CRITICAL 5

Forging a Common Understanding for Critical Infrastructure

Shared Narrative

March 2014

Forging a Common Understanding for Critical Infrastructure

The following narrative represents the shared views of the Critical 5 member nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) with the objective to provide a high-level overview of the meaning and importance of critical infrastructure.[1] This project supports the ongoing effort to clearly articulate and communicate a common message on the value, purpose, and historical trajectory of this important functional domain and seeks to arrive at a common understanding of critical infrastructure and its role in society. The narrative identifies shared priorities and interconnections among our countries and lays the foundation for future collaboration. The approach used in this narrative is to identify similarities in definition, approach, concept, and implementation in order to arrive at a shared understanding of critical infrastructure.

Proposed definition of critical infrastructure

In order to forge a common understanding of critical infrastructure, the Critical 5 members analyzed the definitions and the specified sectors identified in the national infrastructure plans to identify commonality and overlap to find the similarities and differences to build a bridge of common understanding among our unique nations and situations. While each definition of critical infrastructure is slightly different there are common threads that run throughout.[2] We propose the following definition as the starting point for a discussion about critical, nationally significant infrastructure: **Critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations.** Throughout the narrative, the unique scope and intentions of the specific country definitions will be included, but this definition is recommended in order to provide a common framework to shape international engagement on critical infrastructure.

Evolution of the security environment

Each of the Critical 5 nations has been involved in developing and securing its infrastructure for decades. However, there have been significant shifts in the global security environment that have caused each of the members to approach infrastructure security and resilience in new ways. Arising from the unstable security environment of the first decade of the new millennium (from such events as the September 11 , 2001 terrorist attacks, the 2002 bombings in Bali, the 2005 London bombings, the unprecedented

[1] It is also possible that this shared narrative could set the stage for future shared narratives on related topics as identified by Critical Five leadership.

[2] For further information on the specific definitions each country uses for critical infrastructure, please see the individual country pages at the end of this document.

damage from natural disasters and the global financial crisis) addressing critical infrastructure security and resilience became a focus for each member nation. Each disaster demonstrated the important role of national governments in helping cultivate secure and resilient critical infrastructure.

Disasters and changes in the global security environment also encouraged the nations to think broadly about the array of threats and hazards facing their national infrastructure. The Critical 5 nations have adopted an all-hazards approach to address the current and future challenges facing their infrastructure. In particular, trends like climate change and demographic shifts are likely to accelerate in the future and have an impact on infrastructure systems and assets. Since there are high consequences to service disruption, it is important for nations to address these trends as part of critical infrastructure security and resilience. In many cases, the best time to address these trends and other potential disruptors is when the infrastructure systems and assets are being designed. Critical infrastructure, particularly built systems and assets, can have a very long lifespan, so each Critical 5 nation recognizes the importance of planning for future shifts that could disrupt the services infrastructure provides.

Security and resilience within critical infrastructure

The national governments of the Critical 5 nations have established departments and offices to help manage the risks to their critical, nationally significant infrastructure (in conjunction with the owners/operators), and in an effort to increase our international cooperation, each one of the Critical 5 nations has come together to build a shared narrative that outlines the similarities and differences among the members. By forging a common understanding of what each member means by critical infrastructure security and resilience, the members will be able to find opportunities to share information and analysis as well as leverage best practices.

Each of the Critical 5 nations highlights the importance of secure and resilient systems.[3] Therefore, it is important to reach a common definition of critical infrastructure resilience. An examination of the Critical 5's strategic guidance documents finds that each of the countries recognizes **resilience as the need for systems to have the capacity to be flexible and adaptable to changing conditions, both foreseeable and unexpected, and to be able to recover rapidly from disruption**. Although the definition can be broadened, we propose that when discussing critical infrastructure resilience among the Critical 5 partners, this definition can form the foundation of what each country is trying to achieve.

Similar to critical infrastructure resilience, one can reach a common definition for critical infrastructure security. It is implied that **the end goal of security is to use physical, personnel and/or cyber defense measures to reduce both the risk to critical infrastructure and the risk of loss due to a disruption in essential services by minimizing the vulnerability of critical infrastructure assets, systems and networks.** We are articulating this common goal to facilitate the discussion on how each nation works to enhance secure infrastructure and resilience.

[3] Each of the country definitions for resilience can be found in the individual country sections; See Annex A, "Critical Five Countries Definition of Critical Infrastructure and Associated Sectors."

Each nation provides strategic guidance on the need for both critical infrastructure security and resilience. Australia, Canada, New Zealand, the United Kingdom and the United States are approaching critical infrastructure security from a national security lens – whether regarding their physical assets, cyber assets, or a combination of the two. Importantly, through each of the members' strategic documents it can be observed that national, economic and societal security is the driving force behind the need for critical infrastructure security and resilience. In New Zealand, the security and prosperity of both the economy and society are the main priorities. Critical infrastructure provides essential services that are vital to the safety and security of the population and securing these services and ensuring the services can recover rapidly in the event of a disaster is a top priority for each of the countries.

Critical infrastructure and economic prosperity

Each of the Critical Five Members has articulated how important critical infrastructure is to promoting economic prosperity and economic security. Governments make investments in critical infrastructure – whether directly or through partnerships – in order to strengthen their economies and help their societies prosper. Critical infrastructure forms the backbone to modern society by providing essential services that help businesses grow and flourish, such as high-speed communications, modern transportation networks, and reliable energy, which facilitates trade and economic growth. Critical infrastructure services are vital to economic growth, so governments work to ensure that these services are as secure and resilient as possible. By ensuring critical infrastructure is secure and resilient, the governments can protect and increase the strength and vitality of their respective economies. As Canada noted in its national strategy, "resilient critical infrastructure stimulates economic growth, attracts and retains businesses and creates employment opportunities." [4]

When governments focus on making critical infrastructure more secure and resilient by managing risk, trust and confidence is enhanced in the public-private relationship, which then facilitates economic growth. This trust and confidence in critical infrastructure is essential to achieving safe, secure and prosperous societies. For instance, New Zealand recognizes that critical infrastructure is an important driver of economic growth for this very reason. New Zealand notes that "in order to promote growth and investment, companies need to be confident that the infrastructure systems supporting their businesses are secure and resilient." [5] This concept of secure and resilient infrastructure instilling confidence in investors and their businesses is highlighted within the strategic guidance of all the Critical 5 member nations. [6]

---

[4] Public Safety Canada, *National Strategy for Critical Infrastructure*, (Public Safety Canada, 2009). Pg. 3

[5] *The Business Growth Agenda: Building Infrastructure*, (New Zealand Government, 2012). Pg. 2

[6] For further examples on the importance of critical infrastructure to the economy, see Australia's *Critical Infrastructure Resilience Strategy (2010)*; the United Kingdom's *Investing In Britian's Future* (2013); and the United States' *Presidential Policy Directive 21:Critical Infrastructure Security and Resilience* (2013)

Common approaches to managing critical infrastructure

While each of the Critical 5 nations has unique characteristics, the intent behind the security and resilience of vital infrastructure assets and systems is the same and all countries are focused on managing the risk. All of the Critical 5 members work hard to build partnerships with their individual owners and operators, all of them promote collaboration, information sharing, and risk management. These commonalities provide the foundation through which the security and resilience of critical infrastructure can expand internationally and build the relationships between the Critical 5 members.

Each of the Critical 5 nations maintains strong partnerships with their national, regional and local government counterparts and the critical infrastructure owners and operators. These partnerships are essential, because critical infrastructures systems are owned and operated by both private and public sector stakeholders. In addition, all partners recognize the importance of being a national leader for infrastructure security and resilience, and in general, they work in similar ways to build these partnerships.

Information sharing is critical to the critical infrastructure security and resilience strategy as well, and each nation strives to share timely and relevant information in a safe and trusted environment. Whether it is through the dedicated business-government forum that includes online and face-to-face interactions like Australia's Trusted Information Sharing Network (TISN), the United Kingdom's work setting up safe "information exchanges" [7] that provide online guidance tools and resources for owners and operators via a secure extranet website, or hosting forum with the relevant communities. Each country is actively engaged in building up these types of trusted information sharing channels by using public facing websites, information portals and gateways, partnerships, or a myriad of other approaches.

At the national level, the governments work to make their critical infrastructure more secure and resilient in order to maintain and improve upon the essential services provided by that infrastructure. Below is a quick look at the common actions the governments take in order to promote critical infrastructure security and resilience and help deliver the essential services to their respective populations:

- Looking across regions and using their analytical resources to identify nationally significant critical infrastructure sectors and the services they provide.
- Coordinating with public and private sector partners on how to make that infrastructure more secure and resilient.
- Sharing important and timely information with relevant stakeholders.
- Collaborating with partners and stakeholders to share best practices.

[7] Centre for the Protection of National Infrastructure, *Information Exchanges*, http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/ (accessed September 16, 2013). The information exchanges allow one company to learn from the experiences, mistakes and successes of another without fear of exposing company sensitivities.

- Identifying cross-sector dependencies.
- Developing a workforce and culture that is ready to handle the complex challenges impacting critical infrastructure.
- Identifying and assessing the criticality of infrastructure.
- Using a risk management approach that identifies ways to reduce risk to critical infrastructure.

Common critical infrastructure sectors

All countries identify critical infrastructure sectors. [8] For the purpose of discussion, it is also useful to see where there are commonalities and differences among the identified critical infrastructure sectors.

Every Critical 5 member nation has identified the following sectors as critical:

- Communications
- Energy [9]
- Healthcare and Public Health
- Transportation Systems
- Water (to include Wastewater and Storm Water Systems)

In addition, several members of the Critical 5 also highlight the following sectors as critical:

- Banking and Financial Services[10]
- Critical Manufacturing[11]
- Emergency Services[12]
- Food and Agriculture[13]
- Government Facilities[14]
- Information Technology[15]

[8] The list of each country's critical infrastructure sectors can be found in Annex A.
[9] The United States has several critical infrastructure sectors that relate to energy, including dams and nuclear reactors, materials and waste. Australia has identified sub-sectors that also relate to energy, including onshore and offshore oil and gas, electricity systems, and the coal supply.
[10] Australia, Canada, the United Kingdom and the United States reference banking and financial services.
[11] Canada and the United States highlight critical manufacturing as a critical sector.
[12] Canada, United Kingdom and the United States include emergency services as a sector. Australia includes emergency services as a sub-sector.
[13] Australia, Canada, the United States and the United Kingdom [food sector only] have identified food and agriculture as a sector.
[14] Canada, New Zealand, the United Kingdom and the United States all highlight this sector as a critical. Australia has clearly articulated the government's role in critical infrastructure security and resilience, but has not made government facilities a sector.
[15] Canada, New Zealand and the United States include information technology as a sector. The United Kingdom has a Communication sector that includes radio and television broadcasters, postal communications and telecommunications but does not specifically include information technology in this category.

It is clear from this survey that there is significant overlap between the Critical 5 nations. At the same time, each of the countries prioritizes the vital services that underpin the safety and security of their respective populations. As Critical 5 partners work to develop strategies for strengthening international ties, we can use this understanding of how our sectors align as a starting point for discussions on how we can work together and have a fruitful, beneficial relationship.

Conclusion

It is clear from the survey of existing plans, strategies, and guidance, that the Critical 5 members are developing common strategies for addressing critical infrastructure security and resilience. This narrative proposes that we accept the following definitions to form the basis of a common understanding and to help facilitate a coordinated approach to, and next steps to enhance, critical infrastructure security and resilience:

- Critical Infrastructure: the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations *(also referred to as nationally significant infrastructure)*
- Resilience: systems have the capacity to be flexible and adaptable to changing conditions, both foreseeable and unexpected, and are able to recover rapidly from disruptions
- Security: the use of physical, personnel and/or cyber defense measures to reduce both the risk to critical infrastructure and the risk of loss due to a disruption in essential services by minimizing the vulnerability of critical infrastructure assets, systems and networks.

In addition to developing common definitions, the research has also elucidated the common approaches each member country shares as well as the common types of infrastructure each member country deems critical. This baseline assessment will help each of the members find common ground and inform our discussions on key issues of mutual interest going forward.

Annex A: Critical Five Countries' Definitions of Critical Infrastructure and Associated Sectors

AUSTRALIA

Australia defines its critical infrastructure as 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 defense and ensure national security.[16] The definition acknowledges that some elements of critical infrastructure are not assets, but are in fact networks or supply chains.

Australia has adopted a resilience-based approach to critical infrastructure in order to enable it to adapt to change, reduce the country's exposure to risk and learn lessons from past incidents. Australia notes that a key element of disaster resilience is enhancing "the capacity to withstand and recover from emergencies and disasters."[17] Australia's resilience strategy encourages organizations to identify ways in which they can be flexible and adaptable in the face of unforeseen shocks. Australia's Critical Infrastructure Resilience Strategy states that:

> *"A resilience approach to managing risks to our critical infrastructure encourages organisations to develop a more organic capacity to deal with rapid on-set shock. This is in preference to the more traditional approach to developing plans to deal with a finite set of scenarios, especially in the context of an increasingly complex environment."* [18]

[16] Australian Government, *Critical Infrastructure Resilience Strategy*, (Australian Government, 2010). Pg. 8
[17] Ibid. Pg. 9
[18] ibid. Pg. 5

Australian Critical Infrastructure:[19]

Banking and Finance - Financial services	**Health** - Supply of blood and blood products/hospitals
Communications - Broadcast media - Postal services - Telecommunications networks	**Transport** - Aviation - Land based mass passenger transport (including bridges and tunnels) - Land freight - Maritime: Shipping and ports
Energy - Electricity systems - Offshore oil and gas - Onshore oil and gas - Coal supply	**Water Services** - Water utilities
Food Chain - Food supply sector	*Other critical sub-sectors:* - Labs holding high risk biological agents - Chemical manufacturing industry - Defence industries - Emergency Service

[19] The bolded sectors in the table represent the broad sectors recognised under the *Critical Infrastructure Resilience Strategy*. These sectors comprise a number of more detailed sub-sectors that are primarily used as the basis for conducting threat assessments.

CANADA

Critical infrastructure refers to 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 the government.[20] Canada's strategic vision is for the nation to build a safer, more secure and more resilient Canada through its critical infrastructure. In Canada, the *Emergency Management Framework for Canada*, which informs the *National Strategy for Infrastructure*, defines resilience as "the capacity of a system, community or society exposed to hazards to adapt to disturbances resulting from hazards by persevering, recuperating or changing to reach and maintain an acceptable level of functioning."[21]

The National Strategy for Critical Infrastructure is based on the understanding that "enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters."[22] In addition, the *Emergency Management Framework for Canada* highlights the importance of reducing risk through prevention, mitigation, preparedness, planning and response. Embedded in their disaster risk reduction concept is the need for resilience, which they define as "the capacity of a system, community or society exposed to hazards to adapt to disturbances resulting from hazards by preserving, recuperating or changing to reach and maintain an acceptable level of functioning." [23]

Canadian Critical Infrastructure:

Energy and Utilities	Information and Communication Technology
Finance	Manufacturing
Food	Safety
Government	Transportation
Health	Water

[20] Public Safety Canada, *National Strategy for Critical Infrastructure*, (Public Safety Canada, 2009). Pg. 2
[21] Emergency Management Policy Directorate, *An Emergency Management Framework for Canada (2nd ed.)*, (Emergency Management Policy Directorate, 2011). Pg. 8
[22] *National Strategy for Critical Infrastructure.* Pg. 2
[23] *An Emergency Management Framework for Canada*. Pg. 8

NEW ZEALAND

Infrastructure has been identified as one of the six key drivers of economic growth in New Zealand (in the Business and Growth Agenda 2012) and is defined as "the fixed, long-lived structures that facilitate the production of goods and services and underpin many aspects of quality of life. Infrastructure refers to physical networks, principally transport, water, energy and communications."[24]

In New Zealand, infrastructure is identified as an important contributor to improving living standards for all New Zealanders.[25] To that end, the New Zealand government expresses its vision that "by 2030 New Zealand's infrastructure is resilient and coordinated and contributes to economic growth and increased quality of life." [26] New Zealand defines resilient infrastructure as being "able to deal with significant disruption and changing circumstances." [27] There are two key outcomes the government would like to drive through its infrastructure strategy: better use of existing infrastructure and better allocation of new investment.[28]

New Zealand's National Security System, released in May 2011, takes a broad, all-hazards, approach to national security. With regard to critical infrastructure, it highlights "new points of vulnerability" from the integrated and networked character of national and international infrastructures, such as electricity, gas and water grids, telecommunications networks, air, rail and shipping services, and the extent to which daily life depends on their efficient functioning. New Zealand's Cyber Security Strategy from June 2011 has identified as one of its three objectives the need to improve cyber security for critical national infrastructure and other businesses.

New Zealand's Critical Infrastructure:

Energy	Transportation
Social Infrastructure	Water
Telecommunications	

[24] National Infrastructure Unit, *New Zealand National Infrastructure Plan*, (New Zealand Government, 2011). Pg. 1
[25] Treasury. *Higher Living Standards.* (New Zealand Government, 2013). http://www.treasury.govt.nz/abouttreasury/higherlivingstandards
[26] *New Zealand National Infrastructure Plan* 2011. Pg. 11
[27] ibid., Pg. 12
[28] ibid., Pg. 2

UNITED KINGDOM

The UK's national infrastructure are those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of essential services upon which daily life depends. The United Kingdom uses critical infrastructure as "a broad term to describe critical national infrastructure and other infrastructure of national significance as well as infrastructure and assets of local significance."[29] Within the UK Government, the Home Office leads on policy related to the security of CNI in relation to terrorist threats and the Civil Contingencies Secretariat in Cabinet Office leads on policy related to improving the resilience of CNI and mitigating the impact of natural hazards.

In the UK, one of the National Security Strategy objectives is to ensure "a secure and resilient UK– protecting our people, economy, infrastructure, territory and way of life from all major risks that can affect us directly – requiring both direct protection against real and present threats such as terrorism and cyber attack, resilience in the face of natural and man-made emergencies and crime, and deterrence against less likely threats such as a military attack by another state."[30]

Furthermore, the UK Home Office set out the UK Government's counter terrorism strategy in CONTEST, outlining that it will continue to reduce the vulnerability of the national infrastructure, especially the most critical parts, and that Government will take a wider focus on strengthening protective security for civil nuclear and hazardous sites as well. It will ensure that high quality advice on protective security is available to those responsible for crowded places; implementation will be for local authorities and business owners.

The UK's Centre for the Protection of National Infrastructure (CPNI) has issued strategic guidance that serves as a model of resilience and shares best practices and advice to enable owners and operators of the UK's critical infrastructure to improve the security and resilience of their assets.[31] The guidance posits that "building resilience in our infrastructure is important to reduce our vulnerability to natural hazards. This can be achieved by improving (where necessary) protection; encouraging an ability in organisations and their infrastructure networks and systems to absorb shocks and recover; and enabling an effective local and national response to emergencies."[32]

The United Kingdom's definition of resilience is defined as "the ability of assets, networks and systems to anticipate, absorb, adapt to and/or rapidly recover from a disruptive event. In its broader sense, it is

---

[29] Centre for the Protection of National Infrastructure, *Keeping the Country Running: Natural Hazards and Infrastructure* (2011). Pg. 12

[30] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (October 2010) Pg. 22[31] HM Government, *Resilience in Society: Infrastructure, Communities and Businesses*, (2013). https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses (accessed September 26, 2013)

[31] HM Government, *Resilience in Society: Infrastructure, Communities and Businesses*, (2013). https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses (accessed September 26, 2013)

[32] *Keeping the Country Running: Natural Hazards and Infrastructure.* Pg. 5

more than an ability to bounce back and recover from adversity and extends to the broader adaptive capacity gained from an understanding of the risks and uncertainties in our environment."[33]

United Kingdom's Critical Infrastructure:

Communications	Health
Emergency Services	Government
Energy	Transportation
Food	Water
Finance	

[33] Ibid., Pg. 14

UNITED STATES

The United States refers to critical infrastructure as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[34]

The United States, under the guidance of *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience*, is developing a national policy to promote critical infrastructure security and resilience. The Nation's critical infrastructure provides essential services that underpin American society, and therefore, critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. [35] Resilience and security are both defined within *PPD 21*, with resilience "meaning 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"[36] and security referring to "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." [37]

United States' Critical Infrastructure:

Chemical	Financial Services
Commercial Facilities	Food and Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare and Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors, Materials and Waste
Emergency Services	Transportation Systems
Energy	Water and Wastewater Systems

[34] The White House Office of the Press Secretary, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed August 26, 2013).
[35] ibid.
[36] ibid.
[37] ibid.

The **Critical Five** is an international forum, established in 2012, comprising members from government agencies responsible for critical infrastructure protection and resilience in Australia, Canada, New Zealand, the United Kingdom, and the United States. The Critical Five aims to strengthen cooperation between member countries on addressing the threats to critical infrastructure, as well as to share information, practices and ideas on domestic policy and operational approaches to critical infrastructure protection and resilience.

CONTACT

Critical Infrastructure Policy, Public Safety Canada

http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx

ci-ie-information@ps.gc.ca