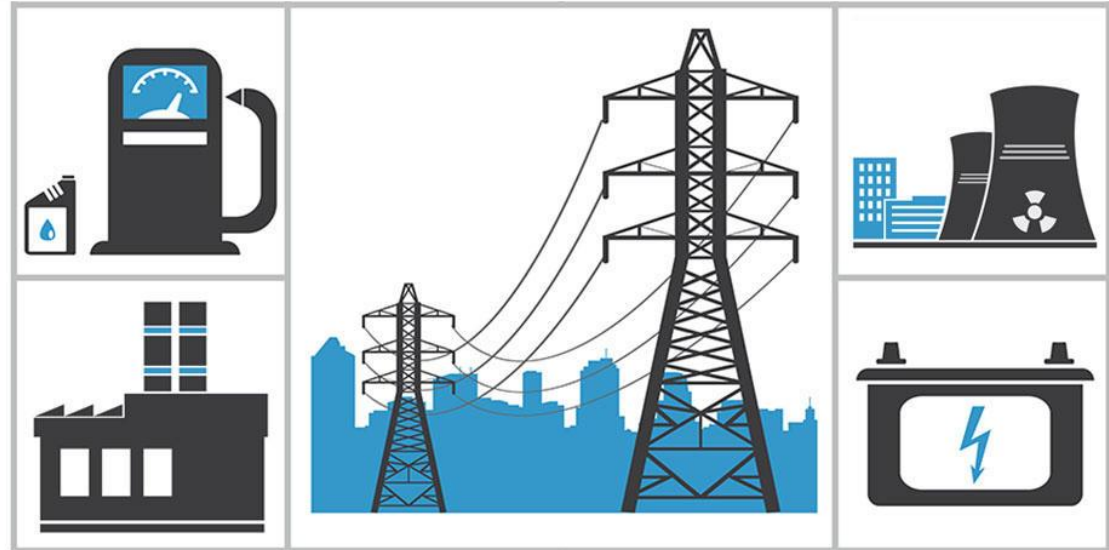


Industrial Cyber Security Laws

What is “Critical” Infrastructure?

- Electricity
 - Nuclear
 - Coal
 - Wind
 - Hydro
- Water
- Sanitation
- Public Transport
- Gas



<https://www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure>

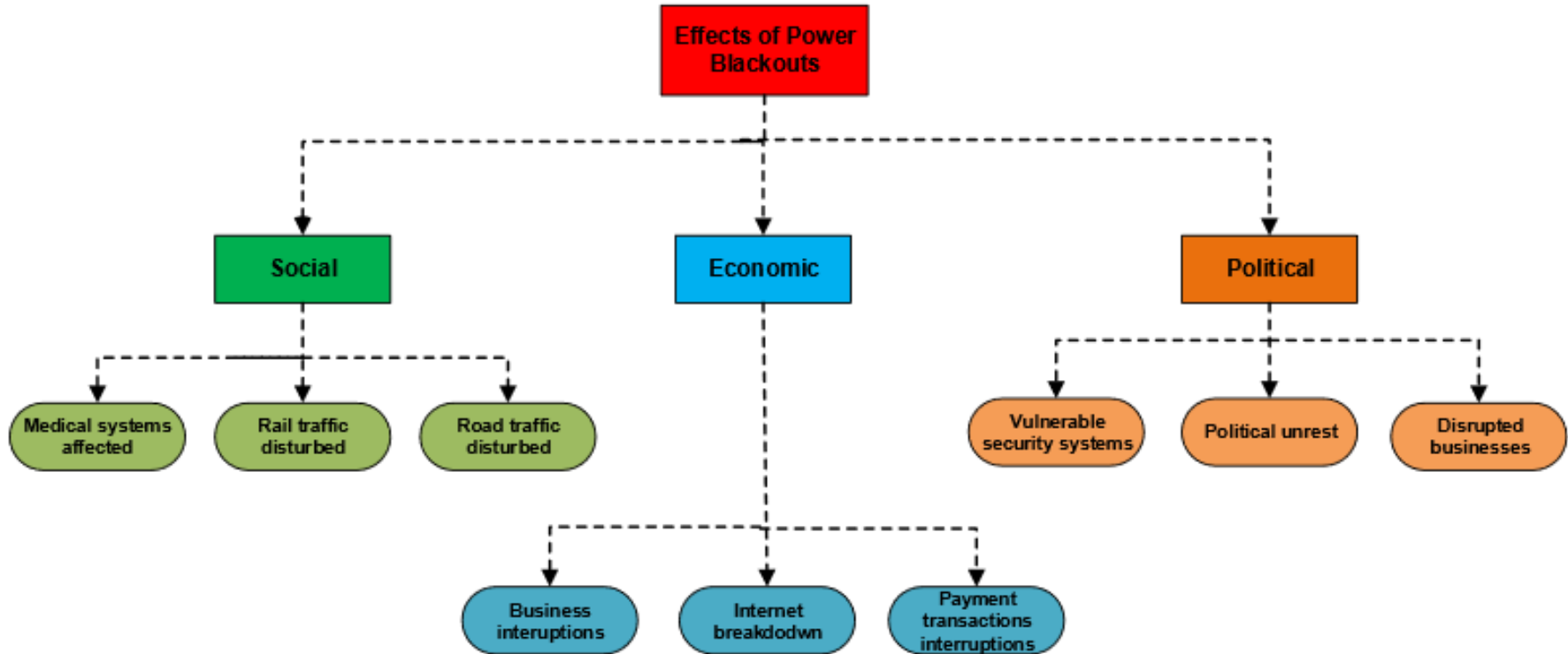


Figure 5. Major electric power system blackout causes.

Security of Critical Infrastructure

Act 2018 of Australia, Critical infrastructure assets are defined as:

- *a critical electricity asset*
- *a critical port*
- *a critical water asset*
- *a critical gas asset*
- *Declared by the Minister if it relates to a relevant industry or affects national security*

2020 Amendment expands CI definition:

- *communications*
- *data storage and processing*
- *defence*
- *financial services and markets*
- *food and grocery*
- *health care and medical*
- *transport*
- *higher education and research*
- *energy*
- *space technology*
- *water and sewerage*

“The Security of Critical Infrastructure Act 2018 (the Act) seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure.” -- Department of Home Affairs (2020)

Three key elements of the act

- A register of critical infrastructure assets
- An information gathering power
- A Ministerial directions power

The screenshot shows the Australian Government Department of Home Affairs website. At the top, there is a navigation bar with a 'Menu' icon, the Australian Government logo, and a search icon. Below the navigation bar, a blue banner displays the text 'Australian Government COVID-19 travel restrictions and information for visa holders'. A breadcrumb trail below the banner reads: 'Home → About us → Our functions → National security → Security coordination'. The main content area is titled 'Security coordination' and 'Security of Critical Infrastructure Act 2018'. On the left, a sidebar lists various links under the 'Security coordination' heading: 'Critical infrastructure resilience', 'Five Country Ministerial 2018', 'Five Country Ministerial 2020', 'National Security Hotline', 'National security powers', 'Reform of ASIO's questioning powers', and 'Register of Critical Infrastructure Assets'. The main content area features a list of links: 'About the Act', 'Annual reports', 'Free trade agreement obligations', 'Safeguards', 'Protection from penalties', and 'Moneylenders'. Below this, a section titled 'About the Act' contains a paragraph about the 'Protecting Critical Infrastructure and Systems of National Significance' and mentions the 'Security Legislation Amendment (Critical Infrastructure) Bill 2020'.

Enhanced Cyber Security Obligations

- Incident Response Plan
- Cyber Exercises
- Vulnerability Assessments
- Access to System Information

Positive Security Obligation

- Notification of cyber security incidents
- 12 hours if having a significant impact on the availability of the asset; or,
- 72 hours if having a relevant impact on the availability, integrity, reliability or confidentiality of the asset.

The screenshot shows the official website of the Australian Government Department of Home Affairs. The header includes the Australian Government crest and the department's name. A blue banner at the top contains a link to 'Australian Government COVID-19 travel restrictions and information for visa holders'. Below the banner is a breadcrumb trail: Home → About us → Our functions → National security → Security coordination. The main content area is titled 'Security Legislation Amendment (Critical Infrastructure) Bill 2020' and includes a sub-header 'Protecting Critical Infrastructure'. The text states that the bill was introduced into Parliament on 10 December 2020 and explains that critical infrastructure is essential for Australia's economic prosperity and way of life, including electricity, communications, transport, and banking. It also notes that interconnectedness of critical infrastructure creates vulnerabilities without proper safeguards.

Menu

Australian Government
Department of Home Affairs

[Australian Government COVID-19 travel restrictions and information for visa holders](#)

Home → About us → Our functions → National security → Security coordination

Security coordination

- Critical infrastructure resilience
- Five Country Ministerial 2018
- Five Country Ministerial 2020
- National Security Hotline
- National security powers

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Protecting Critical Infrastructure

The [Security Legislation Amendment \(Critical Infrastructure\) Bill 2020](#) was introduced into Parliament on 10 December 2020.

All Australians rely on critical infrastructure to deliver essential services that are crucial to our economic prosperity and our way of life, such as electricity, communications, transport and banking.

Critical infrastructure is increasingly interconnected and interdependent. Connectivity without proper safeguards creates significant vulnerabilities. Interconnectedness

What is a Cyber Crime?



Australian Government

Federal Register of Legislation


- Computer intrusions
- Unauthorised modification of data, including destruction of data
- Unauthorised impairment of electronic communications, including denial of service attacks
- The creation and distribution of malicious software (for example, malware, viruses, ransomware)
- Dishonestly obtaining or dealing in personal financial information.

<https://www.legislation.gov.au/Details/C2019C00043>

[Home](#)[What's new](#)[Constitution](#)[Acts](#)[Legislative instruments](#)[Notifiable instruments](#)[Gazettes](#)[Bills](#)[Other](#)[Feedback](#)

[Text](#)[Download](#)[Buy print copy](#)

Criminal Code Act 1995

 - C2019C00043
In force - Superseded Version
[View Series](#)

[DETAILS](#)[EXPAND](#)

TABLE OF CONTENTS.

[Expand All](#) | [Collapse All](#)

- [Volume 1](#)
- [Volume 2](#)
 - [Schedule—The Criminal Code](#)
 - [Chapter 8—Offences against humanity and related offences](#)
 - [Chapter 9—Dangers to the community](#)
 - [Chapter 10—National infrastructure](#)
 - [Part 10.2—Money laundering](#)
 - [Part 10.5—Postal services](#)
 - [Part 10.6—Telecommunications Services](#)
 - [Part 10.7—Computer offences](#)
 - [Part 10.8—Financial information offences](#)
 - [Part 10.9—Accounting records](#)
 - [Dictionary](#)

Other definitions in different jurisdictions (US, SG, LK)

United States of America, Patriot Act of 2001, **Critical Infrastructure** is defined as:

“systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”

<https://www.congress.gov/bill/107th-congress/house-bill/3162>

Singapore, Cybersecurity Act, Section 7(1):

*“a **Critical Information Infrastructure** is a computer or a computer system located wholly or partly in Singapore, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore.”*

https://www.ifaq.gov.sg/csa/apps/fcd_faqlmain.aspx

Sri Lanka, Cyber Security Bill 2019, Section 17:

An institution is said to have **Critical Information Infrastructure**:

“(a) the disruption or destruction of the computer system or computer program would have serious impact on the national security, public health, public safety, confidentiality, or economic well-being of citizens, or the effective functioning of the government or the economy of Sri Lanka; and

(b) the computer program or the computer system is located wholly or partly in Sri Lanka.”

<https://www.cert.gov.lk/documents/Cyber%20Security%20Bill.pdf>