|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Region**  **\*divided by UN geoscheme** | **Country**  **/ regional entity** | **How infrastructure is defined?** | **What is designated as critical infrastructure?** | **Source** |
| Americas | Argentina | In Sept 2019, Argentina passed a resolution which defined and designated CI and CII  *Critical Infrastructures are* ***those that are essential for the proper functioning of essential services*** *of society, health, safety, defense, social welfare, the economy and the effective functioning of the State, whose destruction or disturbance, total or partial, affects and/or impacts them significantly.*  *Critical Information Infrastructures are information technologies, operation and communication, as well as the associated information, which are vital for the operation or security of Critical Infrastructures.* | • Energy  • Information and Communications Technologies  • Transport  • Water  • Health  • Food  • Finance  • Nuclear  • Chemical  • Space  • State | Resolution 1523/2019:  <https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1523-2019-328599/texto>  Definition and designation is in Annex:  <https://www.argentina.gob.ar/sites/default/files/infoleg/res1523-1.pdf>  Further relevant definitions:  <https://www.argentina.gob.ar/sites/default/files/infoleg/res1523-2.pdf> |
| Americas | Brazil | Decree No. 9,573 of 22 November 2018 approved the National Critical Infrastructure Security Policy (PNSIC), which defines **critical infrastructures as facilities, services, goods and systems** whose interruption or destruction, in whole or in part, would have a serious social, environmental, economic, political, international or security impact on the state and society. Likewise, it characterises critical infrastructure security as a set of preventive and reactive measures designed to preserve or restore the **provision of services** related to critical infrastructures. | • Water  • Energy  • Transport  • Communications  • Finance  • Biosafety and Bioprotection  • Defense | National Policy and security of critical infrastructure:  <https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic>  <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>  National strategy on security of critical infrastructure:  <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm>  National security plan of critical infrastructure:  <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm> |
| Americas | Canada | Critical infrastructure (CI) 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 government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence. | 1. Water 2. Safety 3. Health 4. Finance 5. Transportation 6. Energy and utilities 7. Food 8. Manufacturing 9. Government 10. Communication technology | Public Safety Canada – Canada’s Critical Infrastructure  <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx>  National Strategy for Critical Infrastructure:  <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf> |
| Americas | Chile | Chile passed in December 2023 a Framework Law on Cybersecurity and Critical Information Infrastructure, establishing a national cybersecurity agency.  Scope of the law:  Requires public and private entities that qualify as Providers of Essential Services and those that, in addition to providing Essential Services, are qualified as Operators of Vital Importance (OIV) by the new National Cybersecurity Agency. | To be defined by the new Cybersecurity Agency. | Chile Framework Law on Cybersecurity and Critical Information Infrastructure:  <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06> (Approved in December 2023) |
| Americas | Colombia | (2022) Defines Critical Cyber Infrastructure: Systems and assets, physical or virtual, supported by Information and Communication Technologies, whose significant affectation would have a serious impact on the social or economic well-being of citizens, or on the effective functioning of the government or the economy.  **It establishes security obligations for authorities owning critical infrastructure, or providing essential services.** The authorities, defined as holders of critical infrastructure or providing essential services, shall endeavour to have a digital security plan, protection of networks, critical cyber infrastructures, essential services and information systems in cyberspace and shall periodically carry out a digital security risk assessment. To this end, they must have the necessary rules, policies, procedures, technical, administrative and human resources to effectively manage the risk, and in compliance with the best practices and standards that may be required. | No defined sectors. | Government of Colombia normative paper on critical infrastructure: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866> |
| Americas | United States of America | The National Institute of Standards and Technology (NIST) defines critical infrastructure as ‘system 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’. | 1. Chemical sector 2. Commercial facilities sector 3. Communications sector 4. Critical manufacturing sector 5. Dams sector 6. Defense industrial base sector 7. Emergency services sector 8. Energy sector 9. Financial services sector 10. Food and agriculture sector 11. Government facilities sector 12. Healthcare and public health sector 13. Information technology sector 14. Nuclear reactors, materials and waste sector 15. Transportation systems sector 16. Water and wastewater systems | NIST  [critical infrastructure - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/critical_infrastructure)  Cybersecurity and infrastructure security agency – critical infrastructure sectors:  [Critical Infrastructure Sectors | CISA](https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors) |
| Asia | Taiwan | The Executive Yuan in Taiwan has promulgated the Guidelines for National Critical Infrastructure Security Protection ("Guidelines") and defined Critical Infrastructure ("CI") as "public or private, physical or virtual assets, production systems, and networks that, if damaged by human or natural causes, can affect the functioning of government and society, causing loss of life or property, economic recession, environmental changes, or other threats to national security or interests."  Additionally, the Executive Yuan recognizes the information and communication systems and supervisory control and data acquisition (SCADA) systems that are essential for supporting the continuous operation of CI as "Critical Information Infrastructure," which should be managed along with the corresponding CI.  To protect the operation of CI, Cyber Security Management Act ("CSMA") of Taiwan obligates, among others, specific CI providers to adopt cybersecurity maintenance plans and report any cyber security Incident to the relevant government authorities.  Pursuant to Article 3 of the CSMA, CI is defined as an "asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities."  That being said, the specific CI and CI providers within the CSMA's purview are subject to the Executive Yuan's announcement and regular re-examination, according to Article 3 of the CSMA. | The Guidelines elaborated on CIs based on the following structures:   1. Sector: Divided by functionality, there are eight main sectors: energy, water resources, communication and broadcasting, transportation, finance, emergency rescue and hospitals, government agencies, and science parks and industrial parks. 2. Subsector: The sectors are further divided into subsectors according to their respective functional business areas. For instance, subsectors of the energy sector include electricity, oil, natural gas, and so on. 3. Functional facilities and systems under the subsectors: This refers to the facilities, equipment, transportation networks, information and communication systems, control systems, monitoring systems, security systems, and key technologies necessary to maintain important functional operations in the subsectors.   However, it is worth mentioning that the designation of the CI providers under the CSMA is kept confidential by the government authorities. Therefore, we are unable to identify the specific CI and CI providers in accordance with the regulations of the CSMA. | Guidelines: <https://ohs.ey.gov.tw/File/EF5E72C88077DE72> (Traditional Chinese version only)  CSMA:  <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297> |
| Asia | India | As per IT Act 2000 (amended 2008), Critical Information Infrastructure (CII) means ‘Computer Resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety’. | 1. Telecommunications 2. Power and energy 3. Banking and financial services 4. Transportation 5. Strategic entities 6. Government enterprises 7. Healthcare | Bank Info Security – India to Launch Critical Infrastructure Security Framework:  <https://www.bankinfosecurity.asia/india-to-launch-critical-infrastructure-security-framework-a-22282>  The Information Technology Act of 2000:  <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C> |
| Asia | Singapore | Under section 7(1) of the Cybersecurity Act, 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. | 1. Energy 2. Water 3. Banking and finance 4. Healthcare 5. Transport (including land, maritime, and aviation) 6. Infocomm 7. Media 8. Security and emergency service 9. Government | Cybersecurity Act Overview  <https://www.csa.gov.sg/faq/cybersecurity-act>  Cybersecurity Act, Critical Infrastructure:  <https://www.csa.gov.sg/legislation/Cybersecurity-Act#:~:text=The%20CII%20sectors%20are%3A%20Energy,and%20Emergency%20Services%2C%20and%20Government>. |
| Africa | Ghana | Critical Information Infrastructure (CII) constitutes assets (real/virtual), networks, systems, processes, information, and functions that are vital to the nation such that their incapacity or destruction would have a devastating impact on national security, the economy, public health and/or safety. CII may comprise a number of different infrastructures with essential interdependencies and critical information flows between them. The Cybersecurity Act, 2020 (Act 1038) defines a critical information infrastructure as a computer system or computer network that is essential for national security or the economic and social well-being of citizens. | 1. National security and intelligence 2. Information and communication technology 3. Banking and finance 4. Energy 5. Water 6. Transport 7. Health 8. Emergency services 9. Government 10. Food and agriculture 11. Manufacturing 12. Mining 13. Education | Directive for the Protection of Critical Information Infrastructure:  <https://www.csa.gov.gh/resources/Directive_CII.pdf>  Cybersecurity Act of 2020:  <https://www.csa.gov.gh/resources/cybersecurity_Act_2020(Act_1038).pdf> |
| Africa | South Africa | Requirements for declaration of infrastructure as critical infrastructure: Infrastructure qualifies for declaration as critical infrastructure, if­ (a)   the functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and (b)   the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice­ (i)   the functioning or stability of the Republic; (ii)   the public interest with regard to safety and the maintenance of law and order; and (iii)   national security. | No defined sectors, critical infrastructures are based off the definition. | Critical Infrastructure Protection Act of 2019:  <https://static.pmg.org.za/Critical_Infra_Protection_Act8of2019.pdf>  Cybersecurity Water Policy and the Legislative Context of the Water and Wastewater Sector in South Africa:  <https://www.mdpi.com/2071-1050/13/1/291> |
| Europe | European Union | In Europe, there are two main directives focusing on the protection of critical infrastructure and essential services, and some specialised approaches such as the one focused on the financial sector, all approved at the same time to seek coherence.  The Critical Entities Resilience (CER) Directive lays down obligations to take specific measures, to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market.  Moved from assets to critical entities providing essential services with Directive 2022/2557:  *Critical entities provide essential services in upholding key societal functions, supporting the economy, ensuring public health and safety, and preserving the environment.*  However exact critical entities are defined by member states:  *Member States will have to identify the critical entities for the sectors set out in the Critical Entities Resilience (CER) Directive by 17 July 2026. They will use this list of essential services to carry out risk assessments and to then identify the critical entities. Once identified, the critical entities will have to take measures to enhance their resilience*. | **List of essential services & sectors**   1. **Energy sector,** with services such as the electricity production and energy storage; 2. **Transport sector,** with services such as management and maintenance of airport or railways infrastructure; 3. **Banking sector,** with essential services such as taking deposits and lending; (This sector has an additional specific regulation on cybersecurity) 4. **Financial market infrastructure sector,** with services such as the operation of trading venue and of clearing systems; 5. **Health sector**, with distribution, manufacturing, provision of healthcare, and medical services; 6. **Drinking water sector**, with drinking water supply and drinking water distribution; 7. **Waste water sector,** with waste water collection, treatment and disposal services; 8. **Digital infrastructure sector**, with services such as public electronic communications networks and services, the provision and operation of internet exchange point service, domain name system, top-level domain, cloud computing and data centre; 9. **Public administration sector** services; 10. **Space sector,** with the operation of ground-based infrastructure services; 11. **Production, processing and distribution of food sector,** with the large-scale industrial food production and processing, food supply chain services and food wholesale distribution services. | Critical Entites Resilience (CER) Directive:  <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557>  Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2) https://eur-lex.europa.eu/eli/dir/2022/2555/oj  Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA)  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 |
| Europe | United Kingdom | Not everything within a national infrastructure sector is judged to be 'critical'. The UK government's official definition of CNI is:  *'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*  *a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or*  *b) Significant impact on national security, national defence, or the functioning of the state.'* | 1. Chemicals 2. Civil Nuclear 3. Communications 4. Defence 5. Emergency Services 6. Energy 7. Finance 8. Food 9. Government 10. Health 11. Space 12. Transport 13. Water | National Protective Security Authority- Critical National Infrastructure:  <https://www.npsa.gov.uk/critical-national-infrastructure-0> |
| Oceania | Australia | The 2023 Critical Infrastructure Resilience Strategy defines 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 the social or economic wellbeing of the nation, or affect Australia’s ability to conduct national defence and ensure national security.*  *Each class of critical infrastructure asset is defined by the Security of Critical Infrastructure Act 2018. A single critical infrastructure asset includes multiple parts such as premises, computers, and data, which function together as a system or network.*  *If multiple components operate as a single system or network that meets the definition of a critical infrastructure asset, they are considered a single asset.*  *If components operate as separate systems or networks that each meet the definition of a critical infrastructure asset, they are considered separate assets.* | 1. Communications 2. Financial services and markets 3. Data storage and processing 4. Defence 5. Higher education and research 6. Energy 7. Food and grocery 8. Healthcare and medical 9. Space technology 10. Transport 11. Water and sewerage | Critical Infrastructure Resilience Strategy: <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf> |