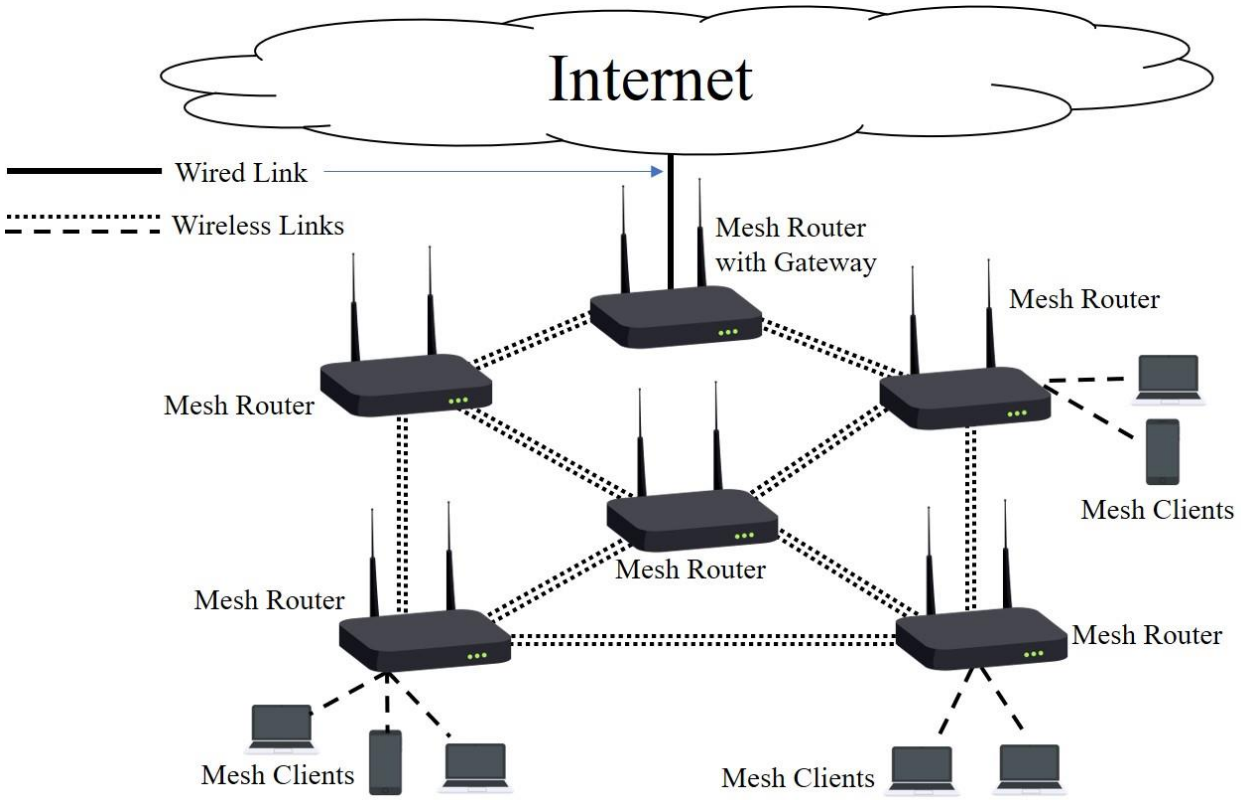

Figure 8: *Illustrative mesh network.*[13]
Icons with the permission of www.pngtree.com.

Mesh networks can relay messages exploiting "routing" or "flooding". In the case of routing the destinations(s) is designated and the transmission propagated by hopping along a path from one node to the next self-healing and reconfiguring the pathway as required. Routers direct traffic from source to destination. In addition to sending packets of data from internal networks (Local Area Networks (LANs) or geographically larger Wide Area Networks (WANS)) to the Internet, routers can also be used to segment these networks from the wider Internet. Flooding involves distributing the data from one node to the others in a network i.e., a message is delivered to all linked nodes. This is the modern equivalent of broadcasting and is used in much the same way e.g., AMBER alerts.

Broadcasting is still an important constituent of public communications. Traditionally it has provided the means to deliver news and weather updates and critical alerts and emergency information to local and national communities. Increasing reliance is being placed on the Internet and broadcasters have become dependent on IP based network services.

[13] Authors' figure based on Data Bridge Market Research (2019).

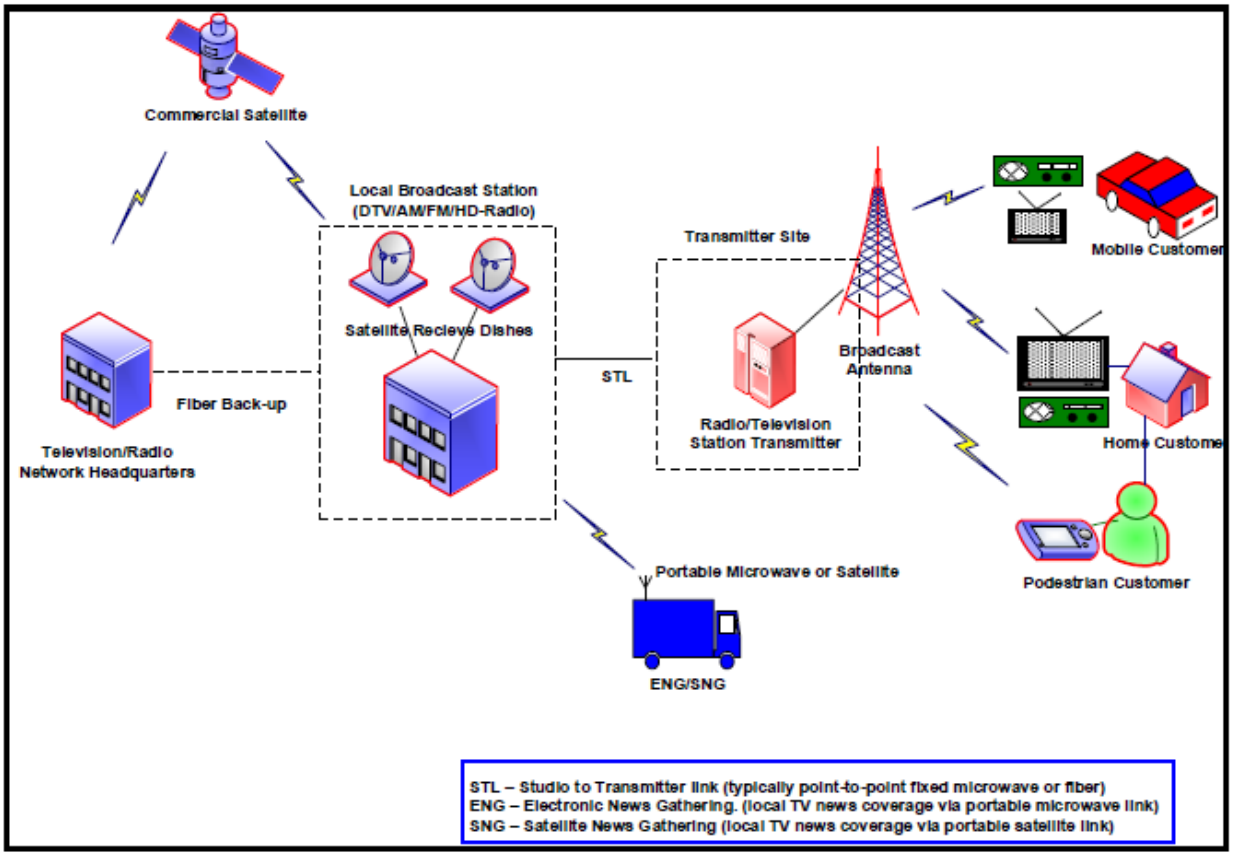

Figure 9: *Broadcast architecture.*[14]
With the permission of the US Department of Homeland Security (DHS).

These architectural depictions are illustrative. The telecommunications industry has been rapidly transforming, and the five components do not exist in silos. They rely on a common core backbone and increasingly share a supporting, integrated infrastructure. For example, as noted, the broadcast industry is becoming increasingly reliant on the Internet and Internet Protocol (IP) based infrastructure to support its core operations. The Communications Security, Reliability and Interoperability Council (CSRIC) observed that:

> *Customer demands and business imperatives are bringing about the convergence of traditional circuit switched networks interoperating with broadband and packet-based Internet Protocol (IP) networks. The evolution of wireless, wireline, and cable networks is driving toward next generation global communications networks. Many networks and providers have developed the capability to carry voice, video, text, and data transparently to many types of end-user devices (US Department of Homeland Security 2010) (US Department of Homeland Security, 2010).*

In summary, the NCIM *Telecommunications Services* sub-model differentiates between CI transmission means. These are framed as capabilities i.e., the ability to communicate via wireline. An additional

[14] Page 40, Communications Security, Reliability and Interoperability Council (2015).

function, *Other Telecommunications Services,* has been distinguished. It includes Internet providers and service resellers as an independent function liable to "failure" and therefore serving as a source of vulnerability and potential risk.

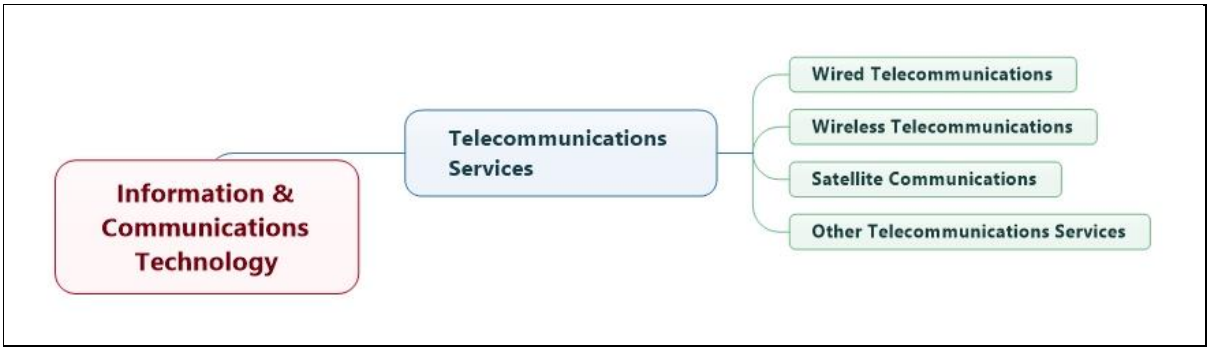

Figure 10: *Characterizing telecommunications CI by transmission means.*

3.3.2 Roles

In addition to transmission means, CI functions can be characterized by role i.e., telecommunications infrastructure can also be viewed in terms of three components—Access, Core (backbone) and Management.

- **Access** networks connect end users (subscribers) to their immediate service providers and provide entrée to telecommunications services. Access networks are geographically bounded and supported by interconnected Central Offices in metropolitan areas. Typically the distances between Junctions/Central Offices are relatively short and network topography (this may be ring or mesh) may allow for adjacent Central Offices to offer back-up redundancy. Access failure could result from physical disruption to the network, overloading or denial of service.

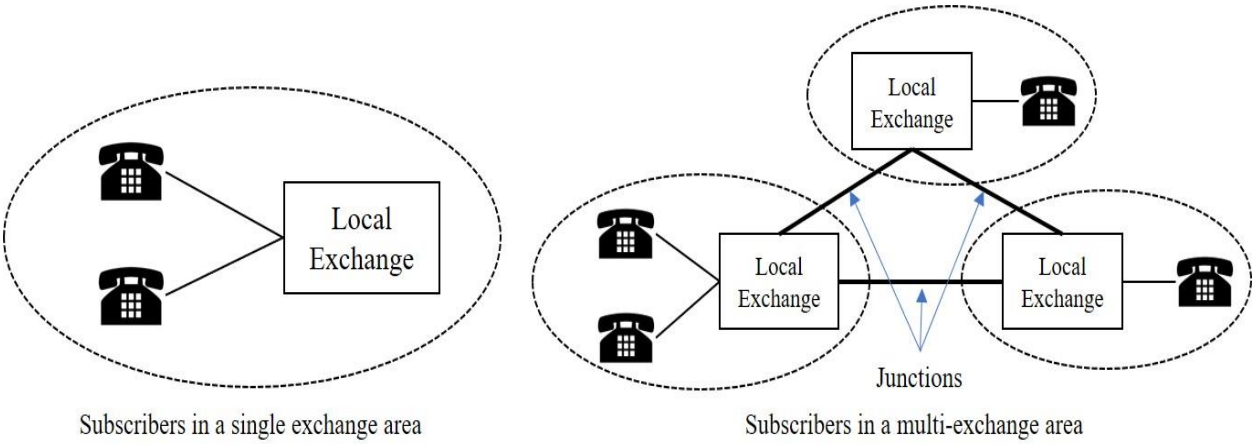

Figure 11: *Illustrative single and multi-exchange networks.*[15]
Icons with the permission of www.pngtree.com.

[15] Authors' figure based on Angelfire (2015).

Local communications routed through local exchanges/networks may remain intact even if long distance transport "fails."

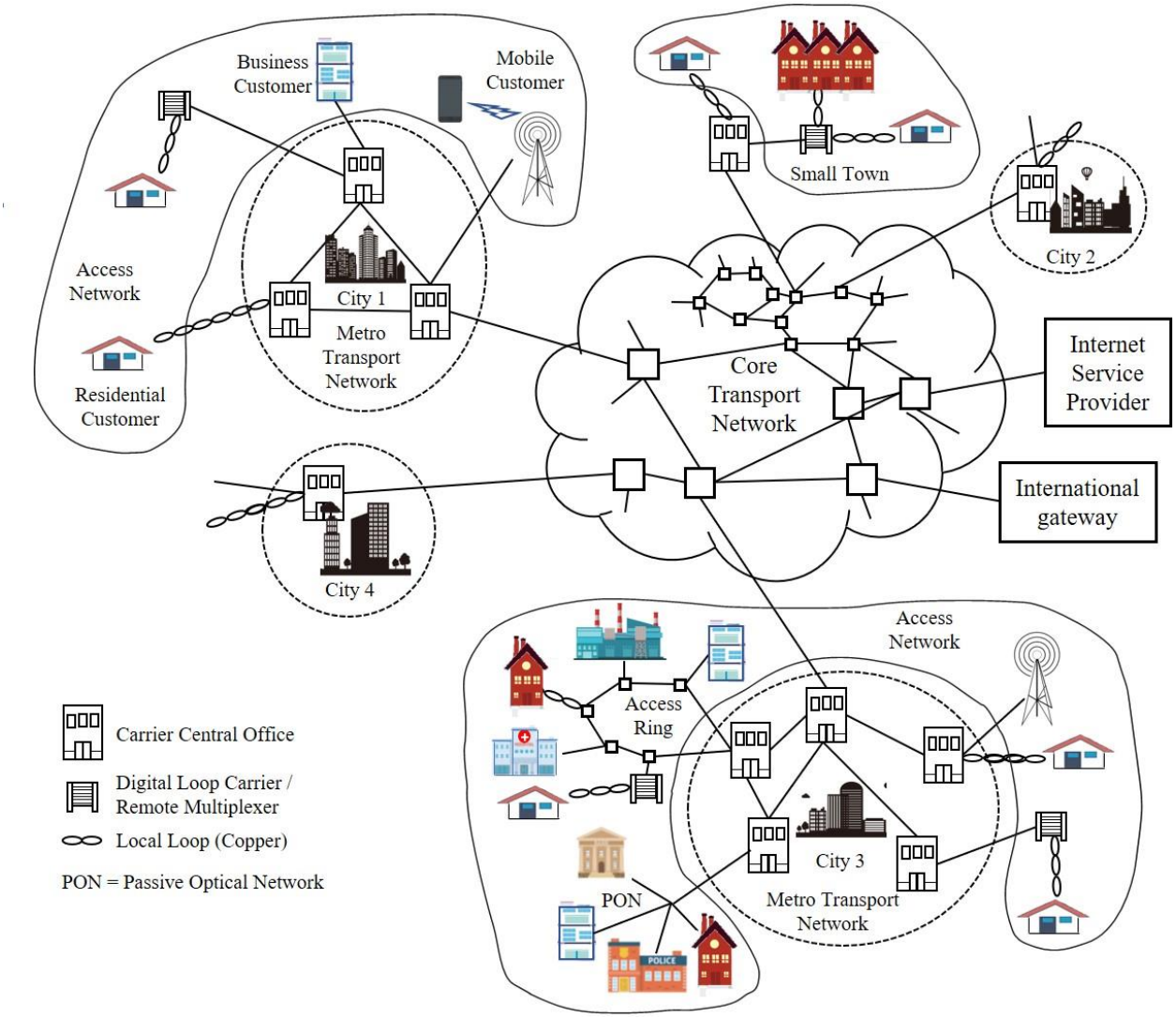

Figure 12: *Illustrative telecommunications network.*[16]
Icons with the permission of www.pngtree.com.

Many analysts have concluded that the "last mile" enabling access is the most vulnerable link as it is not usually "backed up."

- **Routing** involves selecting transmission paths and directing the forwarding of structured (logically addressed) packets from source through intermediate nodes (routers, switches, bridges and

[16] Authors' figure based on Gorshe, S. (2005).

gateways) to destination. Given the complexity of larger networks, routing has been automated for the most part.

- **Switching** includes automated traffic routing and function on local (distribution Routers) and transport (backbone routers and international gateway) levels The prior distinction between switching and transmission has become blurred as transmission networks have increasingly deployed digital cross connect systems (DCSs) that switch subscribers' traffic between the various DCS interfaces according to a provisioned routes.
- **Transport** is used to describe the long distance core carriage network that provides connectivity between local/metro networks, community central offices, service providers (e.g., Internet) and regional or international gateways. Transport itself can be characterized in terms of three planes.

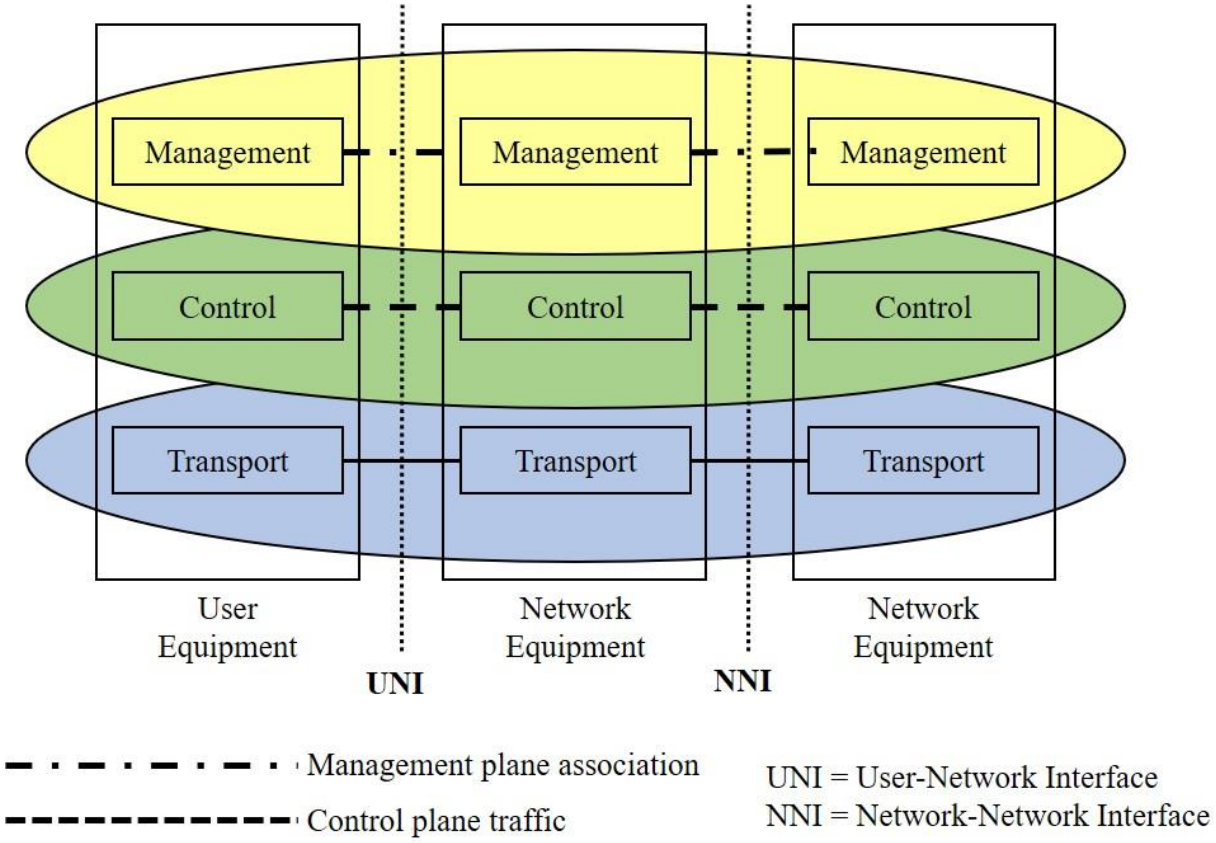

Figure 13: *Management and Control Planes for ICT Operations.*
Icons with the permission of www.pngtree.com.

Figure 13 illustrates the management and control planes and the relationships to ICT transport operations; the planes are:

- Management supports centralized operations support system.
- Control allows for configuration of the networks in real time; and includes traffic management and alarm monitoring.
- Transport includes the physical media (the "pipe") and interfaces.

In the NCIM Management and Control planes are described as Network Management. When assessing risk it is worth noting that there are more transport hubs/repeater stations than switching centres, and that current technology (SONET/SDH) incorporate automatic protection switching capabilities.

Transport may deserve particular attention. In assessing risk it is worth noting the reliance on undersea communication cables and the physical dangers the geographic of concentration of landing sites and virtual dangers the introduction of control systems connected to the Internet and operating on commercial software present. A 2012 report observed that "undersea communication cables are, in fact, the only technology that can transmit large amounts of bandwidths across bodies of water at low latencies (delays) and low costs. In fact, undersea cable systems transmit nearly 99% of all trans-oceanic Internet and data traffic" (Sechrist, 2012). The author noted for example that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network uses undersea fiber-optic communications cables to exchange financial data between dispersed financial institutions. He concluded that the risk to global safety and security was being compounded by the vulnerability of cable systems to cyber-attacks through new network management systems. Cable vulnerability is a topical issue; US authorities have recently raised concern over Russian submarine activities near the undersea cables. Most breaks—attributable to fouling by anchors—take place close to shore and can be repaired within days. "The Russians appear to be looking for vulnerabilities at much greater depths, where the cables are hard to monitor and breaks are hard to find and repair" (Sanger, 2015).

The NCIM characterizes Telecommunications Services through these two lens (Figure 14).

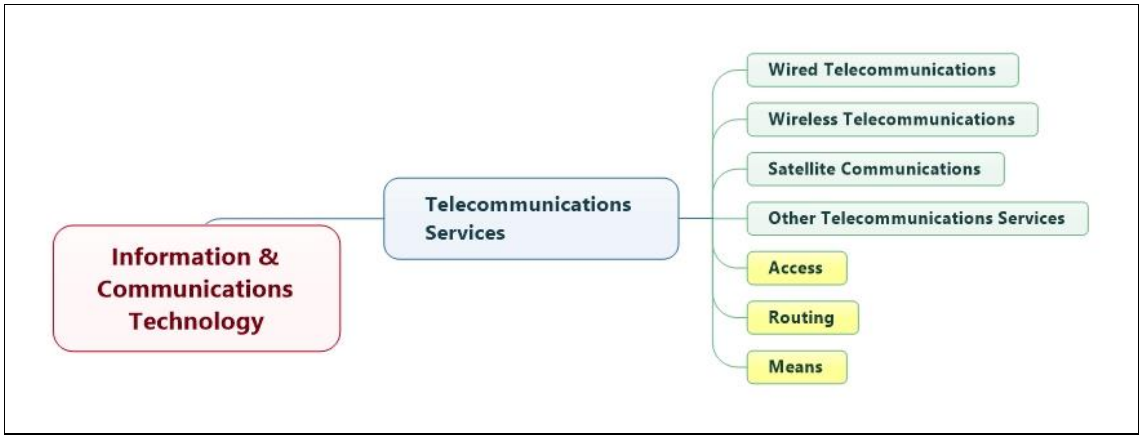

Figure 14: *Characterizing telecommunications services by transmission means and component role.*

3.4 Telecommunications Sub-Model

The focus of the NCIM project is to facilitate development of a deeper understanding of inter and intra-sector dependencies. Two logic models depicting functional relationships—Network Maintenance and Repair and Network Operations—the ICT sector were created to illustrate the model and stimulate dialogue. The Network Maintenance and Repair logic model (Figure 15) is largely self-explanatory. It depicts key interdependencies e.g., reliance on the *Manufacturing* Sector to provide spare parts and the *Energy* Sector to provide electric power, the *Transportation* Sector to maintain road infrastructure (enabling access to sites) and the *Safety* sector to provide security and response to incidents.

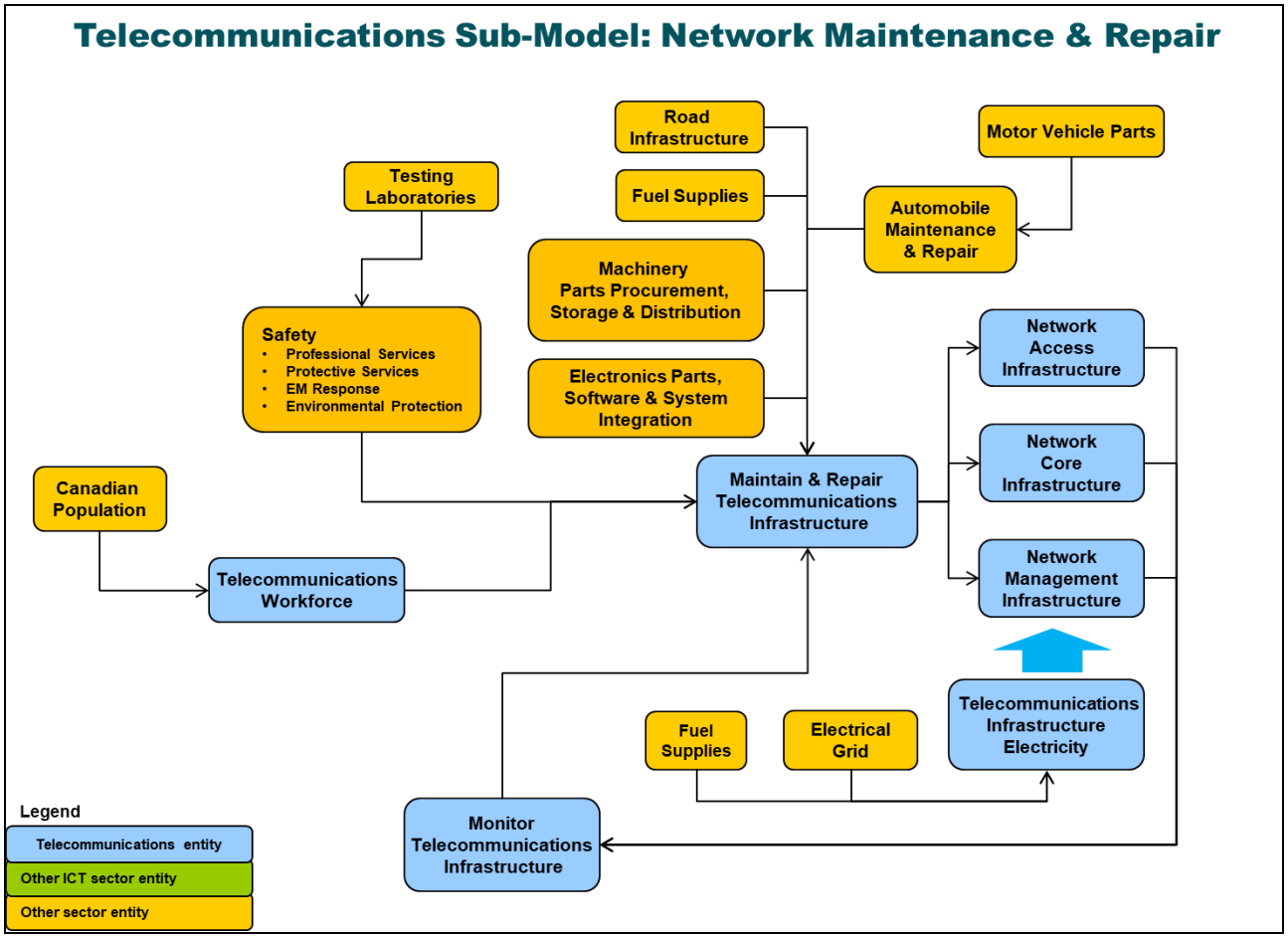

Figure 15: *Telecommunications—network maintenance and repair.*

The Network Operations logic model (Figure 16) distinguishes maintenance, management and operating functions and relates these to the telecommunications mediums (wired, wireless and satellite). These respond to NAICS codes, allowing the economic activity associated with each to be monitored, and, more importantly as noted previously, each telecommunications medium has unique infrastructure elements and corresponding vulnerabilities, and the strength of the dependencies on and by other sectors may vary. As shown, on the left, all 10 CI sectors and *Information Services* rely on telecommunications e.g., a disruption in services will have cascading consequences.

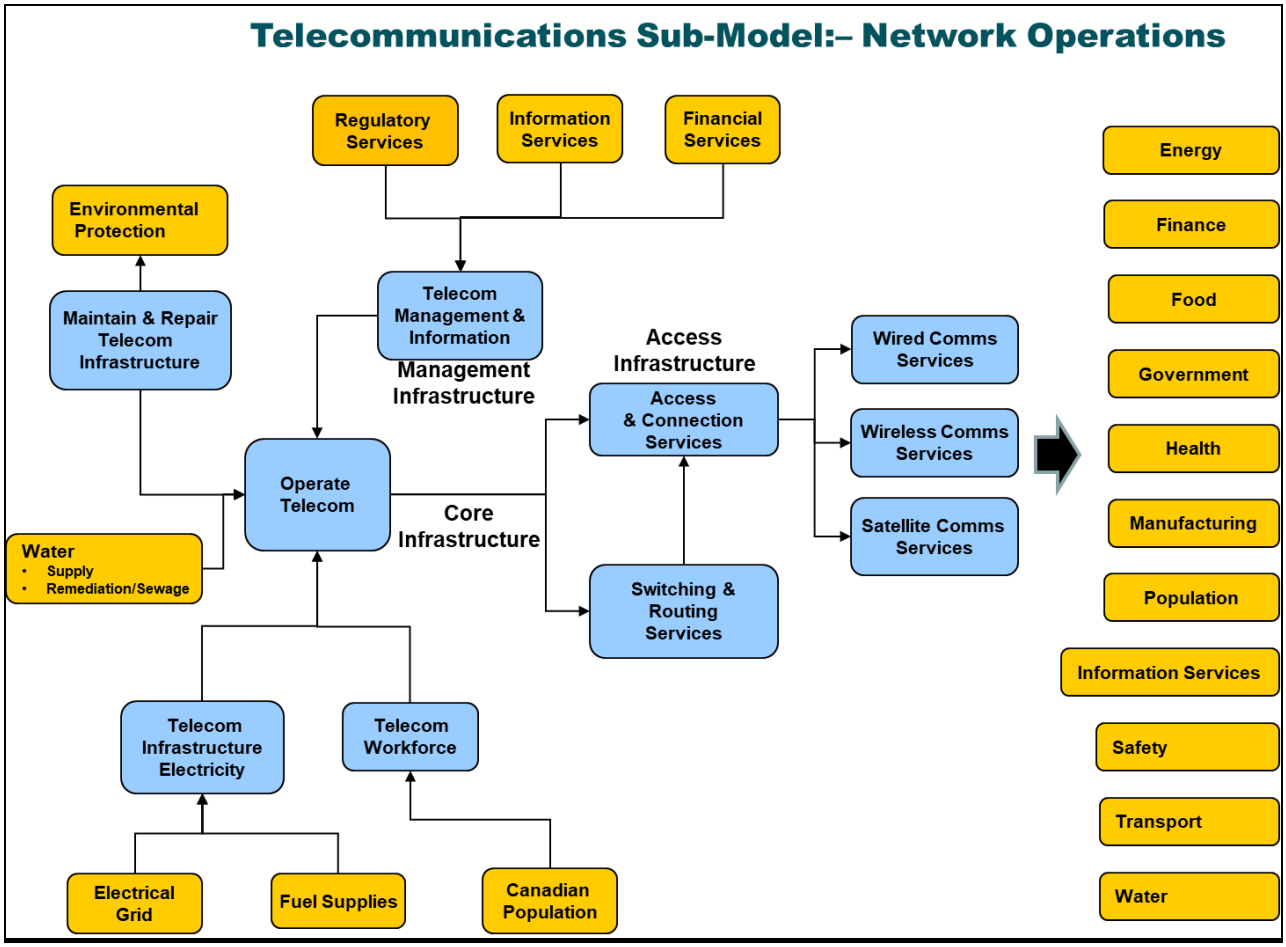

Figure 16: *Telecommunications sub-model—network operations.*

3.4.1 Radio and Television Broadcasting

Both public and privately-owned broadcasters operate in Canada. Tradition reliance on individual stations broadcasting their signals freely over the air for direct reception by consumers has declined, replaced by cable and (direct to home) satellite services. Both redistribute broadcast signals—the former via landlines and the latter via satellites. Both radio and television rely heavily on electricity. Many stations maintain generators to supply power in the event of a power failure. Both broadcasting stations and the distribution median are vulnerable to physical destruction or disruption and their signals/data stream vulnerable to corruption or denial.

The radio spectrum may also be used for personal, non-commercial purposes. National regulating authority licence “amateur” (“ham”) radio operators specifying frequency allocations—typically distributed throughout the Radio Frequency (RF) spectrum to allow the operators selection of an effective frequency—and output power. Relying on batteries and/or generators “amateur” operators may provide essential communications services when regular communications are unavailable.

3.4.2 Internet

The Internet is a global system of interconnected Internet Protocol (IP) networks i.e., a network of computer networks. It relies on access through an Internet Service Providers (ISPs) and routing and transport via telecommunications infrastructure to realize connectivity and enable the direction/delivery and rapid exchange of digitized information. The Internet might be best described as a collaborative self-policing enterprise. There is no centralized governance structure or process(es) ordering technological implementation or determining entrée and usage policies. Each constituent network sets its own course. The Internet Engineering Task Force (IETF), an open, non-profit organization and community of network designers, operators, vendors and researches; oversees development of standardized core protocols (e.g., IPv4 and IPv6[17]). Another not-for-profit, the Internet Corporation for Assigned Names and Numbers (ICANN), oversees assignment of unique indicators e.g., top-level domain names, Internet Protocol (IP) address spaces and address blocks to regional internet registries.

Users access the Internet through computerized devices connected to networks via wired (e.g., telephone, copper or fiber optic cables), wireless (e.g., wireless local area network (WLAN)) or satellite.

The World Wide Web (www) is one of the prime and most popular applications in use on the Internet. Documents, images and video clips are catalogued (referenced and logically interrelated) using Uniform Resource Indicators (URIs). URIs identify source services, servers, databases and records. Browsers (e.g., Internet Explorer, Google Chrome, Mozilla Firefox, Safari) enable users to navigate from one web page to another via embedded hyperlinks, and search engines (e.g., Yahoo, Google) enable keyword driven access to online information. The "Web" has enabled individuals and organizations to publish material and reach wider audiences at lower costs and to share information in near real time.[18] This has lead to an increased reliance on *Information Services*.

3.5 Information Services Sub-Model

Information Services have become increasingly important in knowledge-based societies; economic prosperity and public safety and national security is linked to data capture, storage, retrieval and evaluation. Consolidation and investigation of pooled "big" data enabled by advances in communications and computing offers unprecedented opportunities to discern macro-level patterns/profiles in near-real term. Protection of classified, proprietary and personal information is a long standing concern, exacerbated by recent trends to amalgamate and outsource information hosting. Cloud-based data storage represents a logical next step in specialization and globalization. At the same time, it introduces new dependencies on telecommunications to ensure access to data and applications if and as required to support critical business processes. Data centres and server farms represent one of the largest and faster growing consumers of electricity. Many of the newer and larger data centres are very energy efficient; the older and small, medium and corporate (majority of) data centres are decidedly less efficient.

---

[17] Internet Protocol Version 4 (IPv4), the initial standard, remains in widespread use. In order to accommodate the growing number of users Internet Protocol Version 6 (IPv6) has been introduced and is now being deployed.

[18] The Internet can be and is being utilized for illicit purposes. Exchanges are conducted on the *dark web*. In addition, access to the Internet expands vulnerability. It was not designed with security in mind. A recent US Federal Bureau of Investigation (FBI) Private Industry Notification (PIN) (Federal Bureau of Investigation, 2015) drew attention to the use of a web site *Shoban* to identify the IP addresses of internet-connected devices e.g. ICS and SCADA systems. Examples cited include tampering with temperatures controls of US laboratory and intrusion into a water facility in a US city.

In 2013 U.S data centers consumed an estimated 91 billion kilowatt-hours of electricity, equivalent to the annual output of 34 large (500-megawatt) coal-fired power plants. Data centers electricity consumption is projected to increase to roughly 140 billion kilowatt annually be 2020, the equivalent annual output of 50 power plants (US Natural Resources Defense Council, 2015).

The increasing use of data and the exponential demand for energy by data centres "the Data Center sector could be using up to 20% of all available electricity in the world by 2025" (Data Economy , 2017) is noteworthy in any appreciation of sectorial interdependencies.

The logic model capturing functional relationships relating to Information Services and cyber dependencies is shown below (Figure 17).

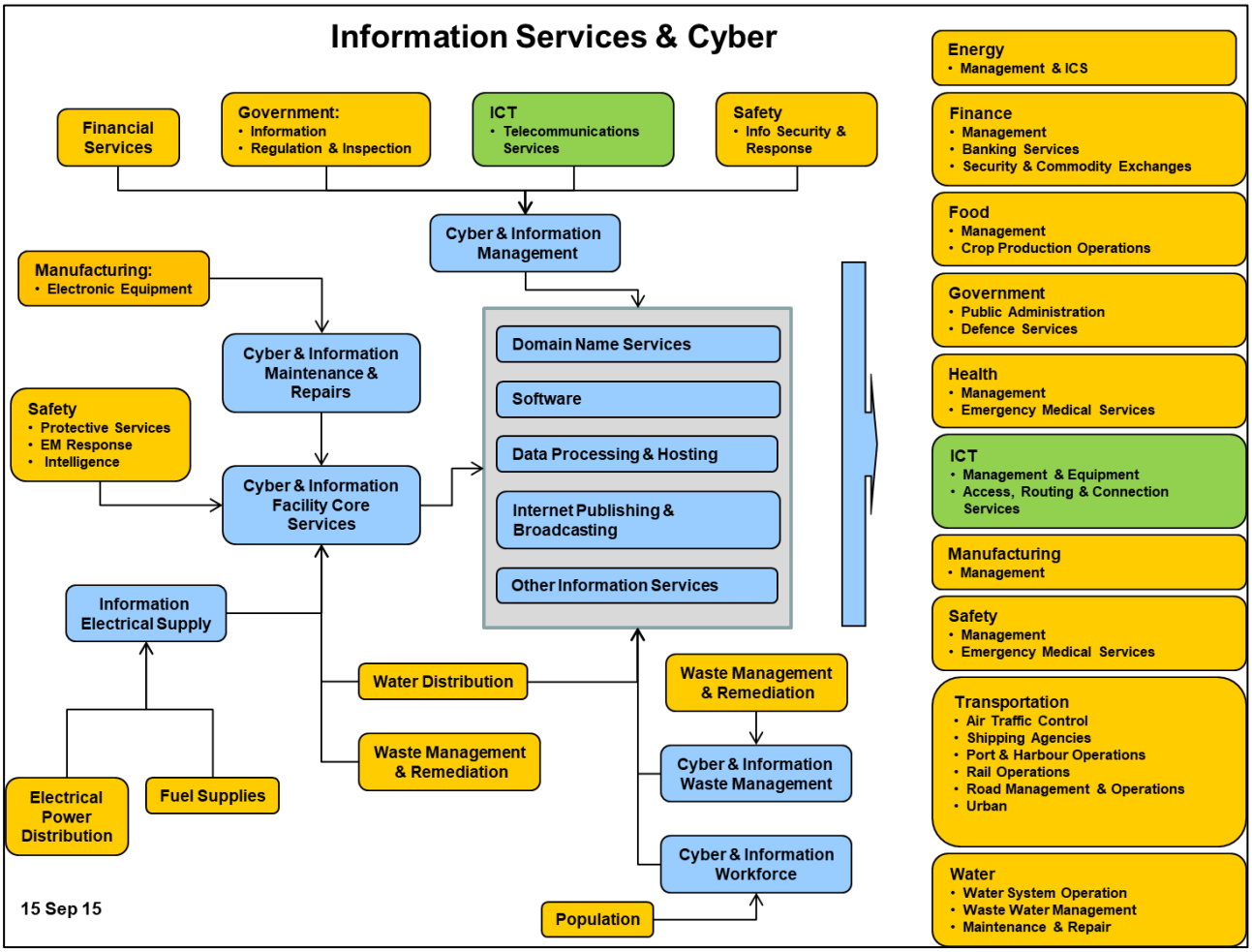

Figure 17: *Information services sub-model.*

Cyber supply chains have become as important as traditional physical supply chains. Cyber4Sight advices that "third-party platforms are being targeted as points-of entry-top to an organization's internal systems" and concludes that "2016 may see cybercriminals carrying out supply-chain attacks through exploitation of both public and private cloud infrastructure" (Booz, Allen, Hamilton 2015). Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems are a particular concern. These

are used to control manufacturing processes and critical infrastructure operations. While CI sectors own and operate these systems; ICT provides the enabling telecommunications networks.

A complete list of the NCIM functions for ICT Sector can be found at Annex B.

3.6 Generic Models

Complementary logic models were developed for generic activities common to all CI sectors e.g., *Core Facilities*, *Management* and *Maintenance and Repair*. In the case of Core Facilities, the logic model (Figure 18) describes the dependencies relating to the basic "housekeeping"/"lifeline" services general purpose, government and residential buildings require to provide administrative direction and to support non-specialist staff operations/business processes. These include *Electricity*, *Telecommunications* (specifically *Wired Communications*), and *Water and Wastewater* services and support, in turn, *Management*, production/Operations and *Maintenance and Repair* functions. (In this case supplies of *Petrol* and Natural Gas (*NG*) refer to supplies to support onsite generators which can be used to provide power in the event of a disruption in electrical distribution.)

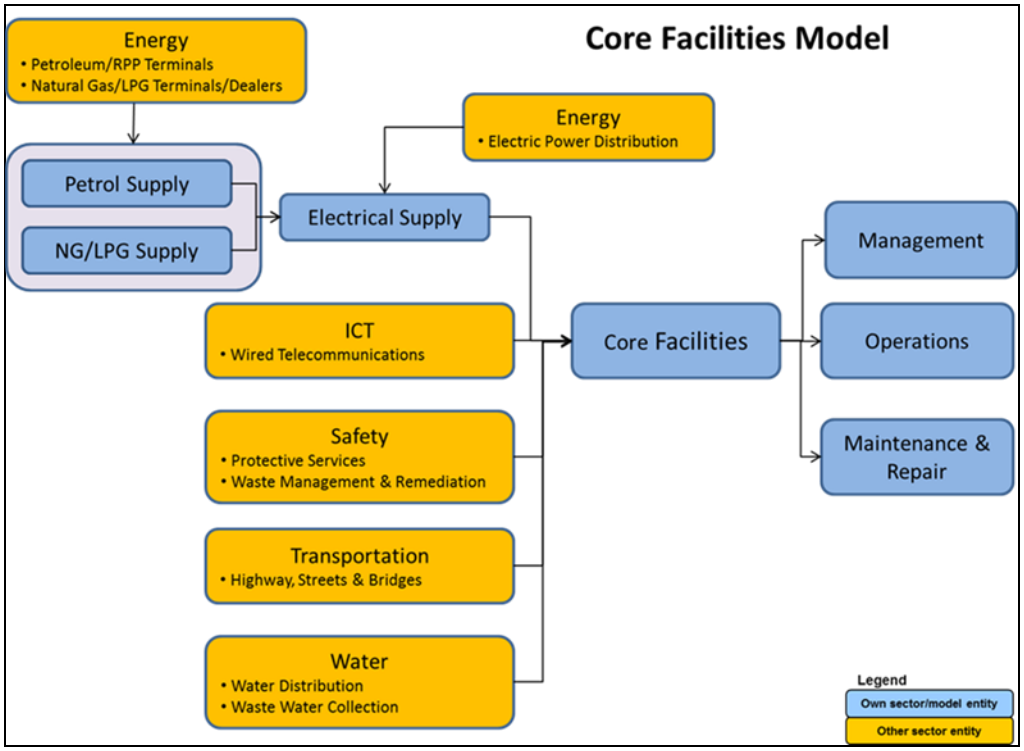

Figure 18: *Generic core facilities model.*

Generic NCIM *Management* and *Maintenance and Repair* models are shown below (Figure 19 and Figure 20). *Management* normally works from *Core Facilities* (e.g., administrative office and headquarters). And each sector relies on an available trained Labour Force. The degree of dependence on either may vary by sector and is entered separately in the NCIM. Similarly common upstream dependencies/inputs can be identified and are required to support *Maintenance and Repair* activities which sustain and support *Operations*, *Core Facilities* and sector *Vehicle Fleets*.

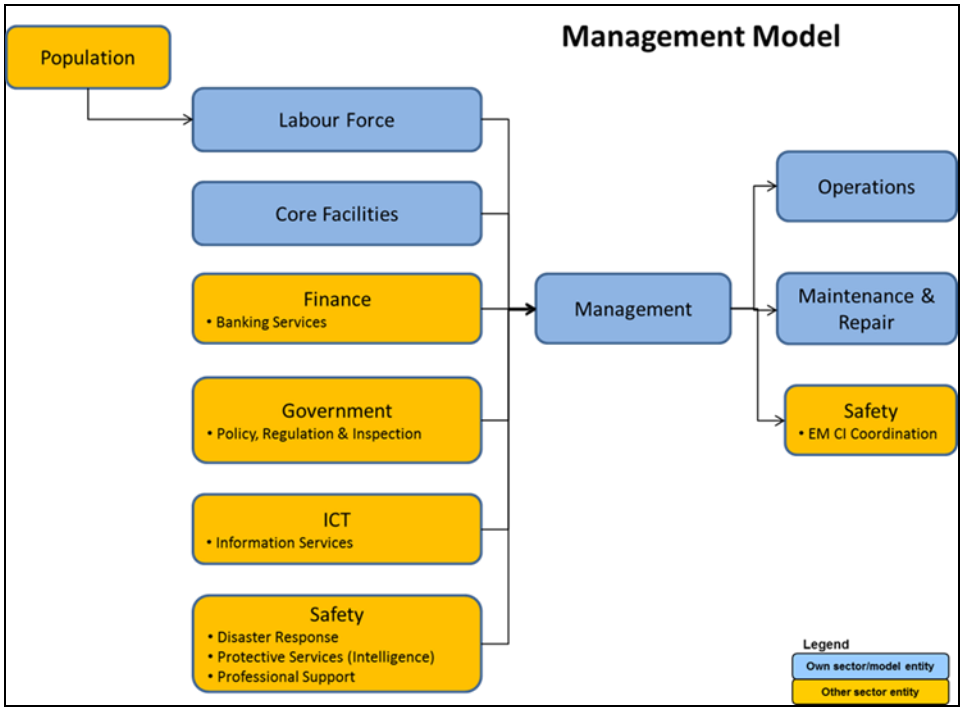

Figure 19: *Generic management model.*

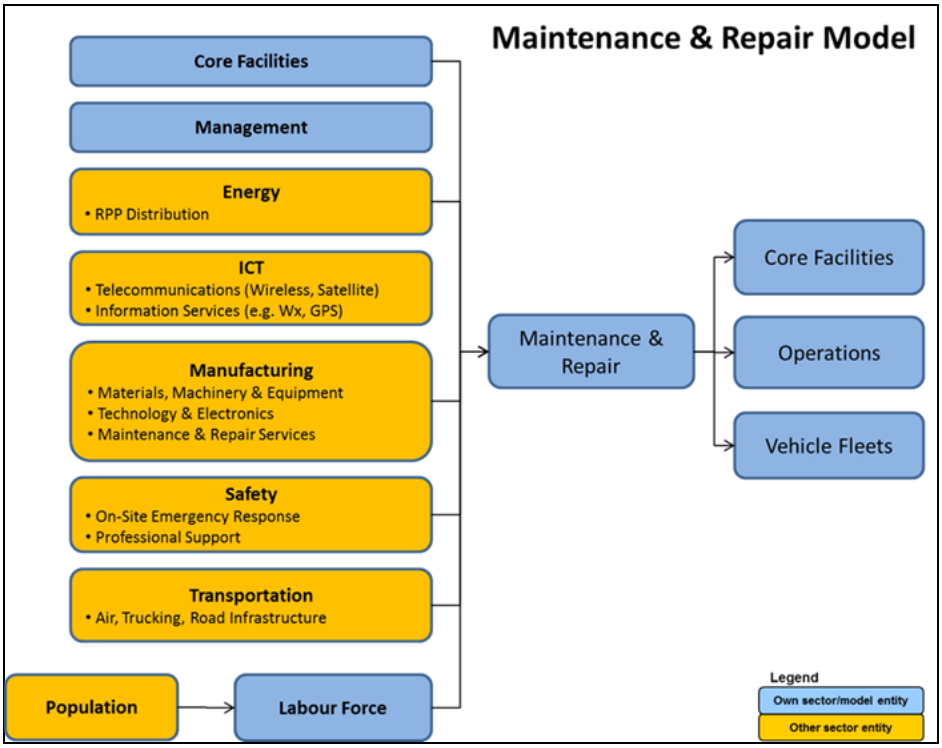

Figure 20: *Generic maintenance and repair model.*

3.7 RiskOutLook Representation

The dependencies depicted in the sector logic models (developed as simplified PowerPoint flow charts) were subsequently interpreted in more detail in terms of NAICS codes and a relational database generated using Microsoft ACCESS. The key *nodes* and relationships identified were then entered into a software application called *RiskOutLook*. Its roots derive from efforts to understand risk in order to prepare for Y2K.

RiskOutLook represents system and relational dependencies as a directed graph. Entities are distinguished as nodes and linked in a network. Each entity/node is considered to have an independent likelihood and consequence of failure. In applying the NCIM, functions are treated as nodes. The connections between entities in turn are represented as directed vectors, and each is assigned a dependency strength i.e., an evaluation of the likelihood that a downstream entity will fail if the upstream entity fails. *RiskOutLook* uses ordinal numbers to represent likelihood and consequence estimates. Normalized values are used and, hence, an agreed scale was needed to frame judgement—an element of subjective judgement is required to determine what constitutes *failure* and to assess the likelihood and impact of failure and ensure scoring consistency. A logarithmic scale[19] was adopted and a word ladder developed to facilitate scoring. The word ladder and consequence descriptions were based on those used in support of Public Safety's All Hazard Risk Approach.

[19] On a logarithmic scale, each mark on the scale is the previous tick mark *multiplied* by some number. Examples include the Richter scale for measuring the magnitude of earthquakes.

Using these entries, *RiskOutLook* calculates cumulative risk. It allows upstream dependencies to be traced and exploratory analysis conducted e.g., what is the effect of reducing or eliminating the likelihood or impact of failure at an upstream node. An example of the application's visualizations is shown below (Figure 21 and Figure 22). The first depicts the inter-sector dependencies associated with Wireless Services. The *RiskOutLook* models traces these to specific nodes/functions and these have been grouped into CI sectors for presentational purposes. The second offers a visual representation of (high level) intra-sector dependencies.

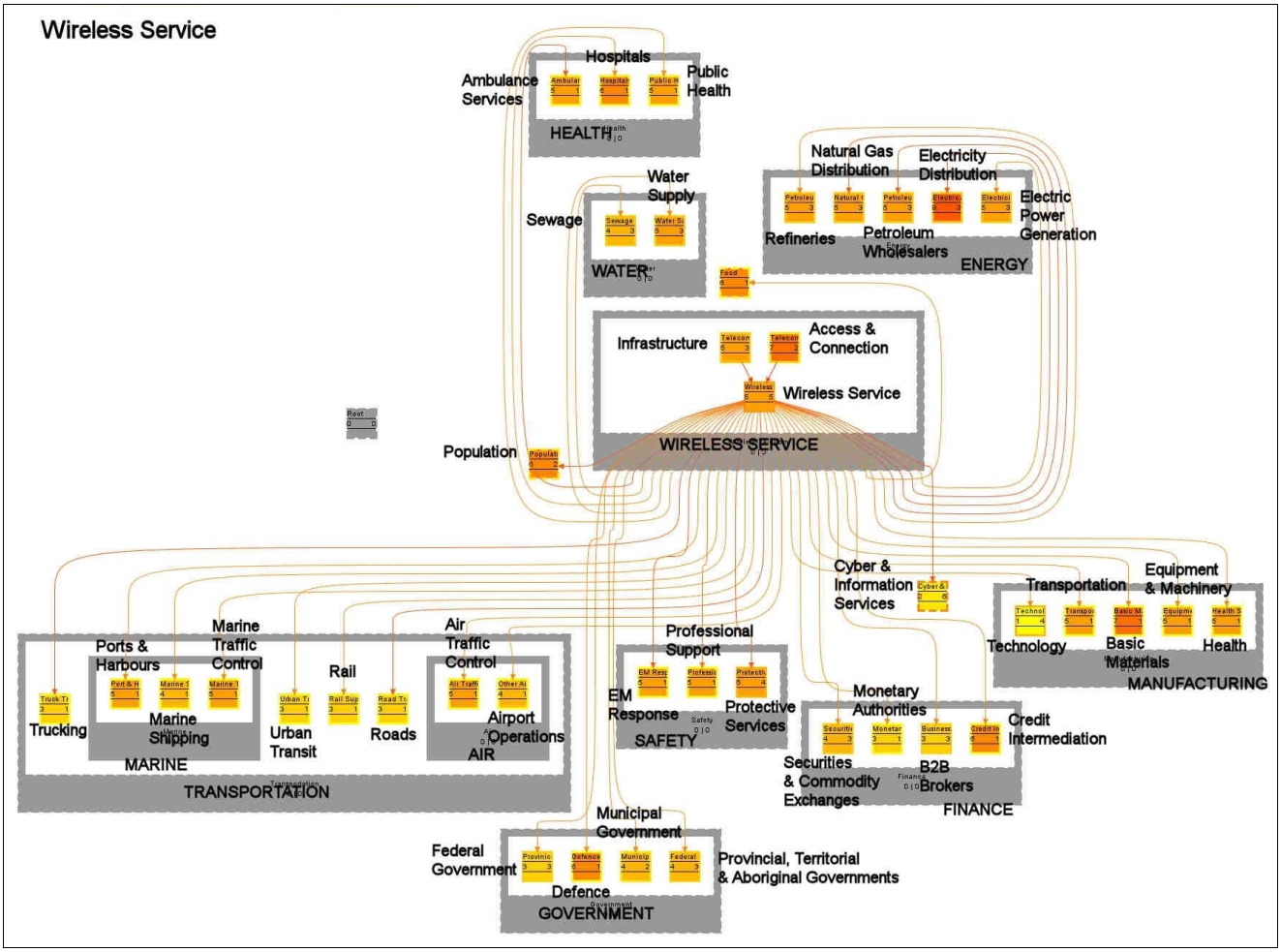

Figure 21: *Wireless services.*

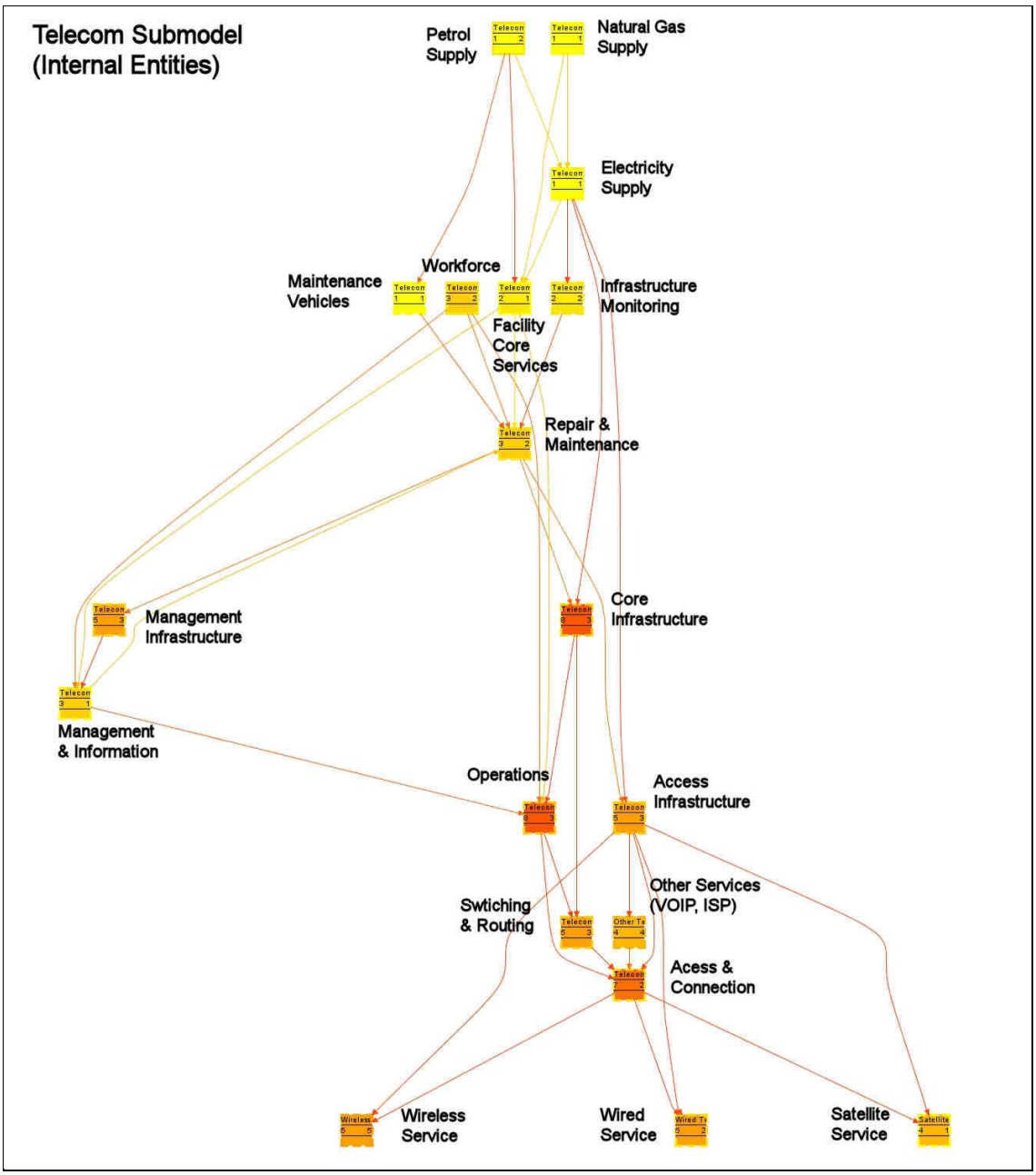

Figure 22: *Telecommunications intra-sector dependencies.*

4 Trends and Vulnerabilities

"Flows of data and information are, in some cases, replacing physical flows of goods" (US Department of Homeland Security, 2014). "The concept of critical infrastructure as discrete, physical assets has become outdated as everything becomes linked to cyberspace" (US Department of Homeland Security, 2014). Noteworthy trends in the ITC sector which will shape inter-sector and intra-sector dependencies include an increasing growth in mobile computing devices/applications, an increasing collection and use of big analytics/big data, an increasing exploitation of telecommunication links to enable remote monitoring and operation of systems, an increasing adoption of cloud services, a resultant increasing demand for ITC services and, given the pace of technological innovation, an increasing complexity of the supporting (physical, virtual and social) networks and infrastructure. The reliance of *Safety* sector and First Responders is of particular import. Canada is preparing for roll out of a Fifth Generation/5G wireless network reducing the latency in accessing content and potentially introducing a paradigm shift enabling real time operation of devices e.g., self-driving cars.

ICT systems are typically "open, chaotic, multi-order, recursively interdependent, widely dynamic, non-linear and unpredictable" (Bell, 2007). Networks offer an inherent element of resilience through the existence of alternate routes. Many threats such as small scale floods, fires and storms would result in localized and generally temporary disruption in services. Large scale hazards (e.g., an earthquake) would result in broader and longer disruption in services. Congestion risks compromising surviving ITC services and rationalization and optimization efforts driven by economic pressures and enabled by advances in technology have often reduced capacity.

"Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks" (US Department of Homeland Security, 2014). And malicious attacks pose another type of threat. They can be directed against physical infrastructure, virtual infostructure or users' confidence. Fortunately, although cyber threats are increasing in frequency, scale, sophistication and severity a catastrophic attack i.e., an attack on the national level is considered unlikely. A recent statement by the Director of US National Intelligence is instructive:

> *Rather than a "Cyber Armageddon" scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security* (Clapper, 2015).

Undermining assurance in processes and institutions may prove as much a threat as disrupting services. He went on to say:

> *Cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability. In the future, however, we might see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it* (Clapper, 2015).

One of systemic risk relates to attraction and retention of trained professionals. "The demand for ITC talent continues to grow"; "having a steady supply of skilled talent is critical" The Information and Communications Technology Council 2017).

5 Conclusion

The NCIM was developed in response to a national requirement for a more sophisticated understanding, ideally more quantitative, of interdependencies between CI sectors. Characterizing sectors and identifying functional relationships is an essential first step. The NCIM is a representation of a complex ecosystem. As with all models, it can be used to communicate/educate and to support analysis i.e., detailed examination and assessment. The NCIM can be used to elaborate and articulate concepts, to support operational/contingency plans, and to order gaps, evaluate options and inform acquisitions. While it is too early to judge the NCIM's utility and suitability, case studies suggest it has value to offer. It is expected that, moving forward, modifications to enhance the NCIM will be identified—both in response to potential requirements for more detail to accommodate additional case studies and in response to changes in the public safety and security environment.

The *ICT* sector is particularly susceptible to change. Digitalization and mobility are transforming business practices in both other CI sectors and the *ICT* sector as networks increase their relevance. Pervasiveness and the emergent Internet of Things will require security and privacy concerns to be an intrinsic consideration in every device, application and network.

5.1 Way Ahead

This report is one in a series of DRDC – CSS Reference Reports characterizing Canada's 10 CI sectors. (*Safety* was the first sector to be documented.) Documenting the characterization and modelling of the remaining sectors and producing a complementary *User's Guide to the NCIM* remain priorities.

Concurrently, support is/will be provided to initiatives exploiting the NCIM to investigate vulnerabilities using risk scenarios and to inform contingency and investment plans.

This Document will be posted on the Defence Research Reports website (http://pubs.drdc-rddc.gc.ca/pubdocs/pcow1_e.html). It is hoped that it will stimulate discussion and prompt feedback. Comments will be reviewed and, periodically, the NCIM will be refreshed.

Initial analysis indicates that, in the wake of an earthquake off the BC coast, *Food Distribution* would pose a significant risk. Opportunities permitting, the findings should be reviewed and confirmed. In addition, consideration should be given to modelling a risk scenario nominated by the *ICT* sector SMEs. This would provide an opportunity to expose and validate NCM characterization of the sector

References

Angelfire (2015), Access Network Planning and Technologies. Introduction to Telecommunications Networks, Angelfire Corporation Technical Reports, http://www.angelfire.com/nt/access1/web2001chap1.htm accessed 2 October 2015.

Bell Canada (2007), Cyber Interdependencies within Canada's Key Infrastructure Sectors, Bell Canada, July 2007.

Booz Allen Hamilton (2015), Cyber4Sight Special Report: 2016 Cyberthreat Predictions, Booz Allen Hamilton, 17 December 2015.

Canadian Radio-television and Telecommunications Commission (2019), About Us, The Canadian Radio-television and Telecommunications Commission Website, https://crtc.gc.ca/eng/acrtc/org.htm accessed 2 December 2019.

Canadian Security Telecommunications Advisory Committee (2015), CSTAC, The Canadian Security Telecommunications Advisory Committee, http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html accessed 30 July 2015.

Canadian Telecommunications Emergency Preparedness Association (CTEPA) (2009), Emergency Preparedness within the Telecom Industry, CTEPA, October 2009, https://www.slideserve.com/Antony/canadian-telecommunications-emergency-preparedness-association accessed 2 December 2009.

Canadian Telecommunications Resiliency Working Group (CTRWG) (2017), Canadian Telecommunications Resiliency Working Group, CTRWG Presentation to Regional Adaptation Workshop Telecom Breakout Session, 11 May 2017, https://cleanairpartnership.org/cac/wp-content/uploads/2017/05/Telecom_CTR_-_Presentation_for_May-11.pdf accessed 16 December 2019.

Canadian Wireless Telecommunications Association (CWTA) (2019), About CWTA, CWTA Website, https://www.cwta.ca/about-cwta/ accessed 2 December 2019.

Clapper, J, R. (2015), Statement for the Record on Worldwide Cyber Threats, US House Permanent Select Committee on Intelligence, 10 September 2015.

Communications Security, Reliability and Interoperability Council (2015), Cybersecurity Risk Management and Best Practices Working Group 4: Final Report, Communications Security, Reliability and Interoperability Council, March 2015, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf accessed 10 November 2015.

Data Bridge Market Research (2019), Wireless Mesh Network Market Research Report 2019: Industry Analysis By HypeLabs, Quantenna Communications, Hewlett Packard Enterprise Development, Qorvus Systems, Inc, FireTide Creative, Fluidmesh Networks And Others. *Stock News Magazine*, 5 April 2019, https://stocknewsmagazine.com/wireless-mesh-network-market-research-report-2019-industry-analysis-hypelabs-quantenna-communications-hewlett-packard-enterprise-development-qorvus-systems-inc-firetide-creative-fluidmesh-ne/ accessed 11 April 2019.

Data Economy (2017), Data Centres of the World will Consume 1/5 of Earth's Power by 2025*, Data Economy*, 12 December 2017, https://data-economy.com/data-centres-world-will-consume-1-5-earths-power-2025/ accessed 23 April 2019.

Department of National Defence (2017), Strong, Secure Engaged: Canada's Defence Policy, Department of National Defence, June, 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf accessed 19 June 2017.

Emergency Management Ontario (2016), Ontario Ministry of the Solicitor General website, https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/ci/ci.html, accessed 7 December 2016.

Federal Bureau of Investigation (2015), Private Industry Notification 151106-001, Federal Bureau of Investigation, 6 November 2015.

Gorshe, S. (2005), Introduction to Transport Networks for Telecommunications, PMC-Sierra, July 2005.

Information and Communications Technology Council (ICTC) (2017), *Digital Economy Annual Review 2017*, ICTC, https://www.ictc-ctic.ca/wp-content/uploads/2018/02/ICTC-Annual-Review-2017-EN.pdf accessed 9 April 2019.

Innovation, Science and Economic Development Canada (2016), Canadian ICT Sector Profile 2016, Innovation, Science and Economic Development Canada, https://www.ic.gc.ca/eic/site/ict-tic.nsf/eng/h_it07229.html accessed 9 April 2019.

Organization for Economic Co-operation and Development (2014), Glossary of Statistical Terms, Organization for Economic Co-operation and Development, http://stats.oecd.org/glossary/detail.asp?ID=6274 accessed 14 October 2014.

Public Safety and Emergency Preparedness Canada (2004), Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection, Government of Canada, November 2004, Appendix B, http://ccpic.mai.gov.ro/docs/Canada_non_paper.pdf accessed 2 July 2016.

Public Safety Canada (2009), National Strategy for Critical Infrastructure, Public Safety Canada, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx accessed 15 October 2014.

Public Safety Canada (2011), Federal Emergency Response Plan, Public Safety Canada, January 2011, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf accessed 14 October 2014.

Public Safety Canada (2014), Action Plan for Critical Infrastructure (2014–2017), Public Safety Canada, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx accessed 15 October 2014.

Sanger, D.E. and Schmitt, E. (2015), Russian Ships Near Data Cables Ate Too Close for U.S. Comfort, *The New York Times*. 25 October 2015, http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0 accessed 3 November 2015.

Sechrist, M. (2012), New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems, Harvard University, Belfer Centre for Science and International Affairs, February 2012, http://ecir.mit.edu/images/stories/sechrist-dp-2012-03-march-5-2012-final.pdf accessed 3 November 2015.

Statistics Canada (2017), North American Industry Classification System (NAICS) Canada 2017 Version 3.0, Statistics Canada, https://www150.statcan.gc.ca/n1/en/pub/12-501-x/12-501-x2016003-eng.pdf?st=Ty2Ak0d accessed 13 March 2019.

U.S. Department of Homeland Security (2010), Communications Sector-Specific Plan, 2010, U.S. Department of Homeland Security, http://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2010-508.pdf accessed 9 November 2015.

US Department of Homeland Security (2014), The 2014 Quadrennial Homeland Security Review, US Department of Homeland Security, June 2014, http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf accessed 17 February 2016.

U.S. Department of Homeland Security (2016a), Information Technology Sector-Specific Plan: An Annex to the NIPP 2013, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf accessed 31 August 2016.

U.S. Natural Resources Defense Council (2015), America's Data Centers Consuming and Wasting Growing Amounts of Energy, U.S. Natural Resources Defense Council, February 2015, https://www.nrdc.org/resources/americas-data-centers-consuming-and-wasting-growing-amounts-energy accessed 5 October 2015..

Annex A Key Stakeholders

- **Public Safety Canada (PS)** has two prime responsibilities. The first relates to collaboration with other federal departments and provincial and territorial governments, academia, national associations and non-governmental organizations to strengthen national emergency preparedness and enhance resiliency. The second is to assist in coordinating a federal response to emergencies and PS manages the Government Operations Centre and Regional Operations Centres.
- **Innovation, Science and Economic Development Canada (ISED) (formerly Industry Canada (IC))** mandate is to promote Canadian industry and contribute to fostering a growing and competitive economy. As the Primary Department for Emergency Support Function Number 4 Telecommunications, Industry Canada has specific responsibilities in the event of an emergency. These include:
  - coordinating with the telecommunications industry;
  - restoration and expansion of telecommunications infrastructure and services;
  - safeguarding and restoration of national telecommunications-related cyber and information technology resources; and
  - coordinating federal actions to provide the required temporary emergency telecommunications and restoration of the affected telecommunications infrastructure (Public Safety Canada, 2011).
- **The Canadian Radio-television and Telecommunications Commission (CRTC)** was established in 1968 to regulate and supervise Canadian broadcasting and telecommunications in the public interest. The CRTC is governed by the Broadcasting Act of 1991 and the Telecommunications Act of 1993. The Broadcasting Act seeks to ensure that all Canadians have access to a wide variety of high quality Canadian programming. The Telecommunications Act seeks to foster increased reliance on market forces for the provision of telecommunications services; provide efficient and effective regulation, where required; and ensure that Canadians have access to reliable telephone and other telecommunications services at reasonable prices. 1 The Acts also give authority to the CRTC to collect fees from the broadcasting and telecommunications industries, which fully fund the independent public authority's work (The Communications Radio-television and Telecommunuications Commission, 2015).
- The **Canadian Security Telecommunications Advisory Committee (CSTAC)** was established in 2010 to provide a forum for public and private stakeholders to share information and collaborate on a strategic level to promote telecommunications infrastructure resilience. Membership includes senior executives from the Canadian telecommunications industry, Industry Canada, Communications Security Establishment Canada, Public Safety Canada, Canadian Security Intelligence Service and the Privy Council Office (The Canadian Security Telecommunications Advisory Committee, 2015).
- The **Canadian Telecommunications Cyber Protection (CTCP) Working Group.**
- The **Canadian Telecommunications Emergency Preparedness Association (CTEPA)**. CTEPA was founded in 2000 to provide emergency planners representing wire line, wireless and satellite facility-based telecommunications companies a forum to promote industry preparedness. Specific objectives include:

- To promote a high level of informed practice amongst emergency managers in the telecom industry;
- To promote best practices for emergency preparedness for and through its membership; and
- To establish a process designed to facilitate mutual aid support in the event of a regional, national or international disaster communications companies in Canada.

- The **Canadian Telecommunications Resiliency Working Group (CTRWG)** was formed in 2016. It replaced CTEPA and has somewhat similar objectives to the CTEPA:
  - Share information on infrastructure interdependencies;
  - Develop proactive strategies to promote the resiliency of the critical infrastructure;
  - Develop policies/procedures to implement during incidents affecting Canadian critical telecommunications infrastructure;
  - Lead and participate in industry/government emergency preparedness exercises; and
  - Coordinate and act against threats that impact the Canadian telecommunications critical infrastructure.
- **The Canadian Wireless Telecommunications Association (CWTA)** members include cellular, PCS, messaging, mobile radio, fixed wireless, and mobile satellite carriers. The CWTA's primary role is to represent the wireless industry's interests before government and various regulatory agencies (The Canadian Wireless Telecommunications Association, 2019).
- The **Canadian Anti-Fraud Centre (CAFC),** located in North Bay, is jointly managed by the RCMP, Competition Bureau and the Ontario Provincial Police (OPP). It serves as a central repository for fraud related information and intelligence e.g., it collects and collates information on mass marketing fraud, advance fee fraud and identification thefts.
- Traditionally **Telephone Companies** (TELCOs) provided telephony services. The largest TELCOs—which dominating services—in Canada include Bell, Rogers and TELUS. Their corporate histories can be traced to the development of local exchanges and extensions to regional/national networks and wired to wireless networks. They now offer an increasing diverse range of ICT services.
- **Internet Service Providers** (ISPs) provides domain name registration, Internet access and web hosting services. Offerings may also include electronic mail, data storage and/or access to cloud-based applications.
- The vast majority of Canadian broadcasters including private radio and television stations are members of the **Canadian Association of Broadcasters** (CAB). The CAB serves as a national voice with specific interests in copyright advocacy, broadcast codes and accessibility (e.g., closed captioning).
- The Canadian **Broadcast Standards Council** (CBSC) is an independent organization established by the CAB to administer standards established by CAB members.
- The **Canadian Broadcasting Corporation/Societe Radio-Canada** (CBC/Radio-Canada) is a Crown corporation serving as the national public radio and television broadcaster.

Annex B Information and Communications Technology NCIM Functions

Table B.1: *Telecommunications NCIM functions.*

Telecommunication Functions	
Function_Name	**Function_Definition**
Telecommunications	Telecommunications industry
Telecom Management and Information	The collection and collation of applicable information/intelligence and subsequent formulation and implementation of management plans, programs and projects and provision and for providing telecommunications services
Telecom Network Management	The design, development and administration of practices related to directing operations of telecommunications networks
Telecom Control Systems	Industrial Control Systems (ICS), including SCADA systems, used to support automatic, remotely operated management of communications networks
Telecom Services	Services provided to enable the transfer or transmission of data over communications networks
Wired Telecommunications	The transmission of data between two points via a physically connected, wire-based communications network e.g., telephone lines, fibre-optic cables
Wireless Telecommunications	The transfer of data between points when at least one point is not physically connected via wires or cables e.g., through electromagnetic waves
Satellite Telecommunications	The transfer of data between ground stations and space-based geostationary transponders
Other Telecom Services (ISP, VOIP)	Telecommunications network access and transmission services provided by Internet Service Providers (ISP) including long-distance reselling, satellite tracking and VOIP services
Telecom Access and Connection	Entrée and connection to and from communications devices and networks.
Wired Telecom Access	Entree and connection to and from wired communication devices and networks
Wireless Access	Entree and connection to and from wireless communication devices and networks
Satellite Telecom Access	Entree and connection to and from satellite communication devices and networks
Telecom Switching and Routing	The automated selection of pathways and channelling of communications
Telecom Switching - Wire Line	The automated routing of wired communications
Telecom Switching - Wireless	The automated routing of wireless communications

Telecommunication Functions	
Function_Name	**Function_Definition**
Telecom Switching - Satellite	The automated routing of satellite communications
Telecom Switching - Internet	The automated routing of Internet communications
Telecom Transport	The long distance, core carriage, backbone network that provides connectivity between local/metro networks, community central offices, service providers (e.g., Internet) and regional or international gateways
Telecom Maintenance and Repair	Maintenance and repair activities undertaken to sustain and/or restore functioning of telecommunications services (e.g., facilities, equipment and networks)
Telecom Infrastructure Monitoring	The visual and virtual inspection of telecommunications infrastructure and monitoring of the volume and integrity of telecommunications flows
Telecom Maintenance Vehicles	Motor vehicles owned and operated by utilities and employed to support the maintenance and repair of telecommunications infrastructure (e.g., facilities, and equipment)
Telecom Workforce	The staff and workers employed in establishing, managing and maintaining telecommunications services
Telecom Facility Core Services	The aggregate of "hotel" services (electricity, wired communications, water and wastewater) within telecommunications transmission, operations and headquarters facilities
Telecom Electrical Supply	The provision and internal distribution of electricity within telecommunications facilities used to provide 'hotel' services and to operate fixed systems
Telecom Petrol Supply	The provision and internal distribution of petroleum/petrol products to telecommunications facilities and housed equipment
Telecom NG/LPG Supply	The provision and internal distribution of natural gas/liquefied natural gas to telecommunications related facilities and housed equipment
Telecom Facility Wired Telecom Networks	Wired-based connectivity and communications networks used to manage and operate telecommunications facilities and housed equipment
Telecom Facility Water and Wastewater	The provision and internal distribution of potable water to and collection and removal of wastewater from telecommunications facilities and housed equipment

Table B.2: *Information services NCIM functions.*

Information Service Functions	
Function_Name	**Function_Definition**
Cyber and Information Services	Information services provided over telecommunications networks.
DNS Services	The registration and hosting on services of Domain Name System (DNS) including address compilers, directories and electronic databases
Data Processing and Hosting	Hosting or data processing services including web hosting, video and audio streaming, application hosting or general time-share mainframe computing
Internet Publishing and Broadcasting	The publishing and/or broadcasting content on the internet or operating web sites and web search portals
Global Positioning System	A satellite-based constellation providing radio-navigation and timing services
Weather Services	Meteorological and weather forecasting services
All Other Information Services	Establishments providing general or industry-specific information services including a search and information retrieval capability
Information Services Facility Core Services	The aggregate of "hotel" services (electricity, wired communications, water and wastewater) within Information Services facilities
Information Services Electrical Supply	The provision and internal distribution of electrical power to Information Services facilities and housed equipment
Information Service Wired Telecom Networks	Wired telecommunication networks and network services owned by enterprises providing information services.
Information Services Water and Wastewater	The provision and internal distribution of potable water and the collection and removal of waste water from Information Services facilities and equipment

Table B.3: *Radio wave NCIM functions.*

Radio Wave Broadcasting Functions	
Function_Name	**Function_Definition**
Radio Wave Broadcasting	Operating radio and television broadcasting studios and facilities. (Emergency broadcast services)

Bibliography

Baylon, C., Brunt, R. and Livingstone, D. (2015), Cyber Security at Civil Nuclear Facilities: Understanding the Risks, Royal Institute of International Affairs, Chatham House Report, September 2015, https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks accessed 15 October 2015.

Government of Canada (2013), Cyber Incident Management Framework for Canada, Government of Canada, August 2013, http://publications.gc.ca/collections/collection_2013/sp-ps/PS4-184-2013-eng.pdf accessed 7 July 2017.

Department of National Defence (2017), Strong Secure Engaged: Canada's Defence Policy, Department of National Defence, June 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf accessed 19 June 2017.

Lucas, M., Sands, A. and Wolfe, D.A. (2009), Regional Clusters in a Global Industry: ICT Clusters in Canada, *European Planning Studies* Vol. 17, No. 2 February 2009.

Mell, P. and Grace, T. (2011), The NIST Definition of Cloud Computing, U.S. Department of Commerce, NIST Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf accessed 15 July 2015.

Public Safety Canada (2016), Fundamentals of Cyber Security for Canada's Critical Infrastructure Community, 1st Edition, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf accessed 7 July 2017.

Stoneburner, G. (2001), Underlying Technical Models for Information Technology Security, NIST Special Publication 800-33, U.S. Department of Commerce, December 2001 http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf accessed 15 July 2015.

Townsend, A.M. and Moss, M.L. (2005), Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communication, April 2005.

U.S. Department of Homeland Security (2016b), Communications Sector-Specific Plan: An Annex to the NIPP 2013, Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf accessed 31 August 2016.

US Department of Homeland Security (2016c), National Cybersecurity and Communications Integration Centre. Seven Strategies to Defend ICS, Department of Homeland Security, 2016, https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf accessed 23 January 2016.

List of Symbols/Abbreviations/Acronyms/Initialisms

CAB	Canadian Association of Broadcasters
CAFC	Canadian Anti-Fraud Centre
CBC	Canadian Broadcasting Corporation
CBSC	Canadian Broadcast Standards Council
CI	Critical Infrastructure
CONOP	Concepts of Operation
CSRIC	Communications Security, Reliability and Interoperability Council
CSS	Centre for Security Science
CTEPA	Canadian Telecommunications Emergency Preparedness Association
CTCP	Canadian Telecommunications Cyber Protection
CTCP WG	Canadian Telecommunications Cyber Protection Working Group
CWTA	Canadian Wireless Telecommunications Association
DCSs	Digital Cross Connect Systems
DHS	Department of Homeland Security (U.S.)
DNS	Domain Name System
DRDC	Defence Research and Development Canada
FBI	Federal Bureau of Investigation
HFC	Hybrid Fiber/Coaxial
IC	Industry Canada
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IMT	International Mobile Telecommunications
IP	Internet Protocol
ISED	Innovation, Science and Economic Development Canada
ISP	Internet Service Provider
ITU	International Telecommunication Union
NAICS	North American Industry Classification System
NCIM	National Critical Infrastructure Interdependency Model
NCSF	National Cross Sector Forum
NGNs	Next Generation Networks
OECD	Organization for Economic Co-operation and Development
OPP	Ontario Provincial Police
PS	Public Safety Canada
PSTN	Public Switched Telephone Network
RF	Radio Frequency
RFID	Radio Frequency Identification
SCADA	Supervisory Control And Data Acquisition
SDN	Service Delivery Network
SME	Subject Matter Expert
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TELCO	Telephone Companies
TT and C	Telemetry, Tracking and Command
URIs	Uniform Resource Indicators

VSAT	Very Small Aperture Terminal
WANS	Wide Area Networks
WLAN	Wireless Local Area Network

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.) DRDC – Ottawa Research Centre Defence Research and Development Canada, Shirley's Bay 3701 Carling Avenue Ottawa, Ontario K1A 0Z4 Canada	2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.) CAN UNCLASSIFIED 2b. CONTROLLED GOODS NON-CONTROLLED GOODS DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

The National Critical Infrastructure Interdependency Model—Volume VII: Characterizing the Information and Communications Technology Sector

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Chouinard, P.; Hales, D.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
April 2020	49	30

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Reference Document

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada, Shirley's Bay
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC-RDDC-2020-D046	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Critical Infrastructure Resilience; Capability Based Planning; Risk Analysis

13. ABSTRACT (When available in the document, the French version of the abstract must be included here.)

In an increasingly connected and uncertain world, it is important to broaden horizons and appreciate what partners bring to the table and the challenges they face. A National Critical Infrastructure Interdependency Model (NCIM) was developed to assist Public Safety Canada (PS) and Critical Infrastructure (CI) owners and operators identify dependency relationships and recognize imported risk with a view to informing and enhancing resiliency. Characterization of the 10 CI sectors was an important first step. Functional decompositions and logic models were developed to describe each sector as a prelude to developing a relational database and an integrated model. Subsequently a software application (*RiskOutLook*®) was employed to calculate cumulative/cascading risk. This report describes how the *Information and Communications Technology* (ICT) sector was characterized.

Dans un monde de plus en plus interconnecté et incertain, il est important d'élargir ses horizons et de comprendre ce que nos partenaires nous apportent, de même que les difficultés auxquelles ils font face. On a élaboré un modèle d'interdépendances des infrastructures essentielles nationales (MIIEN) pour aider Sécurité publique Canada (SPC), de même que les propriétaires et exploitants d'infrastructures essentielles (IE) à déterminer les relations de dépendance et à reconnaître les risques importés en vue de favoriser et d'accroître la résilience. La caractérisation des dix secteurs d'IE représentait une première étape importante dans ce but. On a également élaboré des décompositions fonctionnelles et des modèles logiques pour décrire chaque secteur comme premier pas vers la création d'une base de données relationnelles et d'un modèle intégré. Par la suite, on s'est servi d'une application logicielle (*RiskOutLook*®) pour calculer les risques cumulatifs ou en cascade. Le présent rapport fournit une description de la méthode de caractérisation du secteur des *technologies de l'information et des communications* (TIC).