Critical Infrastructure Protection and Resilience Literature Survey: State of the Art

Prepared by:
Erica Wiseman
National Research Council
6100 Ave Royalmount
Montreal, QC

Tamara McLaughlin
National Research Council
6100 Ave Royalmount
Montreal, QC

Contract Scientific Authority:
Nezih Mrad
DRDC Centre for Security Science
613-947-1198

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of the Department of National Defence of Canada.

DRDC Project #CSSP-2013-TI-1039

---

Contract Report
DRDC-RDDC-2015-C160
March 2014
Critical Infrastructure (CI) Interdependency Model Development in Support of Federal Government Continuity CSSP-2013-TI-1039 was supported by the Canadian Safety and Security Program which is led by Defence Research and Development Canada’s Centre for Security Science, in partnership with Public Safety Canada. The project was led by Public Safety Canada in partnership with National Research Council of Canada.

Canadian Safety and Security Program is a federally-funded program to strengthen Canada’s ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence.
Critical Infrastructure Protection and Resilience Literature Survey: State of the Art

Prepared for
Nezih Mrad, PhD., Operational Research & Analysis Scientist
Nezih.Mrad@drdc-rddc.gc.ca
Nezih.Mrad@forces.gc.ca
Defense R&D Canada, Centre for Security Science – Ottawa

Prepared by
Erica Wiseman, PhD., Strategic Information Analyst
Erica.wiseman@nrc-cnrc.gc.ca

Tamara McLaughlin, Information Specialist
Tamara.mclaughlin@nrc-cnrc.gc.ca

DRDC Project # CSSP-2013-TI-1039
NRC Project # 18526

NRC-KM employees make every effort to obtain information from reliable sources. However, we assume no responsibility or liability for any decisions based upon the information presented.
CIPR Literature Survey: State of the Art
March 2014

Table of Contents

1 EXECUTIVE SUMMARY ........................................................................................................................................... 7

2 BACKGROUND ........................................................................................................................................................... 9
  2.1 CONTEXT ......................................................................................................................................................... 9
  2.2 KEY ISSUES ................................................................................................................................................. 9
  2.3 KEY QUESTIONS ......................................................................................................................................... 9

3 INTRODUCTION .................................................................................................................................................... 10

4 DEFINITIONS AND CI SECTORS ..................................................................................................................... 10

5 EMERGING TRENDS .............................................................................................................................................. 14
  5.1 MAJOR TERMS .............................................................................................................................................. 14
  5.2 TOP SUBJECTS ........................................................................................................................................... 19
  5.3 EMERGING TRENDS ................................................................................................................................... 22
    5.3.1 General CIPR Topics ............................................................................................................................. 24
    5.3.2 CI Sectors .......................................................................................................................................... 26
    5.3.3 Mitigation: Physical Countermeasure ................................................................................................. 27
    5.3.4 Mitigation: Non-physical countermeasures ....................................................................................... 29
  5.4 KEY PLAYERS ........................................................................................................................................... 31
  5.5 METRICS AND SURVEYS .......................................................................................................................... 33

6 NATIONAL CIPR STRATEGIES .......................................................................................................................... 35
  6.1 OVERVIEW OF NATIONAL STRATEGIES ............................................................................................ 35
    6.1.1 Canadian National Strategy & Action Plan ......................................................................................... 36
    6.1.2 US National Strategy .......................................................................................................................... 39
    6.1.3 UK National Strategy ........................................................................................................................ 40
    6.1.4 Australian National Strategy ............................................................................................................ 42
  6.2 COMPARISON OF NATIONAL STRATEGIES .......................................................................................... 43
    6.3 CYBER SECURITY STRATEGIES .......................................................................................................... 45
      6.3.1 Canadian Cyber Security Strategy .................................................................................................. 45
      6.3.2 UK Cyber Security Strategy ........................................................................................................ 47
      6.3.3 Australian Cyber Security Strategy ............................................................................................... 47
  6.4 COMPARISON OF CYBER SECURITY STRATEGIES ............................................................................. 48

7 CONCLUSION ......................................................................................................................................................... 49

8 REFERENCES ......................................................................................................................................................... 52

9 APPENDIX ......................................................................................................................................................... 59
  9.1 SEARCH STRATEGY ...................................................................................................................................... 59
  9.2 R&D MOMENTUM ..................................................................................................................................... 59
  9.3 BUILDING THE CI SECTOR GROUPS ..................................................................................................... 61
  9.4 CANADIAN AFFILIATIONS PROFILE ....................................................................................................... 62
List of Figures

Figure 1: Publication velocity ................................................................. 14
Figure 2: Top 23 terms (≥150 publications) ....................................................... 15
Figure 3. Top 300 Terms Cluster Map ............................................................ 16
Figure 4. Top 300 Terms Cluster Map – Additional Clusters ......................... 18
Figure 5. Top 32 Subject Groups – with 200+ records ...................................... 19
Figure 6. Top 32 Subject Groups, Percentage Share Comparison, Early vs. Late Period 20
Figure 7. 60 Subject groups cluster map (filter set to 23%) ............................... 21
Figure 8. General CIPR Topics, 2008-2013: Recent Trends ............................... 25
Figure 9. CI Sectors, 2008-2013: R&D Momentum ........................................... 26
Figure 10. Mitigation: Physical countermeasures, 2008-2013: R&D Momentum 28
Figure 11. Mitigation: Non-physical countermeasures, 2008-2013: R&D Momentum 30
Figure 12. Top 10 Publishing Countries .............................................................. 31
Figure 13. Top Affiliations - with 30+ Publications .............................................. 32
Figure 14. Canadian Affiliations - with 3+ Publications ........................................ 33
Figure 15. 4 Quadrants Momentum Indicator .......................................................... 60
List of Tables

Table 1: Key Definitions in CIPR ................................................................. 11
Table 2: Critical Infrastructure Sectors around the World .................................................. 13
Table 3. 4 Thematic Groups of 60 subject groups ......................................................... 23
Table 4. Metrics Related to CIPR ............................................................................... 33
Table 5. Number of National CIPR Strategy Publications for Selected Nations 35
Table 6. List of National Strategy Documents used for Comparison between Nations 36
Table 7. Search Terms ............................................................................................... 59
Table 8. Building the CI Sector Groups ....................................................................... 61
Table 9. Canadian Affiliations Profile .......................................................................... 62
1 EXECUTIVE SUMMARY

Defence R&D Canada’s Centre for Security Science (CSS) is working in partnership with Public Safety Canada (PS) to develop an integrated national and regional Critical Infrastructure (CI) Dependency model for CI risk analysis and risk mitigation in support of the 2010 National Critical Infrastructure Strategy. To frame discussions and serve as a starting point, CSS has requested that NRC Knowledge Management perform an exploratory study of existing scientific, industrial and government (domestic/international) literature on critical infrastructure protection and resilience (CIPR) and related concepts.

This report presents a review of the key definitions, international CI sectors, major and emerging research trends in CIPR and a high level comparison of the Canadian, US, UK and Australian national CIPR strategies. A total of 4,597 records published between 2003 and 2013 were retrieved and analyzed using text mining software and a variety of visualization tools to identify trends in the literature and key players. An extensive bibliography is provided with this report listing various international CIPR related strategies, policies, frameworks; some of which were used in the comparison section of the report.

<table>
<thead>
<tr>
<th>Key Question</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key definitions</strong></td>
<td>Clear definitions were only found for critical infrastructure and CI resilience, but not for critical assets or CI protection.</td>
</tr>
<tr>
<td></td>
<td>Only one military source that provided definitions was found and did not differ much from the civilian.</td>
</tr>
<tr>
<td></td>
<td>In very general terms, CI and CI resilience are defined as follows:</td>
</tr>
<tr>
<td></td>
<td>Critical Infrastructure: key buildings, facilities, systems or networks that are essential and vital to the nation’s functioning and security.</td>
</tr>
<tr>
<td></td>
<td>CI Resilience: the ability to prepare, adapt, respond, recover and continue functioning in the face of a disaster.</td>
</tr>
<tr>
<td><strong>CI Sectors</strong></td>
<td>CI sectors were compared for Canada, US, UK, EU, Australia and NZ.</td>
</tr>
<tr>
<td></td>
<td>Every nation included energy, water, transport, ICT, health, food supply, banking/finance, government services, safety/emergency services.</td>
</tr>
<tr>
<td></td>
<td>The US has the longest list with 16 sectors, Canada with 10, and the UK with 9.</td>
</tr>
<tr>
<td></td>
<td>No means or methods of ranking the sectors in terms of vulnerability or resilience was found but a closer examination of the various metrics and indices in the field may reveal otherwise and thus should be further explored.</td>
</tr>
<tr>
<td><strong>Major topics</strong></td>
<td>General CIPR topics: Disaster/accident/emergency, Vulnerability, Terrorism, Threat, Interdependencies.</td>
</tr>
<tr>
<td></td>
<td>Throughout the dataset close ties are seen between ICT and Cyber security.</td>
</tr>
<tr>
<td></td>
<td>There has been an increasing interest in Disasters (and in particular, Natural disasters) and a comparative decrease in interest in Terrorism in the past five years.</td>
</tr>
<tr>
<td><strong>Emerging topics</strong></td>
<td>General CIPR topics: Mitigation/Prevention, Resilience, Climate change, Sustainability, Cascading effects.</td>
</tr>
<tr>
<td></td>
<td>CI sectors: Coastal &amp; Waterways.</td>
</tr>
<tr>
<td></td>
<td>Mitigation strategies: Detection, Intrusion detection, Structural aspects, Artificial Intelligence, Sustainability and Ontology/semantics.</td>
</tr>
<tr>
<td><strong>Metrics and surveys</strong></td>
<td>51 publications discuss specific metrics or measurements or indices related to the field of CIPR.</td>
</tr>
<tr>
<td></td>
<td>17 publications specifically focused on metrics for protection or resilience of critical infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Six surveys in the dataset involved questionnaires, interviews and the like.</td>
</tr>
<tr>
<td><strong>Key Canadian players</strong></td>
<td>University of British Columbia.</td>
</tr>
<tr>
<td></td>
<td>University of Western Ontario.</td>
</tr>
<tr>
<td>Key Question</td>
<td>Findings</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>University of Ottawa.</td>
</tr>
<tr>
<td></td>
<td>DRDC-Centre for Security Science.</td>
</tr>
<tr>
<td>Comparison of national CIPR strategies</td>
<td>All nations focus on the importance of information sharing and partnerships and view owners/operators of CI as holding the ultimate responsibility for protection and resilience.</td>
</tr>
<tr>
<td></td>
<td>Both Canadian and US CIPR strategies are built on the core themes of prevention, protection or preparedness, mitigation, response and recovery.</td>
</tr>
<tr>
<td></td>
<td>The Canadian strategy is significantly lighter on details than other national plans, however the latest 2014 Action Plan for Critical Infrastructure does provide more detail and guidance.</td>
</tr>
<tr>
<td></td>
<td>Canada remains focused on protection and risk management while other nations have moved more explicitly to resilience.</td>
</tr>
<tr>
<td></td>
<td>Canadian sector-specific plans are not publicly available in contrast to other nations reviewed.</td>
</tr>
</tbody>
</table>

Numerous recommendations for future research are included in the conclusion, including, but not limited to:

- Continue to monitor the emerging topics found in this study, especially climate change, and coastal and waterways as a sector;
- Conduct a more targeted search and analysis of metrics in the field;
- Perform a more in depth analysis of the implementation activities, action plans and/or sector-specific plans associated with the national strategies reviewed in this study as valuable lessons learned which may contribute to improving the resilience of Canada’s own critical infrastructure.
2 BACKGROUND

2.1 Context

In 2009, the Canadian federal government, provinces and territories agreed on a National Strategy\(^1\) and Action Plan for Critical Infrastructure.\(^2\) The purpose of this initiative is to strengthen the resilience of Canadian Critical Infrastructure (CI) by building partnerships, implementing hazards risk management approaches, and advancing the timely sharing and protection of information among partners. The strategy recognized that critical infrastructures are at risk from natural, intentional and accidental hazards and that the risk could be exacerbated by the complex system of interdependencies among critical infrastructure, which can lead to cascading effects across borders and sectors. The Action Plan includes the establishment of sector networks and a cross-sector forum as the basis for collaborative work and information sharing. The Centre for Security Science (CSS) is working in partnership with Public Safety (PS) Canada on initiatives to address some of the objectives identified within the strategy and its action plan in order to increase Canadian infrastructure resiliency, develop strong communities and implement an all-hazards risk management approach. The continuity of national governance to maintain public health, safety, security, economic well-being and the confidence during or after any disaster or emergency is one of the goals. The development of national and regional interdependency modeling tools and methodologies to understand CI interdependencies and the cascading effect of events is another important initiative.

2.2 Key Issues

To frame discussions and serve as a starting point in the development of a national and regional CI model tool, CSS has commissioned an exploratory study of existing scientific, industrial and government (domestic/international) literature on critical infrastructure protection and resilience (CIPR) and related concepts, including, but not limited to, risk mitigation mechanisms, CI interdependencies as well as modeling and simulation tools and techniques. This study examines the existing body of knowledge and attempt to structure the current state of knowledge of CIPR and its interdependencies. It is anticipated that the results of this work will yield a more in depth and enhanced understanding of the concepts, activities and tools associated with CIPR in terms of physical and cyber security systems. Additionally, it will help CSS develop advanced capabilities and expertise in the area, as well as highlight gaps, lessons learned and opportunities for next steps in the pursuit of an integrated CIPR strategy.

2.3 Key Questions

1. Define and compare CI, critical assets, CI protection, and CI resilience from civilian/government and military perspectives.
2. What are the commonly defined Canadian, US and worldwide CI sectors? Can these sectors be ranked in terms of vulnerability and/or resilience?
3. What are the major and emerging research and technology trends in CIPR?
   a. Are there existing metrics or measurement frameworks for assessing CI protection and resilience?
   b. Identify key players in Canada, including working groups.
4. What policies and strategies exist in Canada, US, EU, Iceland, Norway, Denmark, UK, Australia and New Zealand at both the civilian and military levels that focus specifically on CIPR?
   a. Provide a high level comparison of the similarities and differences between the latest version of the Federal Canadian, American, British and Australian CI strategies.
5. What are the key observations/lessons learned for increased CIPR to intentional and unintentional threats and risks?
INTRODUCTION

To address the key questions, data were gathered from three bibliographic databases as well as several web searches. The complete list of sources and the search strategy are described in section 9 of this report. The final dataset used for analysis of major and emerging research and technology trends had a total of 4,597 records published between 2003 and 2013. The data were loaded into VantagePoint, a text mining application, where terms were selected and various subject groupings were made to enable analysis. The key data points or fields used for most analyses were Subjects, Publication Year and Affiliations (sponsoring organizations or institutions affiliated with the authors). The subject field is an amalgam of author-supplied keywords and controlled subject terms. These subject terms were selected to merge singular and plural forms, to group words with very similar meaning, and to normalize vocabularies as much as possible.

Two levels of grouping were made:

Subject Groups: subject terms were organized into 60 groups based on key topics in the CIPR field as identified by literature reviews, relevant websites, and conversations with the client. The 60 subject groups were created by manually grouping together related terms in VantagePoint. For instance, the information and communication technology (ICT) Sector group was created by grouping terms such as communication, information technology, telecommunication, Internet as well as larger terms related to these words, such as wireless telecommunication systems. The 60 subject groups cover 97% of the entire dataset.

Thematic Groups: All the subject groups were further categorized into four thematic “groups of groups” to enable the comparison of groups with similar themes and the detection of topics with increasing levels of research in the last five years. The four thematic groups are: CIPR core concepts, CI sectors, Mitigation: physical countermeasures, Mitigation: non-physical countermeasures. These thematic groups were also created based on a review of the literature and were finalized through conversations with the client.

A bibliography listing the policies and strategies that exist in Canada, US, EU, Iceland, Norway, Denmark, UK, Australia and New Zealand that focus specifically on CIPR (excluding emergency management frameworks for the most part) was produced (not included in this report) from which a high level comparison of the Canadian, US, British and Australian CIPR strategies was developed and presented in section 6.

DEFINITIONS AND CI SECTORS

Table 1 presents key CIPR definitions that are found in select federal documents and websites.

---

VantagePoint is produced by the US company Search Technology: http://www.thevantagepoint.com/
<table>
<thead>
<tr>
<th>Critical Infrastructure</th>
<th>Canada Civilian</th>
<th>US Civilian</th>
<th>Australian Civilian</th>
<th>UK Civilian</th>
<th>US Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada Civilian</td>
<td>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. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.</td>
<td>The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.</td>
<td>Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security. It is important to note that some elements of critical infrastructure are not assets, but are in fact networks or supply chains.</td>
<td>The national infrastructure comprises networks, systems, sites, facilities and businesses that deliver goods and services to citizens, and support our economy, environment and social well-being.</td>
<td>The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. Defense CI is a combination of task critical assets and defense critical assets.</td>
</tr>
<tr>
<td>Australia Civilian</td>
<td>The national infrastructure comprises networks, systems, sites, facilities and businesses that deliver goods and services to citizens, and support our economy, environment and social well-being.</td>
<td>The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. Defense CI is a combination of task critical assets and defense critical assets.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Critical Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada Civilian</td>
</tr>
<tr>
<td>US Civilian</td>
</tr>
<tr>
<td>Australian Civilian</td>
</tr>
<tr>
<td>UK Civilian</td>
</tr>
<tr>
<td>US Defense</td>
</tr>
<tr>
<td>Defined variously as:</td>
</tr>
<tr>
<td>• Assets that “would, if destroyed or disrupted, cause national or regional catastrophic effects”</td>
</tr>
<tr>
<td>• Minimum essential infrastructure</td>
</tr>
<tr>
<td>• Assets deemed “Vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any State, or any local government.”</td>
</tr>
</tbody>
</table>

N/A | N/A | N/A | The DoD recognizes two types of critical assets: defense critical assets, and task critical assets. |
| • A defense critical asset is an “asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions” |
| • A task critical asset is an “asset that is of such extraordinary importance that its incapacitation or destruction would have a
<table>
<thead>
<tr>
<th>CI Protection/CI Security</th>
<th>Canada Civilian</th>
<th>US Civilian</th>
<th>Australian Civilian</th>
<th>UK Civilian</th>
<th>US Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N/A</td>
<td>Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.⁶</td>
<td>N/A</td>
<td>N/A</td>
<td>Defense Critical Infrastructure Protection is a “DOD risk management program that seeks to ensure the availability of DCI”.⁶</td>
</tr>
</tbody>
</table>

| CI Resilience             | The capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure.⁷ | The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.⁹ | In the context of critical infrastructure, resilience refers to:  
  • coordinated planning across sectors and networks  
  • responsive, flexible and timely recovery measures, and  
  • the development of an organisational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly.⁴ | Resilience is the ability of assets, networks and systems to anticipate, absorb, adapt to and/or rapidly recover from a disruptive event.⁷ | The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change.¹⁰ |

⁵ Defense Infrastructure Sector Lead Agent  
⁴ There were no explicit definitions of CI protection and only a single US definition of CI security.
Beyond the definitions presented in Table 1, no other distinctions between military and civilian definitions were found in this study, likely due to the classified nature of military documents. Notable in Table 1 is the lack of federal definitions of critical assets in Canada and critical infrastructure protection in both Canada and the US. At the US federal level, the Department of Homeland Security (DHS) uses the term CI Security, seemingly instead of CI protection. DHS defined security as “reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters”. 11

Table 2 presents the Critical Infrastructure sectors that are identified by various nations around the world. A few noteworthy points about Table 2 include:

- The sectors in the table are listed with Canadian sectors first, followed by US sectors.
- Naming conventions are sometimes the cause of apparent “gaps”. For instance, unlike the US, Canada does not have an Emergency Services sector, but does have a Safety sector. Similarly, Canada has identified an Information and Communication Technology (ICT) sector, while other nations have a Communications sector. Only the US has a separate sector for Information Technology.
- Other gaps can be explained by certain sectors being subsumed by others in different nations. This is notably the case with the US Dams sector which, in Canada, falls under the responsibility of the Safety sector. Similarly, the US Chemical sector is covered in Canada under Manufacturing.

Table 2: Critical Infrastructure Sectors around the World

<table>
<thead>
<tr>
<th>Sector</th>
<th>Canada</th>
<th>US</th>
<th>UK</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy &amp; Utilities</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Water</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Transportation</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Health</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Food</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Finance</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Government</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>ICT</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Services</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Information Technology</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Chemical Sector</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dams</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commercial Facilities</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defense Industrial Base</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nuclear reactors, materials &amp; waste</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5 EMERGING TRENDS

Figure 1 shows the publication velocity in the CIPR domain, based on all publications in the dataset. The overall curve is rising, quite steeply since 2009 which happens to coincide with the publication of the 2nd edition of the US National Infrastructure Protection Plan. While this alone would not necessarily explain the rise, the US does represent roughly 40% of affiliations in the dataset and research and development in that nation is on the rise. The drop in 2013 is likely due to delays in publications being indexed in the search databases as opposed to a decline in interest in the topic.

![Figure 1: Publication velocity](image)

5.1 Major Terms

An examination of the top terms in the dataset can give us evidence of themes in the research literature and gives us indications of the groups and relationships (correlations) between topics. For instance, Figure 2, which presents the top 23 terms in the dataset based on number of publications (≥150 publications), reflects the relative amount of attention devoted to risk assessment/analysis/management as well as ICT and Cybersecurity related terms.
Figure 2. Top 23 terms (≥150 publications)
Cluster analysis based on the co-occurrence of keywords in bibliographic records is another method of visualizing and analyzing topics that are important in a domain and their relationships to each other. Figure 3 shows details of a cluster map based on the top 300 terms, generated using TouchGraph Navigator\(^d\) software. Each node or bubble in the map represents a subject term. TouchGraph’s clustering algorithm clusters terms together based on statistical similarity to each other (i.e. word co-occurrences) and dissimilarity with other clusters. Generally, a cluster illustrates a self-contained group of concepts that is independent from (though still connected to) the rest of the graph. The size of the nodes in this map represents the relative number of publications associated with each node and the lines in between nodes show the correlation coefficient (multiplied by 100) between two nodes. Only correlations of 20% or greater are shown in any of the cluster maps below.

\(^d\) TouchGraph Navigator is produced by the US company TouchGraph LLC: http://www.touchgraph.com/navigator
The cluster map shows the close correlation between many of the subject areas in the dataset. On the far right in purple, many of the terms related to cyber security and ICT are clustered together. This cluster branches off in two directions. To the left, it links to a small cluster on information systems and security (in yellow) which correlates to the large red cluster that includes much of the government related terms such as Department of Homeland Security, US Government, Policy, Legislation, Strategy etc., as well as some of the more general CIPR terms such as vulnerability, attack, threat and terrorism. Interestingly, the term Cyberterrorism is clustered in the red group as opposed to the purple. This has likely occurred because 25% (14/55) of the Cyberterrorism publications are policy related documents from the US Congressional Research Service – thus clustering with the US Government and Policy. Also noteworthy is that Information exchange is clustered in the red group as well. Again, 20% (11/54) of the Information exchange publications are US Congressional Research Service policy related publications. Information exchange may also be showing up with the government cluster because information sharing (and exchange) is a key component of most of the reviewed nations’ CIPR strategies. The red government cluster links to the blue cluster that captures three key terms in the field: Response, Preparedness and Recovery. The blue cluster then links to the orange which is focused on water issues and public health. Moving upwards from the purple ICT/Cyber cluster are two more clusters in shades of green that relate to the Smart grid and Energy and Utilities. The correlation between ICT and Energy and Utilities is also seen in Figure 7.

Other major clusters in the Top 300 map are presented in figure 4. In this figure we see a peach cluster on the upper right that links Decision making/support with Artificial intelligence. At the centre of the graphic is a standalone green cluster that focuses on Sensors, Network security, Cryptography and Authentication. Below is a purple cluster related to risk management that is linked to a cluster of blue nodes on Disasters.
Figure 4. Top 300 Terms Cluster Map – Additional Clusters
5.2 Top Subjects

To gain a higher level view of the dataset and to enable analysis according to concepts of key interest, the data was classified into 60 subject groups that represent 97% of the entire dataset. Many of the major clusters presented appear as groups in figure 5 which lists the top 32 subject groups (200 or more publications). It includes several CI sectors (ICT, Energy and Utilities, Transportation, Safety, water, Health care, Government, Finance), some of the mitigation strategies discussed in the literature (e.g. Modeling & simulation, Risk assessment, Decision making/support, Policy & directives, Engineering, Monitoring & warning etc.), as well as some of the more general topics in the domain (e.g. Disaster/accident/emergency, Vulnerability, Terrorism, Threat, Interdependencies etc.).

Figure 5. Top 32 Subject Groups – with 200+ records
Interesting insights can be seen when these top 32 subject groups are compared between the early (2003-2008) and the later (2009-2013) time periods. Figure 6 documents the percentage share of each group in the early and late time periods. We see in Figure 6 that many of the subject groups have roughly the same number of publications in both time periods. Some of the sectors continue to be relatively stable (no more than a 2% change) such as ICT, Water, Health care, Finance and Government sectors, whereas Energy and Utilities, Transportation and Safety sectors show a slight rise in 2009-2013. Other subjects that increase in the later period include Modeling & simulation, Natural disasters, Cyber-attack, Network security, and SCADA. This reflects an increased interest in Cyber issues and a growing recognition that natural disasters are the most frequent threat to CI. On the other hand we see a drop in Policy & directives and Terrorism. The drop in terrorism may be the counterpoint to the increased focus on natural disasters.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modeling &amp; simulation</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>ICT sector</td>
<td>26</td>
<td>26</td>
</tr>
<tr>
<td>Energy &amp; utilities sector</td>
<td>17</td>
<td>21</td>
</tr>
<tr>
<td>Transportation sector</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Safety sector</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>Cyber security</td>
<td>13</td>
<td>11</td>
</tr>
<tr>
<td>Natural disaster</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Disaster/accident/emergency</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>Engineering</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Risk assessments</td>
<td>13</td>
<td>9</td>
</tr>
<tr>
<td>Water sector</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Sensors</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Decision making/support</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Monitoring &amp; warning</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Network Security</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Health care sector</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Reliability analysis</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Policy &amp; directives</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Risk management</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>SCADA</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Interdependencies</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Finance sector</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Mitigation/Prevention</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Threat</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Environmental aspects</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Impacts</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Response</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Terrorism</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Government sector</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Laws &amp; legislation &amp; regulation</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>
The complete cluster map for all 60 subject groups (2003-2013) is presented in figure 7. The map shows that there are two main groupings that connect roughly half of all the nodes in the map. Two additional small clusters include a blue cluster on the upper left that correlates Environmental aspects with Impacts and a purple cluster at the bottom which correlates Engineering with Software engineering.

Figure 7. 60 Subject groups cluster map (filter set to 23%)
The largest grouping on the right hand side shows a central cluster in yellow in the middle that contains
the ICT sector and the cyber related groups (cyber-attack, cyber security, SCADA). The concepts covered
by the four groups in this yellow cluster were also prevalent in the list of top 24 terms in Figure 2. This
cluster correlates with Network Security and related issues, as well as Sensors and Monitoring &
warning. We also see the Energy and Utilities sector is closely correlated with the ICT sector roughly 45%
(398/868) of Energy and Utilities sector publications also discuss the ICT sector and 34% (398/1156) of
ICT sector publications discuss Energy and Utilities. This draws attention to interdependencies between
these two sectors\textsuperscript{14,15} including the use of advanced computing and communication technologies such as
smart grids\textsuperscript{16} and Supervisory Control and Data Acquisition (SCADA) systems for improved protection\textsuperscript{17,18}
in the Energy and Utilities sector. We also see that Modeling and simulation is often discussed in
correlation with the Energy and Utilities sector, demonstrating that it is often the interdependencies
between CI that are being modeled in the field.

On the left is a smaller ‘emergency management’ cluster that includes three of the four core elements of
Canada’s Emergency Management Framework:\textsuperscript{19} Mitigation/Prevention, Recovery and Response
(Preparedness is on the map but not correlated with this cluster). Unsurprisingly, these groups are found
clustered with various types of Disasters and the Safety sector, since the latter responds to and prepares
for disasters, often through Risk assessments and Risk management activities.

5.3 Emerging Trends

In order to identify emerging research trends in the field of CIPR, an R&D momentum analysis was
conducted. Further explanation of the methodology behind the momentum indicator is included in
section 9.2, but essentially it plots the standard deviation of standardized measures of publication
counts and velocity (the rate of publication increase) on two axes. Nodes to the left of the Y-axis have
below-average velocity, and those found below the X-axis have relatively smaller publication counts. A
third dimension is added by sizing nodes relative to the total number of underlying publications. Even a
small node in the right/lower quadrant may be of interest, since emerging topics (in lower right
quadrant) are typically small in numbers as they begin to attract research attention and increase in
velocity.

For the purposes of this analysis, the 60 subject groups were organized into four thematic groups as
depicted in Table 3. These groups were made based on clusters in the dataset and reviews of the
literature and were finalized with the client. The General CIPR Topics thematic group includes some of
the major topics in the field such as Threats, Disasters, the four core elements of emergency
management: Mitigation/Prevention, Preparedness, Response, Recovery as well as Impacts,
Interdependencies, Cyber-attack and so on. The CI sector includes Canada’s 10 CI sectors\textsuperscript{6} and Coastal &
waterways which was added because it frequently discussed in the literature as a relevant
infrastructure type even though it is not a recognized sector. The two mitigation thematic groups gather
together various activities that represent either physical countermeasures such as Construction,
Intrusion detection, and Structural health monitoring or non-physical countermeasures, which are less
tangible and/or less physical in nature and are more focused on the theoretical side of understanding
and developing strategies for increasing CIPR such as Risk assessment, Education and Policy & directives.
These thematic groups are not mutually exclusive in that Adaptation and Sustainability both fall into the
General CIPR Topics and the Mitigation: Non-physical countermeasures thematic groups. In terms of
mitigation activities, adapting to threats and incorporating concepts of sustainability into daily life can

\textsuperscript{6} Please see section 9.3 for details on how the CI sectors groups were created.
improve resilience. On the other hand, both terms are large concepts closely tied to climate change which is a recognized threat to CI, thus they have been included in the General thematic group as well.

### Table 3.4 Thematic Groups of 60 subject groups

<table>
<thead>
<tr>
<th>Thematic Group</th>
<th>Subject Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>General CIPR Topics</td>
<td></td>
</tr>
<tr>
<td>Adaptation</td>
<td>Natural disaster</td>
</tr>
<tr>
<td>Cascading effects</td>
<td>Preparedness</td>
</tr>
<tr>
<td>Climate change</td>
<td>Probability</td>
</tr>
<tr>
<td>Cyber-attack</td>
<td>Recovery</td>
</tr>
<tr>
<td>Disaster/accident/ emergency</td>
<td>Resilience</td>
</tr>
<tr>
<td>Environmental aspects</td>
<td>Response</td>
</tr>
<tr>
<td>Hazard</td>
<td>Sustainability</td>
</tr>
<tr>
<td>Impacts</td>
<td>Terrorism</td>
</tr>
<tr>
<td>Interdependencies</td>
<td>Threat</td>
</tr>
<tr>
<td>Mitigation/Prevention</td>
<td>Vulnerability</td>
</tr>
<tr>
<td>CI Sectors</td>
<td></td>
</tr>
<tr>
<td><em>Energy and Utilities</em></td>
<td>Manufacturing</td>
</tr>
<tr>
<td>Finance</td>
<td>Safety</td>
</tr>
<tr>
<td>Food / Agriculture</td>
<td>Transportation</td>
</tr>
<tr>
<td>Gov’t</td>
<td>Water</td>
</tr>
<tr>
<td>Health care</td>
<td>Coastal &amp; waterways</td>
</tr>
<tr>
<td>ICT</td>
<td></td>
</tr>
<tr>
<td>Mitigation - Physical</td>
<td></td>
</tr>
<tr>
<td>countermeasures</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Monitoring &amp; warning</td>
</tr>
<tr>
<td>Construction</td>
<td>Reliability analysis</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Sensors</td>
</tr>
<tr>
<td>Cyber security</td>
<td>Software engineering</td>
</tr>
<tr>
<td>Detection</td>
<td>Structural aspects</td>
</tr>
<tr>
<td>Engineering</td>
<td>Structural health monitoring</td>
</tr>
<tr>
<td>Fault tolerance &amp; detection</td>
<td>Visualization</td>
</tr>
<tr>
<td>Forecasting &amp; prediction</td>
<td></td>
</tr>
<tr>
<td>Intrusion detection</td>
<td></td>
</tr>
<tr>
<td>Mitigation – Non-physical</td>
<td></td>
</tr>
<tr>
<td>countermeasures</td>
<td></td>
</tr>
<tr>
<td>Adaptation</td>
<td>Modeling &amp; simulation</td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>Ontology/semantics</td>
</tr>
<tr>
<td>Decision making/ support</td>
<td>Policy &amp; directives</td>
</tr>
<tr>
<td>Education</td>
<td>Risk assessments</td>
</tr>
<tr>
<td>Forecasting &amp; prediction</td>
<td>Risk management</td>
</tr>
<tr>
<td>Knowledge management</td>
<td>Sustainability</td>
</tr>
<tr>
<td>Laws/legislation/regulation</td>
<td></td>
</tr>
</tbody>
</table>
5.3.1 General CIPR Topics

The General CIPR Topics thematic group is the largest in our dataset, comprising 20 subject groups that range from *Natural disasters* (292 publications between 2008-2013) to *Preparedness* (29 publications). Figure 8 shows the recent trends and shifts in focus in the field of CI protection and resilience in the past 6 years. Some interesting observations that can be made from this map include:

- *Natural disasters* (red, 1\textsuperscript{st} quadrant) is increasingly being discussed more than general disasters, likely due to an increasing recognition that the most frequently occurring threat to CI is natural, weather-related disasters.

- Similarly, *Terrorism* (blue, 3\textsuperscript{rd} quadrant) has quite a low rate of acceleration, because although more frightful, terrorist attacks are significantly less frequent than natural disasters.

- *Cyber-attack* (pink, upper right quadrant) is a hot topic in the literature today and a lot of research in the dataset is focused on cyber related issues.

- *Mitigation/Prevention, Resilience, Climate change and Sustainability* are all rising in the emerging topics quadrant. Recent research is shifting from a focus on *Preparedness* (blue, lower left, very few records in recent years) and *Recovery* (blue, bottom of Y-axis), to *Mitigation/Prevention* as part of an effort to reduce the impacts of disasters. *Resilience* is a popular theme in the field and, as recognition grows that it is impossible to prevent all disasters, there is an increased focus on developing resilience to disasters. With the increased recognition that natural disasters are the greatest threat, there is likewise increasing recognition that disaster mitigation efforts need to take climate change into account, often through sustainability practices.

- While *Interdependencies* (red, 2\textsuperscript{nd} quadrant) is a well-established topic in the field, we are seeing an increased use of the term *cascading effects* to discuss interdependencies in recent years.
Figure 8. General CIPR Topics, 2008-2013: Recent Trends
5.3.2 CI Sectors

The CI sectors map (Figure 9) contains the 10 Canadian CI sectors as well as Coastal & waterways. There are very few surprises on this map in that ICT, Energy and Utilities, Transportation and Safety are the most established sectors in the scientific literature. Healthcare, Finance, Government, Food/Agriculture and Manufacturing are all less frequently discussed in the scientific literature. That being said, we are seeing a slow but steady rise in the Healthcare sector (210 publications) as it increased from 27 publications in 2008 to 53 publications in 2012. The Water sector, which has 259 publications between 2008 and 2013, has also been on the rise, growing from 18 publications in 2008 to 66 in 2012. Most interesting in this map is the emergence of the Coastal & waterways group. Although this is not a recognized sector, there is a notable acceleration in research on coastal regions and waterway infrastructure. Although there are only 175 publications in the entire dataset (2003-2013), the subject went from roughly 4 publications per year (2004-2008) to 16 publications in 2009 to 31 in 2012. This group is comprised of such topics as coastal zones, rivers, seas, marine transportation, maritime security, sea level change, ports etc. While there are some overlaps with other sectors (in particular, transportation and water – rivers are a source of drinking water), there are numerous issues (such as flooding of waterways,\textsuperscript{20,21} impacts to major cities due to sea level change,\textsuperscript{22,23} mitigation of natural disaster impacts by shoring up coastal zones\textsuperscript{20,24}) that are increasingly making this an area worth considering on its own.

![Figure 9. CI Sectors, 2008-2013: R&D Momentum](image-url)
5.3.3 Mitigation: Physical Countermeasure

The Mitigation: Physical countermeasures thematic group covers a variety of subject areas that can be viewed as concrete activities that can help reduce the impacts of disasters, ranging from Detection of threats to Engineering and Construction which improves resilience. The thematic group also covers Cyber security and Network security and related activities/subject groups such as Authentication and Cryptography.

Figure 10 shows that the most frequently discussed physical mitigation countermeasures (all on the top half of the chart) include Cyber security (347 publications, 2008-2013), Engineering (282), Sensors (237), Monitoring & warning (228; including monitoring systems and early warning systems), Network security (203) and Reliability analysis (193; assessing the ability of a system to perform its intended function and is often focused on the cyber components of CI). None of these except Monitoring & warning show a particularly high rate of acceleration. Monitoring & warning, which has grown from under 20 publications in 2008 to over 50 in 2012, may be accelerating as a result of the growing recognition that early warning of impending natural disaster, particularly earthquakes and tsunamis, can have a significant effect in disaster risk reduction and consequently reduce the impacts on CI.

Emergence and acceleration are notable for Detection (147), Intrusion detection (67) and Structural aspects (92). Detection appears to be a topic of increasing interest, growing from 9 records in 2008 to over 30 in each year between 2010 and 2012. This subject group covers a range of detection issues including, but not limited to, anomaly detection in digital control systems used by electric power infrastructure and water management systems in a way that is complementary to intrusion detection, damage detection through the Load Loss Damage Index or HEC-FIA (a standalone, GIS-enabled tool for estimating flood related economic damages); attack detection, often in relation to denial-of-service attacks as well as various other detection algorithms, approaches and techniques.

Intrusion detection is a subset of detection that has a significantly higher publication count than any other detection topic and was thus turned into its own subject group in order to investigate further. While the subject does not have many publications on its own, it has gone from 5 publications in 2008 to 18 in 2012. This subject focuses mainly on the monitoring of networks and computers for signs of intrusion and can be used in many critical infrastructure. Intrusion detection is frequently seen discussed with SCADA (Supervisory Control and Data Acquisition) systems, which collect and analyse data from, and control equipment related to, many critical infrastructure systems such as electricity, gas, water, and transportation.

Structural aspects is a larger subject group that includes structural health monitoring (SHM), structural design to improve resilience, structural vulnerability analysis of large scale distrusted systems and the use of robustness evaluation to prioritize the spending of mitigation resources on structural improvement programs for critical infrastructure, amongst other topics. The subject grew from single digits each year prior to 2009 to publications tallying in the low 20s from 2010-2012. SHM represents a notable number of publications in 2010 and 2011 (eight and six publications respectively). SHM relates to monitoring the physical strength and reliability of infrastructure components (e.g. bridges, pipes, tunnels, buildings, railways, etc.) often through wireless sensor networks (WSN) and often in relation to seismic activity. Some articles explore SHM from a more theoretical perspective such as the role of SHM...

---

1 Structural health monitoring was also created as a separate subject group to determine if there was any upward trending. However, except for a jump in publications from 2010-2011 there has not been a significant number of articles for this group.
in data collection for asset management. Others present actual tools such as GENESI, which is a structural health monitoring system for critical infrastructure that uses WSN based monitoring or more generally discuss the challenges associated with using WSNs to monitor the structure health of critical infrastructure.

Figure 10. Mitigation: Physical countermeasures, 2008-2013: R&D Momentum
5.3.4 Mitigation: Non-physical countermeasures

The Mitigation: Non-physical countermeasures research momentum map brings together those mitigation activities that are less tangible and/or less physical in nature and are more focused on the theoretical side of understanding and developing strategies for increasing CIPR. The map covers a variety of topics ranging from Modeling & simulation (892 publications, 2008-2013) to Artificial Intelligence (59 publications).

Modeling & simulation (blue, top) is by far the largest subject in this map and the dataset, yet its rate of acceleration is not particularly high, reflecting that it is a fairly established topic in the field. Many of the other subject groups such as Risk assessment, Risk management, Policy & directives, and Decision making/support (all in the upper left quadrant of Figure 11) have also been fairly steady over the past six years, demonstrating stable research interest in these topics.

The subjects with the greatest momentum are found in the lower right quadrant. These include Artificial Intelligence (59), Sustainability (89) and Ontology/semantics (52). As was seen above in Figure 4, Artificial Intelligence is often discussed in conjunction with Decision making/Support topics. Artificial Intelligence is also discussed in terms of a risk-aware robotic sensor network for CI protection, learning and detection algorithms that can be used in CI monitoring software, AI tools that are used for improving awareness and monitoring of seismic events and the use of AI techniques in event modeling that responds dynamically to user inputs to train crisis managers to name a few.

Sustainability is considered as a component of infrastructure design and urban planning. It can contribute to the survivability of critical infrastructure in the event of disasters in the dataset. In one article, it is discussed as being an outcome of CIPR akin to resilience in that conducting sustainability assessments of critical infrastructure in the face of extreme weather events can increase both resilience and sustainability of the built environment. Another article discusses how systemic robustness, resilience and sustainability can be engineered into interdependent critical infrastructure and can improve resistance to disruptive events. A number of other articles discuss increasing sustainability practices in various CI sectors, such as Food/Agriculture and Water, through the use of adaptive management frameworks which combine predictive modeling and process-based ecosystem management.

Ontology/semantics is a rather small group that relates to modeling and simulation through graphing and is used as the basis of various models. Semantic graphs have been used to assess risk probability and semantic modeling has been used in EMILI, a EU Seventh Framework Programme for Research (FP7) project which deploys innovative information technology for emergency management in large complex CI. Ontologies have been used as a conceptual model to communicate, analyze and simulate CI interdependencies and as the ontological formalism behind a knowledge based system used for federated simulation of CI dependencies. Both ontological and semantic models have also been used together in event detection decision support systems.
Figure 11. Mitigation: Non-physical countermeasures, 2008-2013: R&D Momentum
5.4 Key Players

A breakdown of the top 10 publishing countries is presented in Figure 12. Unsurprisingly, of the majority of publications produced by the top 10, 41% originate in the United States (1,505/3,635). The US is followed by Italy (312) with the UK (269) in third place and Canada ranks 5th with 193 publications. This top 10 list covers 79% of all country affiliations available in the dataset.

Figure 12. Top 10 Publishing Countries

Figure 13 presents the top affiliations with 30 or more publications. One may notice the dominance of US affiliations. The list is dominated by academic institutions (8) followed by four government affiliations and two US national laboratories. Many of the US government related publications are not descriptions of S&T research but government reports and their updates. Overall, the list reflects that much of the S&T research in the broader field of CIPR is still occurring in academic settings. These top affiliations represent 15% of all publications in the dataset.

---

g 3,635 (78% of all dataset) is the total number of records that had a country affiliation associated with it, i.e. only 78% of the dataset had a country affiliation.
Figure 13 presents the top Canadian affiliations with three or more publications and represents 75% of all Canadian publications in the dataset. The University of British Columbia (UBC) tops the list with 24 publications, more than doubling the next highest publishing affiliations in Canada: the University of Western Ontario (UWO, 12), University of Ottawa (12) and DRDC (12). UBC’s publication rate has been fairly stable since 2006 with at least two publications per year and five publications in 2010. The subjects of the UBC publications range from exploring earthquake related transportation disruption, to real time monitoring of energy infrastructure, to modeling CI interdependencies in the I2Sim simulator framework. The majority of UBC’s publications are emanating from the departments of Electrical and Computer Engineering as well as Civil Engineering. University of Ottawa’s publications mainly come from the School of Information Technology and Engineering and cover wireless sensor networks and robotics to name a few subjects. DRDC’s publications are all from Ottawa, with six specifically from the Centre for Security Science, including a literature search on CI in support of Emergency Management BC (EMBC) that was conducted in 2012 and contains roughly 200 references. UWO’s publications are also from the departments of Civil and Environmental Engineering and Electrical and Computer Engineering. Their topics show a large range including four that discuss modeling and/or simulation such as building ontologies for CI interdependency simulators to support collaboration and information exchange, to assessing climate change risk to local infrastructure, to engineering procedures for conducting flood risk assessments. Also of interest here is Dalhousie University, which has a Critical Infrastructure Protection Initiative with a number of potentially interesting research projects including risk governance, cyber security and CI from comparative perspectives. Similarly, École Polytechnique de Montréal has four publications, all of which relate to critical infrastructure interdependencies, with one publication from 2008 that is specifically on modeling. A more detailed profile of these Canadian affiliations is provided in section 9.4.
5.5 Metrics and Surveys

While a specific search on metrics and surveys was not conducted for this study, the general CIPR search did retrieve 56 publications that discussed metrics, measurement or indices and 82 that mentioned surveys. Of the 56 metrics publications, 16 were found to be specifically focused on metrics for protection or resilience of critical infrastructure. Table 4 provides a breakdown of the 56 records that were found to discuss specific metrics or measurements or indices related to the field of CIPR. It is important to note that the categories are not mutually exclusive in that a publication may discuss resilience as well as survivability.

<table>
<thead>
<tr>
<th>Metrics for</th>
<th>Number of publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection/security of CI</td>
<td>9</td>
</tr>
<tr>
<td>Resilience of CI</td>
<td>7</td>
</tr>
<tr>
<td>Survivability</td>
<td>4</td>
</tr>
<tr>
<td>Interdependency of CI</td>
<td>6</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>16</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>17</td>
</tr>
<tr>
<td>Reliability assessment</td>
<td>4</td>
</tr>
<tr>
<td>Soft/qualitative assessment</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4. Metrics Related to CIPR
Publications discussing Metrics in the Protection/security of CI group tend to discuss the concept of CI security more frequently than protection of CI. Some of the security metrics are related to SCADA systems either in terms of information security metrics or Process Control System security in mass transportation. A 2010 article by Adams, Hester and Mahadevan, surveyed potential metrics for effective security systems for critical facilities and made recommendations for selecting metrics and evaluating system effectiveness. Finally, the RESCI-MONITOR tool, which is a multi-agent CI security modelling tool for monitoring CI services and their associated dependencies in real-time is also discussed.

In the Resilience of CI subgroup we find multiple publications from the US Department of Homeland Security (DHS) that discuss the development of a framework for evaluating the resilience of infrastructure and economic systems. This framework was developed from the DHS’s Science and Technology Directorate and Sandia National Laboratories and includes both quantitative and qualitative measures. More information on the framework can be found on Sandia’s CASoS Engineering website. DHS, in collaboration with Argonne National Laboratory, have also developed a community resilience assessment tool that combines measures of CI and organizational resilience with new metrics to evaluate community resilience according to five subsystems including economy, physical infrastructure, government and non-governmental organizations, emergency services and the civilian population. DHS and Argonne National Laboratory have also produced a Resilience Index, a Vulnerability Index, and a Criticality Index. In a non-DHS article, author Timashev presents a generalized quantitative definition of resilience and preparedness as a function of time.

Survivability refers to the ability of CI to handle (and survive) an attack or disaster and new models are being developed to extend beyond simple performance metrics to take into account interdependencies through a probabilistic model. Another survivability metric discussed in the dataset is the Survivable Systems Analysis method.

In terms of Interdependencies, some effort is made to quantify the impact of interdependencies in various sectors during specific events while others focus on the reliability or vulnerability of interdependent infrastructure networks during disasters. Another report describes the findings of the EU Project Methodology for Interdependencies Assessment, which applied metrics to interdependencies in ICT and Energy sectors. The RESCI-MONITOR tool, described above, is also found in this subject group.

In regards to surveys, 82 publications mentioned the word survey but the majority were discussing surveys in terms of a review of a large body of literature. Six surveys that involved questionnaires, interviews and the like were found in the dataset. These surveys include studies that focused on:

1. Understanding enablers and barriers to collaboration among infrastructure owners during disasters.
2. Understanding what water utilities are considering for security system improvement.
3. Comparing a U.S. national water utility’s security measures to facilities in U.S. and Canada to assess facilities, identify improvement areas, and estimate effects of new protective measures.

It should be noted that there is an ISO standard for information security, namely, ISO/IEC 27001 Information Security Management System (ISMS).
4. Assessing public utilities’ leaders’ understanding of the interdependencies in their environment as part of a complex adaptive system and gauging the implications for operations; as well as developing a framework to assess where utilities are today in terms of increasing the resilience of their organizations.\textsuperscript{89}

5. A Laboratory Directed Research Development (LDRD) project that investigated the development of quantitative CI resilience through the application of control design methods.\textsuperscript{90}

6. A Ciena-commissioned survey of 400 senior IT decision makers in Europe regarding increases in security threats.\textsuperscript{91}

Additional focused searches on both CIPR metrics and surveys would likely identify further sources.

## 6 NATIONAL CIPR STRATEGIES

A web search for international strategies, policies, plans and frameworks related to CIPR was conducted for the following nations: Canada, United States, United Kingdom, Australia, European Union, New Zealand, Denmark, Norway and Iceland. Ninety-three publications were identified. While the majority of the publications relate directly to CIPR, some are focused on related fields of emergency management, disaster mitigation, risk assessment and the like, particularly for Canada. Table 5 lists the number of publications found for each of the nations included in the scope of this project.

<table>
<thead>
<tr>
<th>Countries</th>
<th>Number of publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>18</td>
</tr>
<tr>
<td>United States</td>
<td>10</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>15</td>
</tr>
<tr>
<td>Australia</td>
<td>11</td>
</tr>
<tr>
<td>European Union</td>
<td>26</td>
</tr>
<tr>
<td>New Zealand</td>
<td>5</td>
</tr>
<tr>
<td>Norway</td>
<td>2</td>
</tr>
<tr>
<td>Denmark</td>
<td>2</td>
</tr>
<tr>
<td>Iceland</td>
<td>4</td>
</tr>
</tbody>
</table>

### 6.1 Overview of National Strategies

A high level overview and comparison of the CIPR national strategies and cyber security strategies for Canada, US, UK and Australia is presented below. This section focuses on the documents listed in Table 6.
6.1.1 Canadian National Strategy & Action Plan

Canada’s National Strategy for Critical Infrastructure\(^1\) (NSCI) is a 12 page document that was published in 2009. The NSCI builds on the concepts and principles of the Emergency Management Framework for Canada\(^1\) which views the resiliency of critical infrastructure as being achievable through security measures, business continuity practices and emergency management planning. The stated goal of the NSCI is “to build a safer, more secure and more resilient Canada”.\(^1\)

The NSCI establishes a framework for cooperation between all levels of government and amongst the operators and owners of CI and fosters partnerships through sector networks for enhanced information sharing and protection and the identification of a preferred risk management approach.

The NSCI is focused on three key activities, each with its own objectives.

1- Building partnerships - Build partnerships to support and enhance critical infrastructure resiliency. This includes the development of sector networks and the National Cross-Sector Forum which include private sector and government members of all levels (federal, provincial, territorial (FPT)).

2- Implement all-hazards risk management approach - In the context of the NSCI, risk management refers to “the continuous, proactive and systematic process to understand, manage and communicate risks, threats, vulnerabilities and interdependencies across the critical infrastructure community”. The all-hazards risk analysis is to be conducted in collaboration with government and private partners, where owners/operators will ultimately be responsible for implementing risk management and government will support by sharing tools, knowledge and coordinating regional exercises.

3- Sharing and protecting information - Advance the timely sharing and protection of information among partners and key stakeholders. Government will support the

---

Table 6. List of National Strategy Documents used for Comparison between Nations.

<table>
<thead>
<tr>
<th>Countries</th>
<th>Documents used for comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>• National Strategy for Critical Infrastructure(^1)</td>
</tr>
<tr>
<td></td>
<td>• Action Plan for Critical Infrastructure (2009)(^2)</td>
</tr>
<tr>
<td></td>
<td>• Canada’s Cyber Security Strategy(^3)</td>
</tr>
<tr>
<td></td>
<td>• Action Plan 2010-2015 for Canada’s Cyber Security Strategy(^4)</td>
</tr>
<tr>
<td>US</td>
<td>• NIPP 2013: Partnering for Critical Infrastructure Security and Resilience(^9)</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>• Keeping the Country Running: Natural Hazards and Infrastructure(^5)</td>
</tr>
<tr>
<td></td>
<td>• The UK Cyber Security Strategy(^6)</td>
</tr>
<tr>
<td>Australia</td>
<td>• Critical Infrastructure Resilience Strategy(^4)</td>
</tr>
<tr>
<td></td>
<td>• Cyber Security Strategy(^6)</td>
</tr>
</tbody>
</table>
improvement of information sharing and protection through the provision of a wider range of information products (e.g. risk assessments, incident reports, lessons learned), web-based delivery of information products, improved protection from unauthorized disclosure of shared information and an expanded production of all-hazards risk information products.

The NSCI is scheduled to be reviewed three years after launch and every five years thereafter. According to the 2009 Canadian Action Plan for Critical Infrastructure, progress on the NSCI will be measured on strengthened resiliency of critical infrastructure in Canada; a better understanding of the risks to critical infrastructure; and swift and effective response and recovery when disruptions occur.

The 2009 Action Plan for Critical Infrastructure (APCI) builds on the three central themes of the NSCI and the updated 2014 action plan. The 2009 APCI sets out timelines for accomplishing some of the activities described in the NSCI, stating that years one and two will focus on development of sector networks and the National Cross-Sector Forum, as well as improved information sharing. It is envisioned that subsequent years will see the sector networks and information sharing supporting further risk management activities, emergency management planning and exercises. The APCI ’09 also describes roles and responsibilities for the various government levels and the CI owners/operators in regards to CIPR and states that the renewal of the Federal-Provincial-Territorial Critical Infrastructure Working Group will be an integral part of the plan.

The APCI ’09 elaborates on the function of the sector networks, such as the development of sector risk profiles, supporting the development of tools and best practices, advancing the implementation of the NSCI, and addressing international CI issues. The key action for the development of sector networks is as follows:

Sector networks will be established for each of the critical infrastructure sectors. Members of the sector network (e.g., private sector, federal government, provincial and territorial governments) will set priorities and direct sector-specific work plans. Development of the sector networks will build on existing consultation mechanisms.

The National Cross-Sector Forum will be established to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors. Membership comes from the chairs of each sector network.

Year two will include the development of an information sharing framework to accelerate sharing, improve quality of information, and better protect CI information. The framework will include the following elements:

- identification of existing processes for sharing and protecting critical infrastructure information;
- a plan to address gaps and anticipate new pressures and requirements;
- identification of key points of contact to improve government-to-government and government-to-sector communications;
- enhanced process for disseminating information; and
- addressing legal and policy barriers to sharing information.
Year two and beyond will also see the implementation of the all-hazards risk management approach which will involve the sector networks development of risk profiles at the national level, risk assessments and risk management tools and guidance. The risk profiles will help sectors networks in identifying priority areas for further planning, research, and development of plans.

Year three and beyond will see the development of sector-specific work plans which will be shared among FPT governments and owners/operators to address risks. Tools that are developed by the designated federal sector-specific departments/agencies will be available to help sector networks identify critical assets, assess risk and develop measures to address the risks.

On an ongoing basis the FPT governments will also conduct national exercises in collaboration with the private sector to support a common approach to enhancing the resilience of CI.

Additional details on many of the key actions are provided in appendices to the APCI. The APCI was scheduled to be reviewed, in collaboration with the sector networks, the National Cross-Sector Forum and the FPT Critical Infrastructure Working Group, three years after launch and every five years thereafter.

Annex D of the 2014 APCI provides a summary of progress achieved against the 2009 APCI goals. Annex E provides a summary of the updated action items, as aligned to the three core objectives of the NSCI, for the years 2014-2017. These include:

1. Sustain and Enhance Partnerships
   - Develop a call to action for critical infrastructure resilience
   - Provide guidance to ensure appropriate representation on sector networks
   - Address cross-sector issues through multi-sector meetings
   - Strengthen public communications and awareness

2. Share and Protect Information
   - Expand stakeholder membership and participation on the Canadian Critical Infrastructure Gateway and leverage the CI Gateway’s capabilities to improve information sharing and collaboration on specific projects
   - Provide impact assessments during unfolding events of national significance
   - Sponsor security clearances among private sector stakeholders in order to enable increased sharing of sensitive information
   - Expand information sharing and investigate rationalization of existing information sharing arrangements

3. Implement an All-Hazards Risk Management Approach
   - Implement the Regional Resilience Assessment Program (RRAP) across Canada
   - Develop targeted risk assessment products in response to emerging critical infrastructure issues
   - Provide an overall description of key risks for critical infrastructure, including dependencies and emerging trends
   - Assess impacts of potential high impact / low frequency events on critical infrastructure sectors to increase awareness and understanding of risks to critical infrastructure
• Develop standards to improve critical infrastructure resilience and encourage their adoption
• Conduct exercises to strengthen readiness and response efforts
• Finalize national application of an interdependencies model
• Measure progress toward resilience to demonstrate results and monitor progress

6.1.2 US National Strategy

The 2013 US National Infrastructure Protection Plan (NIPP)\textsuperscript{9} is the main document that encompasses both the US National Strategy and Action Plan for Critical Infrastructure Protection and is the 3rd edition of the Strategy. The first NIPP was developed in response to the Homeland Security Presidential Directive 7 issued by President George W. Bush in 2003. This latest update is a response to the 2013 Presidential Policy Directive 21 Critical Infrastructure Security and Resilience (CISR) which called for the integration of both cyber and physical security into an enterprise approach to risk management and aligns with the National Preparedness System called for in Presidential Policy Directive & National Preparedness, by managing risk across the five national preparedness mission areas of prevention, protection, mitigation, response and recovery.

The 2013 version of the NIPP places security and resilience of CI as the primary aim of CI homeland security efforts; updates the CI risk management framework; establishes a process to set CI national priorities jointly with public and private sector; affirms that CISR requires an international effort; focuses on leveraging regional collaborative efforts and presents a detailed Call to Action with steps that will be shaped by each sector’s priorities and in collaboration with CI partners to make progress towards security and resilience.

The goals of the NIPP are as follows:

- Assess and analyze threats to, vulnerabilities of, and consequences to CI to inform risk management activities;
- Securing CI against, human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance CI resilience by minimizing the adverse consequence of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
- Share actionable and relevant information across the CI community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

The core tenets of the NIPP are as follows:

1. Risk should be identified and managed in a coordinated and comprehensive way across the CI community to enable the effective allocation of security and resilience resources;
2. Understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing CISR;
3. Gaining knowledge of infrastructure risk and interdependencies requires information sharing across the CI community;
4. The partnership approach to CISR recognizes the unique perspectives and comparative advantages of the diverse CI community;

5. Regional and SLTT\textsuperscript{1} partnerships are crucial to developing shared perspectives on gaps and actions to improve CISR;

6. Infrastructure critical to the US transcends national boundaries, requiring cross-border collaboration, mutual assistance, and other cooperative agreements; and

7. Security and resilience should be considered during the design of assets, systems and networks.

The \textit{Call to Action} guides the CI community to improve security and resilience through the three goals of building upon partnership efforts; innovating in managing risk; and focusing on outcomes. These three goals are further broken down into 12 activities in the \textit{NIPP}. This \textit{Call to Action} also provides strategic direction on security and resilience through coordinated and flexible implementation by Federal departments and agencies. The \textit{NIPP} also provides a framework for evaluation of progress through its setting of specific goals, priorities, and associated outputs and outcomes.

\textit{NIPP} 2013 focuses on partnerships between public and private CI owners and operators. The value proposition for government is coordination of infrastructure stakeholders’ security activities and the private sector gains a more thorough understanding of their risk landscape, access to timely and actionable information during disasters, and involvement in helping government makes better decisions on security and resilience initiatives. The \textit{NIPP}’s focus on partnerships also helps establish a set of mutual goals and national priorities, common structures and mechanisms that facilitate information sharing and collaborative problem solving.

The \textit{NIPP} identifies 16 CI sectors, each of which has a Sector-Specific Agency, i.e. a Federal department or agency, which acts as the lead coordinator for the sector with established roles and responsibilities. Likewise all the sectors have a Government Coordinating Councils, many of which have a Sector Coordinating Councils and all are members of the Regional Consortia. These three bodies form the CI Partnership Advisory Council. Each sector has its own publicly available sector-specific plan which details how it is implementing the \textit{NIPP}.

The risk management framework in the \textit{NIPP} provides various levels of guidance on the five phases including: Set goals and objectives; Identify infrastructure; Assess and analyze risks; Implement risk management activities; Measure effectiveness. Related activities in the \textit{Call to Action} are described for each phase.

### 6.1.3 UK National Strategy

The United Kingdom published its first National CI Strategy called \textit{Keeping the Country Running: Natural Hazards \& Infrastructure (KCR)}\textsuperscript{5} in 2011. The first noteworthy difference about the UK Strategy is found in the title which explicitly indentifies the focus on natural hazards, seemingly excluding cyber and man-made threats. Terrorism, cyber threats, military crises and natural disasters are covered in the 2010 UK \textit{National Security Strategy}\textsuperscript{97} but the 2010 Strategy deals with many issues beyond critical infrastructure and as such the former was chosen for review here. The \textit{KCR} views the management of risk as not being

\textsuperscript{1} SLTT = State, Local, Tribal and Territorial.
unique to each sector thereby requiring a tripartite arrangement between infrastructure owners, regulators and government to optimize security and resilience.

The KCR is the guiding document of the UK’s Infrastructure Resilience Programme led by the Civil Contingencies Secretariat and has two main sections that discuss building resilience and provides practical guidance on the principles of infrastructure resilience.\(^1\) The building resilience section focuses on six steps including:

1. identifying risks (natural hazards);
2. assessing risks (standards);
3. building resilience (governance);
4. evaluating resilience (sector resilience plans);
5. sharing information and assessing dependencies; and
6. guidance for regulated sectors.

These steps are based on the UK resilience cycle for infrastructure owners. A notable portion of the assessing risk (standards) section is focused on flood resilience standards as the KCR was developed in response to the 2007 UK floods. The assessing risk section also discusses mutual aid protocols. The building resilience (governance) section includes organizational resilience strategies as well as the British Standard 25999 for Business Continuity Management and Development of a British Standards Institute Publically Available Specification in Crisis Management (PAS 200). Evaluating resilience (sector resilience plans) provides an overview of the plans. Sharing information and assessing dependencies uses the principle of ‘right issue, right time, right level’ in line with the statutory guidance for the Civil Contingencies Act (2004) and emphasizes the need to establish effective relationships between emergency responders and infrastructure owners and operators. Practical advice on assessing dependencies and interdependencies (which are viewed separately) is provided in guide 4 described in the next paragraph. Finally eight considerations for regulators in their role of enhancing resilience are listed along with briefer discussions of financing resilience and engagement of unregulated sectors (e.g. oil, energy generation, satellite communications, and providers of ICT) which do have examples of memorandum of understanding for cooperation during emergencies.

Four guides are provided in the practical guidance section including:

1. Guidance on natural hazards (providing worst case scenario descriptions);
2. Checklist for infrastructure owners (providing self-assessment questions in support of developing organizational resilience);
3. Guidance on information sharing (outlining processes for first and secondary responders to get needed CI information during disasters based on a “right issue, right time, right level” assessment); and

\(^1\) The KCR explicitly states that it does not review the causes of the vulnerability of UK infrastructure to natural hazards but directs readers to the Pitt Review and Institution of Civil Engineers’ State of the National report for this information.
The UK identifies nine Critical National Infrastructure sectors which each have a lead government department sponsoring them. Each sector produces annual Sector Resilience Plans, and summaries of unclassified information therein are publicly available. The full Sector Resilience Plans alert ministers to perceived vulnerabilities and sets out action plans to improve resilience. Four additional critical infrastructure of national significance are also identified and include civil nuclear facilities; hazardous sites; iconic sites; and companies/research organizations that hold information of particular economic or strategic value to the UK. The importance of additional locally significant infrastructure is also noted and it is recommended that these are included in local emergency response planning.

6.1.4 Australian National Strategy

Australia’s updated 2010 Critical Infrastructure Resilience Strategy (CIR) places the onus of managing risk and choosing mitigation strategies on CI owners and operators but recognizes that the Government plays a key role in partnering to share information, raise awareness and facilitate collaboration. A description of the role of relevant Australian Government agencies is provided in an appendix of the CIR.

The objectives of the CIR are two-fold:

- Critical infrastructure owners and operators (including the Australian Government) are effective in managing foreseeable risks to the continuity of their operations, through an intelligence and information led, risk informed approach.
- Critical infrastructure owners and operators enhance their capacity to manage unforeseen or unexpected risk to the continuity of their operations, through an organisational resilience approach.

Implementation of the CIR is accomplished through six strategic imperatives.

1. Operate an effective business-government partnership with critical infrastructure owners and operators - This is accomplished through the Government formed Trusted Information Sharing Network (TISN) which is the primary mechanism for building business-government partnerships. TISN provides national level forums for CI owners/operators to share information and work together with relevant government departments on all hazards. It includes seven Sector Groups, two Expert Advisory Groups, and a Community of Interest for cross-sectoral consultations. Develop and promote an organizational resilience body of knowledge and a common understanding of organizational resilience.

2. Assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies - A key element of this initiative is the Critical Infrastructure Program for Modelling and Analysis (CIPMA) managed by the Attorney Generals Department.

3. Provide timely and high quality policy advice on issues relating to critical infrastructure resilience.

4. Implement the Australian Government’s Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators.

5. Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate.
Specific activities for each of these six strategic imperatives are detailed in the *Critical Infrastructure Resilience Strategy Supplement*.

The *CIR* also describes the National Critical Infrastructure Resilience Committee (NCIRC) which coordinates national CI resilience and protection activities and has the following functions:

- Operate as a forum for national dialogue and collaboration on critical infrastructure resilience;
- Identify, develop, propose and promote initiatives that contribute to the resilience of critical infrastructure in Australia;
- Facilitate information sharing between relevant agencies to contribute to resilient critical infrastructure in Australia;
- Facilitate coordination of work on critical infrastructure resilience being undertaken through the NCTC, NEMC and other relevant bodies and agencies; and
- Identify research needs and facilitate research activity to improve the resilience of critical infrastructure in Australia.

Finally, 11 success factors for the *CIR* are identified, including but not limited to:

- effective engagement between governments and industry on exchange of information and development of solutions;
- developing, promoting and integrating best practices and lessons learned into business practice; and
- owners / operators being integrated into the implementation of the Cyber Security Strategy.

The Strategy is scheduled to undergo a comprehensive review in 2015.

### 6.2 Comparison of National Strategies

From a high level perspective, a number of points can be said about the similarities and differences between these four National Strategies. First, each one recognizes the importance of information sharing, the need for partnerships between all levels of governments and CI owners/operators (and in the case of the UK, first responders and regulators), the importance of learning from past events and each other, the need to assess interdependencies, and that the ultimate responsibility for CIPR lies with the CI owners/operators. Each country also identifies a number of CI sectors and assigns government departments/agencies to lead the coordination of CIPR activities. Another similarity can be seen in the Canadian and US Strategies which are both built on the core themes of prevention, protection or preparedness, mitigation, response and recovery.

The Canadian Strategy document is considerably less specific than the other three nations. While the *Action Plan* does elaborate on key activities that will contribute to the accomplishment of the *National Strategy for Critical Infrastructure’s* main objectives, there are only three main objectives and no goals, principles, priorities, core tenets, etc., as seen in the other National Strategies. This may simply be due to the stage of preparedness Canada had reached in terms of its management of threats to CI, in that this initial Strategy is still focused on the building blocks of preparedness, i.e. building the networks, sharing information and implementing risk management approaches. Based on the review of the 2014 draft/consultation version of the Canadian *Action Plan for Critical Infrastructure*, it appears that progress
is being made on all fronts and that there is a more in depth understanding of and activities related to the All-Hazards Risk Management Approach, including the selection of a specific resilience assessment approach (RRAP).

While the Canadian Strategy does include the word resilience, it is still focused more on protection through risk assessments and risk management, particularly in comparison to the Australian Strategy which is explicitly moving away from protection to resilience. The Australian Strategy indicates that it is aiming for an organic capacity to deal with rapid onset crises and that it is deliberately moving away from a traditional approach of developing plans to deal with a finite set of scenarios. It elaborates that its previous strategy focused on protection in terms of legal requirements, due diligence, risk assessment and management, but that its new strategy focuses on organizational resilience through capacity building, improved adaptability, learning from lessons, increasing knowledge and dealing with complexity. Canada’s focus on protection is also in contrast to the US’s focus on security and resilience. While this appears to be a vocabulary issue, it was quite notable in reading the NIPP that the term protection has been replaced by the term security, much as resilience has replaced protection in Australia.

Based on the updates in the Canadian 2014 Action Plan for Critical Infrastructure, sector specific work plans are in progress, but are not publicly available. This differs greatly from the US approach which makes the Sector-Specific Plans publicly available on the Department of Homeland Security website. The US plans have all been updated at least once already and many are in progress of further updates to align with the 2013 NIPP. This also differs from the UK approach which makes summaries of unclassified information of each sector’s resilience plan available to the public.\footnote{Following a review of the TISN website no Australian sector plans were found, however they may be available elsewhere.}

As discussed above, one notable difference in the UK Strategy is the explicit focus on natural hazards to the exclusion of cyber threats and terrorism (which are covered in the UK National Security Strategy instead). Another notable difference in the UK Strategy is their explicit discussion of partnerships with first responders and the role regulators can play in improving resilience of CI. The UK strategy is the only one that emphasizes building relationships between first responders and CI owners. In addition to this unique partnership being discussed in the strategy, the national authority hosts the London Utility Forum, which brings together senior representatives of the utility companies and first responders three to four times a year in order to share information and plan for emergencies.

Criticism of the Canadian National Strategy and Action Plan revolved around the underdevelopment of the overall plan, failure to take into account (and plan for) many of the challenges in bringing sectors together to share information, the inadequacy of the “all-hazards” risk management approach (which was not designed for CI), the lack of standardization and accountability in risk management which can potentially lead to off-loading risks to other sectors where services are interdependent between sectors, and finally, the lack of reporting mechanisms to outside parties.\footnote{Following a review of the TISN website no Australian sector plans were found, however they may be available elsewhere.
6.3 Cyber Security Strategies

This section provides a very high level outline of the main objectives and goals of the Canadian, UK and Australian cyber security strategies. The US is excluded from this section because the 2013 NIPP explicitly states that it integrates both cyber and physical security into a single strategy.¹

6.3.1 Canadian Cyber Security Strategy

Canada’s 2010 Cyber Security Strategy⁹³ is built on three pillars that include various initiatives.

1. Securing Government systems - the government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.
   a. Establishing clear federal roles and responsibilities
   b. Strengthening the security of Federal cyber systems
   c. Enhancing cyber security awareness throughout Government
2. Partnering to secure vital cyber systems outside the federal Government - In cooperation, the Government will support initiatives and take steps to strengthen Canada’s cyber resilience, including that of its critical infrastructure sectors.
   a. Partnering with the Provinces and Territories
   b. Partnering with the private sector and CI sectors
3. Helping Canadians to be secure online - The Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime.
   a. Combating cybercrime
   b. Protecting Canadians online

The complementary Action Plan 2010-2015 for Canada’s Cyber Security Strategy⁹⁴ lists a number of actions, timelines, deliverables, status and leads responsible for the actions. The actions include:

Securing Government Systems

- Consolidate the Government’s information technology security architecture, in order to improve the security of Government networks.
- Establish a mechanism to prevent and address sophisticated incidents on Government networks.
- Invest to reinforce the Government’s cyber security capabilities.
- Strengthen military aspects of cyber security.

¹The US National Institute of Standards and Technology made its Preliminary Cybersecurity Framework available for review in 2013. This Framework is targeted to an organizational level rather than national level and provides a fairly detailed structure to help identify gaps in an organization’s cybersecurity practices and can be used to express cybersecurity requirements to business partners and customers.
- Improve the Government’s plan to respond effectively to a major cyber incident.
- Improve security training and awareness throughout the Government’s security community.

**Partnering to secure vital cyber systems outside the federal Government**

- **Work With Partners Outside the Government of Canada**
  - Develop a new process to coordinate a national response to major cyber incidents.
  - Engage owners and operators of Canada’s critical infrastructure, using the mechanisms established under the National Strategy and Action Plan for Critical Infrastructure.
  - Engage provinces and territories on cyber security, to seek their active engagement in improving the cyber security of their systems and vital systems under their jurisdiction.
  - Develop a Cyber Security Partnership Program for vital systems outside the Government to provide tangible support to their owners and operators.

Additional actions, not included here, are also listed for partnering under the following themes:

- Improving the Canadian Cyber Incident Response Centre’s (CCIRC) Ability to Support Systems Outside the Government of Canada
- Promote Research and Development
- Engage the International Community

**Helping Canadians to be secure online**

- Improve public awareness (includes multiple deliverables)
- Cyber-crime
  - Create a Cyber Crime Fusion Centre to advance situational awareness and analysis of cyber-crime trends, including new methods for performance measurement and statistical collection.
  - Draft a Canadian Cyber Crime Strategy.
  - Improve the legislative tools to better protect Canadians in cyberspace.

Other actions pertaining to governance are prescribed as follows:

**Governance**

- Provide leadership and coordination across Government in order to focus cyber security programs and resources.
- Develop better governance within Government on cyber security.
- Improve collaboration within federal legal community on cyber security.
- Provide the Government with timely and relevant metrics to measure the effectiveness of the efforts under Canada’s Cyber Security Strategy.
6.3.2 UK Cyber Security Strategy

The 2011 UK Cyber Security Strategy\(^9\) identifies four objectives, with associated approaches and anywhere from 11 to 24 associated actions for each objective (not included here), as follows:

1. Tackling cyber-crime and making the UK one of the most secure places in the world to do business
   a. Tackling cyber crime
   b. Making it safer to do business in cyberspace
2. Making the UK more resilient to cyber-attack and better able to protect our interests in cyberspace.
   a. Defending our national infrastructure from cyber attacks
   b. Ensuring that the UK has the capability to protect our interests in cyberspace
3. Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open society
   a. Helping to shape the development of cyberspace
   b. Protecting our way of life
4. Building the UK’s cross-cutting knowledge, skills and capability to underpin all cyber security objectives
   a. Extending knowledge
   b. Enhancing skills
   c. Expanding capability

6.3.3 Australian Cyber Security Strategy

Australia’s 2009 Cyber Security Strategy\(^9\) has three objectives and seven strategic priorities. The objectives are:

1. All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online;
2. Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers; and
3. The Australian Government ensures its information and communications technologies are secure and resilient.

To achieve these objectives the Australian Government applies the following strategic priorities to its programs:

• Threat Awareness and Response - Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest;
• Culture Change - Educate and empower all Australians with the information, confidence and practical tools to protect themselves online;
• Business-Government Partnerships - Partner with business to promote security and resilience in infrastructure, networks, and services;
• Government Systems - Model best practice in the protection of government ICT systems, including the systems of those transacting with government online;
• International Engagement - Promote a secure, resilient and trusted global electronic operating environment that supports Australia’s national interests;

• Legal and Law Enforcement - Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber-crime; and

• Knowledge, Skills and Innovation - Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

Integral to the Australian Cyber Security Strategy are two key organizations including the national Computer Emergency Response Team (CERT Australia), which is a single coordination point for cyber security issues affecting business, and the Cyber Security Operations Center (CSOC), which provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance.

6.4 Comparison of Cyber Security Strategies

Unlike the general National Strategy and Action Plan for Critical Infrastructure, the Canadian Cyber Security Strategy and Action Plan is more comprehensive, detailed and specific. Although details are not provided in this report, the UK and Australian Strategies also provide a number of specific actions that are equally concrete and detailed.
7 CONCLUSION

The goal of this report was to provide DRDC with an overview of major and emerging research trends in the broad field of critical infrastructure protection and resilience (CIPR) as well as to review and compare national CIPR strategies in Canada, US, UK and Australia. The first step of this project involved gathering bibliographic references from a wide range of scientific papers, followed by a web search for national policies, strategies, and frameworks from an extended list of nations. In addition to the major and emerging trends, readings helped identify key definitions in the field, generate a list of CI sectors for a preselected group of nations and identify available metrics or surveys for CIPR.

Rates of publication in the field of CI have increased since 2009. The dataset is dominated by US affiliations (41%) followed by Italy, the UK, Australia and Canada. Top affiliations in Canada include UBC, Western University, University of Ottawa and DRDC - Ottawa, with nearly half of their publications originating from the Centre for Security Science.

The major topics in the field include several CI sectors (ICT, Energy and utilities, Transportation, Safety, water, Health care, Government, Finance), some of the mitigation strategies discussed in the literature (e.g. Modeling & simulation, Risk assessment, Decision making/support, Policy & directives, Engineering, Monitoring & warning etc.), as well as some of the more general topics in the domain (e.g. Disaster/accident/emergency, Vulnerability, Terrorism, Threat, Interdependencies etc.). We see increasing interest in Disasters (Natural disasters in particular) and a comparative decrease in interest in Terrorism. Throughout the dataset close ties are seen between ICT and Cyber security. We also see connections between the Energy and utilities sector and ICT as well as between Modeling & simulation and the Energy and utilities sector. These linkages give indications of interdependencies that are being discussed in the literature as well as the prevalent use of modeling and simulation techniques in the Energy and utilities sector.

A review of key definitions in the field found very few sources which could provide a true comparison of differences between civilian and military definitions of CIPR. This is likely a result of the confidentiality of military documents. Most nations view critical infrastructure as being key buildings, facilities, systems or networks. Only Australia identified supply chains as part of their critical infrastructure. Only the US has an explicit definition of critical assets, but Canada uses the term ‘assets’ as part of their definition of critical infrastructure. Only the US Defense Department has a definition for CI protection. The US NIPP provides a definition for security of CI which seems to be used in place of protection. In terms of resilience all nations other than Canada refer to a sense of preparedness or anticipation of disaster, whereas Canada is focused on the ability to respond and recover. This distinction suggests that Canada is somewhat “behind the times” in its definition, understanding and approach to CI resilience, a fact which is also seen through the comparison of national strategies.

Critical infrastructure sectors across the nations we compared are fairly consistent for the bulk of sectors, with each nation adding or removing a few sectors in their respective plans. Every nation included energy, water, transport, ICT, health, food supply, banking/finance, government services and safety/emergency services. Our review did not find any specific means or method for ranking the vulnerability or resilience of these sectors, however a closer examination of the various metrics and indices in the field may merit further exploration and reveal more in this regard. While the CI sectors’ research momentum graph, in Figure 9, does not provide a ranking of vulnerability or resilience, it does reflect which areas are receiving the most attention either in the form of R&D or money (or both). It is
likely that these sectors will improve their resilience before the sectors that are not being studied as frequently or in as much detail. This hypothesis should be tested in future studies.

Four thematic groups were created to explore emerging research trends including: General CIPR Topics, CI sectors, Mitigation: Physical countermeasures and Mitigation: Non-physical countermeasures. In the General CIPR topics map, Natural disasters followed by Cyber Attacks superseded Terrorism as the threat of concern in the literature. Emergence is increasingly seen in Mitigation/Prevention, Resilience, Climate change and Sustainability, the first two seemingly replacing a focus on Preparedness. The shift to Resilience with its associated ability to adapt in the face of disaster rather than simply respond is also echoed in the national CIPR strategies. Climate change and Sustainability are two topics that could be further explored for their potential impacts (negative for climate change, positive for sustainability) and links to the field of CIPR. While there may not be a tremendous amount of literature on the interdependencies between CIPR and Climate change to date, Figure 11 and readings that have been done in the field suggest that this will continue to be a growing and critical field of research in the coming years. Likewise, while Interdependencies is a well established topic in the field, researching interdependencies from the perspective of Cascading effects has been growing in recent years. This may simply be a shift in vocabulary but suggests that future studies of this nature should include this terminology as part of search and data collection strategies. Further exploration of the term might determine if there is something beyond a change of vocabulary that is emerging from this subject group.

In terms of the research momentum for subjects in the CI sectors thematic group, the largest areas of publication continue to be ICT, Energy and utilities along with Transportation and Safety. Growth is seen in the Healthcare and Water sectors. Emergence is only seen in a single subject group: Coastal & Waterways. Although this is not a distinct sector, there is notable acceleration in research on coastal regions and waterway infrastructure. Despite there being some overlap with other sectors, there are numerous issues that are unique to this subject group, in particular the impacts and effects of flooding of local waterways. This topic is particularly relevant in Canada where over half (60%) of the nation’s worst disasters in the past decade in terms of economic impacts or deaths have been caused by flooding. This is likely to be a continuing trend given the forecasted risks and impacts of climate change. It is recommended that CI security practitioners actively monitor research in this subject area and assess its inclusion as one of Canada’s CI sectors.

For the Mitigation: Physical countermeasures subject groups emergence was seen in Detection, Intrusion detection and Structural aspects. While Detection is a fairly large and generic subject group, Intrusion detection is the largest subtopic in Detection. There appears to be growing interest in this field, largely related to monitoring of networks. Intrusion detection is also often discussed in conjunction with SCADA systems. Given the interconnectedness of all CI sectors and the rise in concern for cyber security, this is an unsurprising area of growth, but one that should command attention in future studies. Structural aspects include research on Structural health monitoring (SHM), and the latter topic has seen a jump in growth in the past few years. While the subject area is still relatively small, attention should be paid to SHM particularly in terms of modeling and simulation and mitigation. For Mitigation: Non-physical countermeasures, the subjects with the greatest momentum include Artificial Intelligence, which is often seen with Decision making/Support, Sustainability and Ontology/semantics which is related to modeling and simulation of CI. It is interesting to note that Sustainability shows emergence both in comparison to other mitigation methods as well as to general topics in the field. Particular attention to the role of

---

m Please see CIPR Literature Survey: Disaster Risk Mitigation Mechanisms for more information on disasters.
sustainability in CIPR may be an interesting path for future research. Notwithstanding, each of these topics could be monitored for new developments in the future.

One limitation of this study lies in the findings related to metrics and surveys for CIPR. The search strategy that was used in this study was very broad in order to detect major and emerging trends in the field rather than to focus (or bias) the search on metrics. Possibly as a result, the number of relevant publications on metrics and surveys is quite low. It is recommended that additional targeted searches be conducted to provide a more detailed overview of metrics in the field. These additional searches should include the concept of ‘critical infrastructure security’ in addition to other terms related to CIPR. Furthermore, investigation could be done into the work at Argonne National Laboratory on their Resilience Index, Vulnerability Index and Criticality Index. Similarly, the UK’s national strategy, which includes a 30-question resilience self-assessment guide for infrastructure owners and operators, could be reviewed.

Ten national Strategy and Cyber Strategy documents were reviewed for Canada, US, UK and Australia. Similarities lie in the recognized importance of information sharing and partnerships and that the ultimate responsibility of protecting and bolstering resilience in CI lies with owners and operators. In contrast to the other nations, Canada’s strategy is less developed, less detailed and is more focused on protection and risk management than on resilience. One caveat to this conclusion is that the analysis focused on the 2009 Canadian Action Plan for Critical Infrastructure, which is currently the only official Action Plan, and the overview of the 2014 Action Plan did reveal an increase in detail and development. Nevertheless, the National Strategy for Critical Infrastructure remains far less detailed than the other nations’ strategies. Many valuable lessons (such as building partnerships with the first responders community) can be learned from a more in depth examination of these other national strategies, particularly in terms of the implementation activities, action plans and/or sector-specific plans. A careful review of these strategies may potentially help Canada improve the resilience of its own critical infrastructure.
8 REFERENCES


23. McLaughlin BJ, Murrell SD, DesRoches S. Case study: Assessment of the vulnerability of Port Authority of NY & NJ facilities to the impacts of climate change. Congress of the Transportation and Development Institute of ASCE; March 13-16, 2011; Chicago, IL.


32. Vijayasarathy R, Ravindran B, Raghavan SV. A system approach to network modeling for DDoS detection using a Naïve Bayesian classifier. In: proceedings from 3rd International Conference on Communication Systems and Networks; January 4-8, 2011; Bangalore, IN.


35. US President's Critical Infrastructure Protection Board, Department of Energy. 21 steps to improve cyber security of SCADA networks. Washington, D.C.: US President's Critical...


44. Qasem A, Zayed T, Chen Z. A decision support system framework for wastewater treatment plants maintenance and rehabilitation. In: proceedings from Annual Conference of the Canadian Society for Civil Engineering; May 27-30, 2009; St. John's, NL.


49. Matel LJ. Creating an LID environment in an ultra urban setting 2010.


67. Peck A, Bowering E, Simonovic SP. Assessment of climate change risk to municipal infrastructure: A city of London case study. In: proceedings from Annual Conference of the Canadian Society for Civil Engineering; June 9-12, 2010; Winnipeg, MB.


87. Notheis M, Cody J. Evaluating intrusion technologies and security benchmarking for water utilities. In: proceedings from AWWA Water Security Congress; April 10-12, 2005; Oklahoma City, OK.


9 APPENDIX

9.1 Search Strategy

A literature search was conducted in the Scopus, NTIS and PAIS and on the web. The basic search strategy used to retrieve records was based on keywords shown in Table 5 below. Terms or phrases in columns A, B and C were combined using Boolean and proximity operators (AND, OR, NEAR) to cover all aspects of the problem. The search targeted substantive fields such as title, keywords (controlled and uncontrolled vocabularies) and abstracts. The time period was limited to records 2003 to the present. After identifying the major disasters since 2003, a subsequent search was conducted to combine terms or phrases in columns B and D to find information on the specific disasters. Roughly 100 sources, including articles, reports, websites and disaster statistic databases, were reviewed for this report.

<table>
<thead>
<tr>
<th>A: Critical infrastructure</th>
<th>B: Mitigation</th>
<th>C: Risk/threats</th>
<th>D: Specific disasters</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Critical infrastructure</td>
<td>• mitigat*</td>
<td>• risk</td>
<td>• bam, OR Kashmir, OR Yogyakarta, OR Sichuan, OR Indonesia, OR Chile, OR Haiti, OR Japan, OR New Zealand, OR Italy, OR China) AND earthquake*</td>
</tr>
<tr>
<td>• Critical assets</td>
<td>• prevention</td>
<td>• threat</td>
<td>• Cyclone Sidr</td>
</tr>
<tr>
<td>• Public infrastructure</td>
<td>• preparedness</td>
<td>• crisis</td>
<td>• Cyclone Nargis</td>
</tr>
<tr>
<td>• Key resources</td>
<td>• protect*</td>
<td></td>
<td>• Hurricane Sandy</td>
</tr>
<tr>
<td></td>
<td>• resilien*</td>
<td></td>
<td>• Hurricane Katrina</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Deepwater Horizon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• (fire OR flood) AND Canada AND disaster</td>
</tr>
</tbody>
</table>

9.2 R&D Momentum

To ascertain the normalized growth rates and compare values according to their standard deviation for each of the subject groups in the thematic groups, we plotted publication numbers and the angle (slope) of their increase or decline over time time (2008-2012), using linear regression. Average slope degrees and standard deviation were then calculated and standardized, to produce Z-scores, a measure of the relative rate of publishing increase (velocity).

Standardized publication counts were also produced for each of the subject groups analyzed. Plotted on 2-dimensional intersecting axes, the z-scores (velocity) and standardized publication counts (mass) provide an expression of the relative momentum of topics within each group.

This indicator is designed to identify rapidly rising subjects with relatively few publications. The challenge of identifying such subjects lies with the publication volume as a confounding factor, for their rapid growth and evolution is dwarfed by the high volume of established subjects. Specifically, the
The notion of “emergence” consists not only of a sharply rising trend line but also of a small footprint (low publication numbers) in the domain of interest. A relatively small footprint is the reason emerging subjects are often overlooked until their disruptive impacts become obvious.

The four-quadrant visualization provides a structured view of the relative position of these subjects within the group. The indicator can also be applied to identify differences between topics with small publication numbers but relatively greater velocity.

A third dimension is added by relating the size of each node to its actual publication count.

One possible limitation of the methodology may be absent or incomplete publication values for certain years in a time series, so the analysis provided by z-scores should also be accompanied by a review of actual values over time wherever possible.
9.3 Building the CI Sector Groups

Table 8. Building the CI Sector Groups

<table>
<thead>
<tr>
<th>CI Sectors</th>
<th>Examples of Keywords added to Sector Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy and Utilities</td>
<td>Electrical power, natural gas, oil production and transmission systems, petroleum, petrochemical, Grid, nuclear energy</td>
</tr>
<tr>
<td>Information &amp; Communication Technology (ICT)</td>
<td>Telecommunications, broadcasting systems, software, hardware and networks including the Internet</td>
</tr>
<tr>
<td>Finance</td>
<td>Banking, securities and investment</td>
</tr>
<tr>
<td>Health Care</td>
<td>Hospitals, Health Care and blood supply facilities, laboratories and pharmaceuticals</td>
</tr>
<tr>
<td>Food</td>
<td>Safety, distribution, agriculture and food industry</td>
</tr>
<tr>
<td>Water</td>
<td>Drinking water and wastewater management</td>
</tr>
<tr>
<td>Transportation</td>
<td>Air, rail, marine, ports, surface and mass transit, roads, highways, bridges, tunnels, pipeline, traffic</td>
</tr>
<tr>
<td>Safety</td>
<td>Chemical, biological, radiological and nuclear safety (excludes the industry in general and focuses on accidents, weapons, warfare etc), hazardous materials, search and rescue, emergency services/response and dams</td>
</tr>
<tr>
<td>Government</td>
<td>Service delivery, facilities, information networks, assets and key national sites and monuments</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Defense industrial base, chemical industry, manufacturing</td>
</tr>
<tr>
<td>Coastal and Waterways</td>
<td>River basin/flow/embankment/control, coastal zones/areas/environment/management/infrastructure, sea level change, marine ecosystems, marine environment, marine transportation/security, ports</td>
</tr>
</tbody>
</table>

Informed by the Canadian and US CI sectors but more closely following the Canadian.
### 9.4 Canadian Affiliations Profile

Table 9. Canadian Affiliations Profile

Table 9 presents the Canadian affiliations that have a minimum of three publications along with their top authors, the affiliations they co-author with, the top keywords and subject groups for their publications as well as a timeline which gives a sense of when they have been most active. The numbers in square brackets shows the number of publications associated with each term. The numbers listed for keywords and subject groups are not mutually exclusive in that a single publication can be counted in more than one keyword/subject group at a time.

<table>
<thead>
<tr>
<th>Organization Name</th>
<th>Top Authors</th>
<th>Co-Authoring Organizations</th>
<th>Top Keywords</th>
<th>Top Subject Groups</th>
<th>Publication Year (Line Chart)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Name</td>
<td>Top Authors</td>
<td>Co-Authoring Organizations</td>
<td>Top Keywords</td>
<td>Top Subject Groups</td>
<td>Publication Year (Line Chart)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>Makrakis, D. [2]; Nayak, A. [2];</td>
<td>Ottawa, ON, Canada [1]; DRDC - Ottawa, Ottawa, ON, Canada [1]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University of New Brunswick, Fredericton, NB</td>
<td>Bagheri, E. [4]; Rahim, A. [3]; Carretero, J. A. [3]; Ghorbani, A. A. [3]; Salah, S. [3]; Uliero, M. [2]; Hosseini, H. [1];</td>
<td>Johnson Controls Int'l., Dubai, United Arab Emirates [1]; University of Western Ontario, London, ON [1]; Information Security Centre of Excellence (ISCE) [1]; Iran Telecommunication Research Center (ITRC), Tehran, Iran [1]; 1 more items with [1]</td>
<td>Risk management [3]; Risk analysis [2]; Computer simulation [2]; Smart grid [1]; Information technology [1]; Security of data [1]; Telecommunication [1]; Public works [1]; Decision making [1];</td>
<td>Modeling and simulation [6]; Risk management [2]; Interdependencies [4]; ICT sector [3]; Adaptation [3]; Risk assessments [2];</td>
<td></td>
</tr>
<tr>
<td>Organization Name</td>
<td>Top Authors</td>
<td>Co-Authoring Organizations</td>
<td>Top Keywords</td>
<td>Top Subject Groups</td>
<td>Publication Year (Line Chart)</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>University of Waterloo, ON [10]</td>
<td>Shen, X. [2];</td>
<td>University of Hawaii, Honolulu, HI, USA [1]; University of Ulster, United Kingdom [1]; Yale University, New Haven, CT, USA [1]; University of Illinois at Urbana-Champaign, IL [1]; 6 more items with [1]</td>
<td>Risk assessment [2]; Computer simulation [1]; Smart grid [1]; Telecommunication [1]; Decision making [1]; Internet [1]; Security [1]; Public infrastructure [1]</td>
<td>Modeling and simulation [4]; Disaster/accident/emergency [3]; Energy and utilities sector [3]; ICT sector [3]; Risk assessments [2]; Decision making/support [2]; Transportation sector [2];</td>
<td></td>
</tr>
<tr>
<td>Organization Name</td>
<td>Top Authors</td>
<td>Co-Authoring Organizations</td>
<td>Top Keywords</td>
<td>Top Subject Groups</td>
<td>Publication Year (Line Chart)</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>University of Calgary, AB</td>
<td>Chai, C.-L. [2]; Tu, Y. L. [2];</td>
<td>University of Saskatchewan, Saskatoon, SK, Canada [2];</td>
<td>Security of data [4]; Risk management [2]; Smart grid [1]; SCADA [1];</td>
<td>Cyber security [4]; ICT sector [3]; Modeling and simulation [3]; Vulnerability [2];</td>
<td>![Graph 1]</td>
</tr>
<tr>
<td></td>
<td>Ulmeru, M. [2]; Deters, R. [2];</td>
<td>Northeastern University, China [1];</td>
<td>Secure system [1]; Computer simulation [1]; Disasters [1]; Public works [1];</td>
<td>Risk management [2]; Response [2]; Energy and utilities sector [2]; Disaster/accident/emergency [2]; Mitigation/Prevention [2];</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Liu, X. [2]; Worthington, P. [2];</td>
<td>13 more items with [1]</td>
<td>Risk assessment [1]; Decision making [1]; 1 more items with [1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zhang, W. J. [2];</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>University of Saskatchewan, Saskatoon, SK, Canada [2]; Northeastern University, China [1]; 13 more items with [1]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dalhousie University, Halifax, NS [6]</td>
<td>Quigley, K. F. [2];</td>
<td>University of Strathclyde, Glasgow, UK [1]; George Mason University, Fairfax, VA, USA [1]; Georgia State University (GSU), Atlanta, GA, USA [1]; University of California, Irvine, CA, USA [1]; 7 more items with [1]</td>
<td>United States [2]; Terrorism [1]; National Security [1]</td>
<td>Natural disaster [2]; Education [2]; Laws &amp; legislation &amp; regulation [2]; Health care sector [2]; Transportation sector [1]; Disaster/accident/emergency [1]; Government sector [1]; Terrorism [1]; Coastal regions and waterways [1]; Impacts [1]; 1 more items with [1]</td>
<td>![Graph 3]</td>
</tr>
</tbody>
</table>

United States [2]; Terrorism [1]; National Security [1] | Natural disaster [2]; Education [2]; Laws & legislation & regulation [2]; Health care sector [2]; Transportation sector [1]; Disaster/accident/emergency [1]; Government sector [1]; Terrorism [1]; Coastal regions and waterways [1]; Impacts [1]; 1 more items with [1] | ![Graph 3]                   |
<table>
<thead>
<tr>
<th>Organization Name</th>
<th>Top Authors</th>
<th>Co-Authoring Organizations</th>
<th>Top Keywords</th>
<th>Top Subject Groups</th>
<th>Publication Year (Line Chart)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carleton University, Ottawa, ON [5]</td>
<td>Dandamudi, S. P. [1]; Walby, K. [1]; Abawajy, J. H. [1]; Vishnukanthan, K. [1]; Sivathayalan, S. [1]; Miller, L. N. [1]; Monaghan, J. [1]; Lau, D. T. [1]; Rudner, Martin [1]; Waller, C. L. [1]</td>
<td>N/A</td>
<td>Public infrastructure [1]; Risk assessment [1]; Internet [1]; Network security [1]; Security [1]; Terrorism [1]</td>
<td>ICT sector [2]; Terrorism [1]; Threat [1]; Education [1]; Fault tolerance &amp; detection [1]; Natural disaster [1]; Network Security [1]; Structural aspects [1]; Policy &amp; directives [1]; Risk assessments [1]; 4 more items with [1]</td>
<td><img src="chart1.png" alt="Line Chart" /></td>
</tr>
<tr>
<td>McGill University, Montreal, QC [5]</td>
<td>McCullough, L. [1]; Wei, F. [1]; Berggraf, L. [1]; Lovegrove, G. [1]; Perez-Sorrosal, F. [1]; Patiño-Martinez, M. [1]; Jimenez-Peris, R. [1]; Osborn, K. [1]; Kemme, B. [1]; Mitchell, D. [1]; 9 more items with [1]</td>
<td>Canadian Seismic Research Network (CSRN) [1]; Harvard Medical School, Boston, MA, USA [1]; Concordia University, Montreal, QC [1]; Modum Bad Research Institute, Vikersund, Norway [1]; 3 more items with [1]</td>
<td>Disasters [1]; Internet [1]; Risk assessment [1]</td>
<td>Modeling and simulation [2]; Transportation sector [2]; Safety sector [2]; Hazard [1]; Environmental aspects [1]; Risk assessments [1]; Structural aspects [1]; Natural disaster [1]; Fault tolerance &amp; detection [1]; Education [1]; 12 more items with [1]</td>
<td><img src="chart2.png" alt="Line Chart" /></td>
</tr>
<tr>
<td>Organization Name</td>
<td>Top Authors</td>
<td>Co-Authoring Organizations</td>
<td>Top Keywords</td>
<td>Top Subject Groups</td>
<td>Publication Year (Line Chart)</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>----------------------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
## Organization Name

**McMaster University, Hamilton, ON [3]**

- **Top Authors:**
  - Aultman-Hall, L. [1];
  - Mekky, W. F. [1];
  - Guo, F. [1];
  - Scott, D. M. [1];
  - Eyles, J. [1];
  - Changiz-Rezaei, S. H. [1];
  - El-Dakhakhni, W. W. [1];
  - Novak, D. C. [1]

- **Co-Authoring Organizations:**
  - University of Vermont, Burlington, VT, USA [1];
  - University of Connecticut, Storrs, CT, USA [1];
  - Nuclear Safety Solutions Limited, Toronto [1]

- **Top Keywords:** Security [1]

- **Top Subject Groups:** Structural aspects [1]; Safety sector [1]; Construction [1]; Transportation sector [1]; Sustainability [1]; Response [1]; Engineering [1]

---

**University of Winnipeg, MB [3]**

- **Top Authors:**
  - Kankanhalli, M. [2];
  - Atrey, P. K. [2];
  - Wang, X. [2];
  - Saini, M. [2];
  - Yan, P. [1];
  - Pizzi, N. J. [1];
  - Moghadas, S. M. [1];
  - Wu, J. [1]

- **Co-Authoring Organizations:**
  - National University of Singapore, Singapore [2];
  - Centre for Communicable Diseases and Infection Control, Infectious Diseases and Emergency Preparedness Branch, Ottawa, ON [1];
  - National Research Council Canada, Winnipeg, MB [1];
  - York University, Toronto, ON [1]

- **Top Keywords:** Secure system [2]

- **Top Subject Groups:** Modeling and simulation [3]; Detection [2]; Threat [2]; Monitoring & warning [2]; Health care sector [1]; Policy & directives [1]; Decision making/support [1]; Safety sector [1]; Natural disaster [1]

---

**Université de Montréal, QC [3]**

- **Top Authors:**
  - Gendron, B. [1];
  - Rees, E. E. [1];
  - Coté, N. [1];
  - Hafsi, T. [1];
  - Bélanger, D. [1];
  - Mauras, E. [1];
  - Farashahi, M. [1];
  - Lelièvre, F. [1]

- **Co-Authoring Organizations:**
  - Bruno Gendron Consultant, Lachine, QC [1];
  - Ministère de l’Agriculture, Des Pêcheries et de l’Alimentation, Québec, QC [1];
  - Concordia University, Montreal, QC [1];
  - Ministère des Ressources naturelles et de la Faune du Québec, QC [1]

- **Top Keywords:** Internet [1]

- **Top Subject Groups:** ICT sector [1]; Natural disaster [1]; Health care sector [1]; Monitoring & warning [1]