The Protection of Critical Infrastructure Against Terrorist Attacks

COMPENDIUM OF GOOD PRACTICES

2022 UPDATE

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

INTERPOL

The Protection of Critical Infrastructure Against Terrorist Attacks

Compendium of Good Practices
2022 Update

Preface

Terrorists have increasingly been exploiting vulnerabilities in the public and private utilities of almost all sectors, including those of transport and energy, and also water infrastructure and nuclear facilities. Critical infrastructure has become a prime objective of terrorist attacks across the world. The interdependencies and interconnected nature of critical infrastructure located across borders raise additional concerns and require bilateral or regional responses. The objective of terrorists is well known: to destroy the way in which we live, tear apart the fabric of our societies and sow division.

While large-scale terrorist attacks against critical infrastructure with significant cascading effects have not yet occurred, the threat posed by such a scenario remains persistent and requires countries to put in place adequate prevention, response and resilience measures.

The Compendium of Good Practices on the protection of critical infrastructure against terrorist attacks, first published in 2018 and updated in 2022, was designed to provide Member States, practitioners, civil society, international and regional organizations, academia, the private sector and all relevant stakeholders with appropriate good practices, tools and case studies from across the world to support the efforts of Member States to protect their critical infrastructure.

The General Assembly and the Security Council have been paying close attention to this topic for a number of years. In the United Nations Global Counter-Terrorism Strategy, under Pillar II on measures to combat and prevent terrorism, Member States resolved to "step up all efforts to improve the security and protection of particularly vulnerable targets, such as infrastructure and public places, as well as the response to terrorist attacks and other disasters, in particular in the area of civil protection, while recognizing that States may require assistance to this effect".

In addition to the more general calls to prevent this threat included in resolutions 1373 (2001) and 1566 (2004), the Security Council adopted resolution 2341 (2017), which was the first global instrument fully devoted to the importance of safeguarding critical infrastructure from terrorist attacks. More specifically, in the resolution the Council recalled its decision in resolution 1373 (2001) that all States should establish terrorist acts as serious criminal offences in domestic laws and regulations and called upon all Member States to ensure that they had established criminal responsibility for terrorist attacks intended to destroy or disable critical infrastructure, as well as the planning of, training for, and financing of and logistical support for such attacks.

In resolution 2396 (2017), the Security Council acknowledged that the Islamic State in Iraq and the Levant (ISIL), also known as Da'esh, had called on its supporters and affiliates, especially terrorist fighters leaving armed conflict zones, to plan and carry out attacks on public places and utilities. In that resolution, the Council stressed the need for States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against "soft" targets.

Since this Compendium was first published, the United Nations and its Member States have been continuing their work to strengthen international cooperation in countering terrorism and tackling terrorist threats against critical infrastructure.

Where the Security Council is concerned, in 2018, the Counter-Terrorism Committee published an addendum to the 2015 Madrid Guiding Principles, which highlights the importance of the protection of vulnerable targets, as called for in principles 50 and 51. In addition, Security Council resolution 2617 (2021) adopted in December 2021 also includes specific provisions on the protection of critical infrastructure and so-called "soft" targets as part of the new mandate of the Counter-Terrorism Committee Executive Directorate and recognized the crucial importance of cooperation with the Office of Counter-Terrorism in this area.

In June 2021, during the seventh review of the United Nations Global Counter-Terrorism Strategy, Member States agreed by consensus that the protection of vulnerable targets should be a priority in our common action against terrorism. General Assembly resolution 75/291 included two preambular and four operational paragraphs on this topic, stressing the need to bring together all relevant stakeholders—Member States, international and regional organizations, the private sector, civil society and academia—to address effectively the unprecedented threat posed by terrorist attacks to critical infrastructure and soft targets.

Over the past four years, Member States have also been very active in adapting their legal, institutional and operational frameworks to the protection of critical infrastructure. This Compendium will demonstrate to readers the speed at which the critical infrastructure protection landscape has been changing.

The Global Programme on Countering Terrorist Threats against Vulnerable Targets, jointly implemented by the Office of Counter-Terrorism, the Counter-Terrorism Committee Executive Directorate, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Alliance of Civilizations, in collaboration with the International Criminal Police Organization (INTERPOL), has been supporting Member States since 2021 in building their capacities, developing connections between experts and identifying good practices for the protection of critical infrastructure.

We are certain that this updated Compendium, made possible thanks to the generous funding of the State of Qatar to the Global Programme, will become a seminal tool in this area, to the benefit of all Member States and their citizens.

Vladimir Voronkov
Under-Secretary-General
Office of Counter-Terrorism

Weixiong Chen
Acting Executive Director
Counter-Terrorism Committee
Executive Directorate

Foreword

We are reminded daily of the threat that terrorists pose to the international community and to our collective prosperity, safety and security. The ability of these entities to cause harm increases exponentially when their activities target critical infrastructure (CI), such as that housing chemical, biological, radiological and nuclear (CBRN) materials, or vulnerable targets, such as public places, utilities and the Internet.

The International Criminal Police Organization (INTERPOL) and the global law enforcement community, in collaboration with all partners gathered within the United Nations Global Counter-Terrorism Coordination Compact, are committed to identifying priority terrorist threats to our countries and to countering them head on. Combating terrorism must be a collective and collaborative effort and the global community needs more than ever to work in partnership to leverage its respective mandates and expertise.

With this in mind, the Working Group on Emerging Threats and Critical Infrastructure Protection, chaired by INTERPOL, contributed to the original production of this compendium of good practices for the protection of CI against terrorist attacks, and now to its 2022 update.

The Compendium, generously sponsored by the Office of Counter-Terrorism and continuously supported by the Counter-Terrorism Committee Executive Directorate, provides policymakers and regional and national authorities with guidelines on good practices for the protection of CI. The Compendium focuses on indicators, standards, risk assessment measures and relevant recommendations, and provides countries with reference material for the development of proactive strategies to reduce terrorism-related risks to CI.

Countering terrorism requires a whole-of-society approach. Together, we continue to identify and address changes in the terrorism threat landscape. Accordingly, those of us involved in the collaborative approach followed in the preparation of this Compendium hope that this document will support you in addressing current and future CI threats. Together, let us pursue sustainable collective efforts in detecting, deterring and disrupting terror at its source.

Stephen Kavanagh
Executive Director, Police Services
INTERPOL

Contents

Boxes

Case studies

Tools

Tables

Abbreviations and acronyms

ABC	automated border control systems (ICAO)
AFS	aeronautical fixed service
AIS	automated indicator sharing (CISA)
API	advance passenger information (ICAO)
ASEAN	Association of Southeast Asian Nations
ASIO	Australian Security Intelligence Organisation
BCN	biological, chemical and nuclear
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (Regulation on the Identification of Critical Infrastructure)
CBRN	chemical, biological, radiological and nuclear
CBRNE	chemical, biological, radiological, nuclear and explosives
CI	critical infrastructure
CI3-T	Integrated Centre for Counter-Terrorism Information and Intelligence–Colombia
CII	critical information infrastructure
CIIP	critical information infrastructure protection
CISA	Cybersecurity and Infrastructure Security Agency (United States)
CNI	critical national infrastructure
CNPIC	National Centre for Infrastructure Protection and Cybersecurity (Spain)
COVID-19	coronavirus disease
CPNI	Centre for the Protection of National Infrastructure (United Kingdom)
CTEPs	CISA tabletop exercise packages (United States)
CTITF	United Nations Counter-Terrorism Implementation Task Force
CTPN	Counter Terrorism Preparedness Network
DoS attacks	denial of service attacks
DTC	digital travel credentials (ICAO)
ECOWAS	Economic Community of West African States
EFTA	European Free Trade Association
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation (United States)
GFCE	Global Forum on Cyber Expertise
GHS	Globalized Harmonized System of Classification and Labeling of Chemicals
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICT	information and communications technology
IED	improvised explosive device
INTERPOL	International Criminal Police Organization

IOM	International Organization for Migration
ISO	International Organization for Standardization
ISIL	Islamic State in Iraq and the Levant
ISPS Code	International Ship and Port Faciilty Security Code
ITU	International Telecommunication Union
NIS	network and information systems
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OPCW	Organization for the Prohibition of Chemical Weapons
OSCE	Organization for Security and Cooperation in Europe
PKD	Public Key Directory (ICAO)
PPPs	public-private partnerships
SARPs	Standards and Recommended Practices (ICAO)
SOLAS Convention	Safety of Life at Sea Convention
TETRA	terrestrial trunked radio
UAS	unmanned aircraft system
UNICRI	United Nations Interregional Crime and Justice Research Institute
UAS	unmanned aircraft system
USAID	United States Agency for International Development
WHO	World Health Organization
WMD	weapons of mass destruction

Introduction: context, objectives and methodology

This Compendium addresses a topic that is still, to a large extent, in its infancy. The pace at which modern economies have become inextricably interconnected over the past two decades, especially through the great strides made by information and communications technology (ICT), has exposed our societies to a set of unprecedented threats and vulnerabilities. Many of these derive from terrorist groups that seek to destabilize communities and create widespread panic by disrupting the very assets and processes on which our societies depend for their survival. These assets and processes are central nodes known as "critical infrastructure" (CI).

The growing awareness that we are now confronted with a new type of security environment, however, has not been matched by corresponding levels of preparedness. Nevertheless, recent attacks on transport systems, repeated acts of sabotage against dams, oil pipelines, telecommunication networks and other facilities are a fresh reminder of the keen interest that terrorist groups of different affiliations have in targeting the infrastructure through which a range of essential services are provided.

It was in this context that the Security Council adopted its resolution 2341 (2017) as the first ever global instrument entirely devoted to the protection of CI against terrorist attacks. Its provisions reflect the determination of the international community to elaborate and upgrade the mechanisms needed to minimize risks to CI caused by terrorist attacks, and to ensure an adequate response to and recovery from such attacks.

In view of the renewed interest in CI protection and resilience and the urgent need for Member States to implement resolution 2341 (2017), in 2018 the Office of Counter-Terrorism and the Counter-Terrorism Committee Executive Directorate developed the first edition of the Compendium of Good Practices for the Protection of Critical Infrastructure Against Terrorist Attacks.[1] The Compendium was conceived as a practical tool to support a wide range of entities (from policymakers to law-enforcement authorities and private-sector stakeholders) with varying degrees of responsibility for designing and implementing the policies and measures needed to give effect to resolution 2341 (2017). Following its release, the Compendium has been used as a leading source of information and good practices and also as a tool to guide discussions at several regional meetings of experts in various parts of the world.[2]

This publication represents an updated and expanded version of the Compendium, which takes account of developments that have taken place since 2018 that are conducive to a broader understanding of the threats posed, the new legal and policy tools available and the fresh steps being taken by countries to tackle the problem. All information included in the 2018 edition has been double-checked for continued relevance. New material (policy and strategic documents, legal instruments, cases studies and tools) have been added through a new round of desk research and expert exchanges via the Connect and Learn Platform of the United Nations Global Network of Experts on the Protection of Vulnerable Targets against Terrorist Attacks. Moreover, a number of Member States have provided information in response to a note verbale circulated to Member States on 2 March 2022 requesting them "to share their good practices on critical infrastructure

[1] The first (2018) edition of the Compendium was developed in the framework of the INTERPOL-chaired working group of the Counter-Terrorism Implementation Task Force on the "protection of critical infrastructure including vulnerable targets. In 2019, the Task Force was folded into the United Nations Global Counter-Terrorism Coordination Compact. Under this new structure, both the Task Force's working groups on the protection of critical infrastructure including the Internet, vulnerable targets and tourism security and on preventing and responding to weapons of mass destruction terrorist attacks were combined to create the Compact's working group on emerging threats and critical infrastructure protection (ETCIP Working Group). The new (2022) edition of the Compendium was developed under the auspices of the ETCIP Working Group.

[2] Casablanca, Morocco (November 2018), Tunis (April 2019), Singapore (January 2019) and Johannesburg, South Africa (November 2019).

protection", including "national and regional good practices, strategies, plans of action, frameworks, tools, case studies, manuals and guidance notes with a focus on critical infrastructure protection."

In line with the 2018 version, the new edition of the Compendium is arranged in thematic blocks which broadly follow the structure of resolution 2341 (2017). Each chapter is introduced by one or more operative paragraphs taken from relevant instruments and includes a background analysis of the issues under consideration. Care has been taken not to presume previous knowledge of CI-related concepts on the part of the reader. This approach stems from recognition that the notion of "critical infrastructure protection" is a relatively new addition to the global public policy discourse.

The underlying practical and legal challenges faced by States are examined from the perspective of current and potential solutions being adopted by individual Governments, international agencies, private-sector entities and civil society organizations. The pragmatic approach followed in the Compendium is illustrated by the wealth of case studies that provide specific examples and implementation options. A number of tables have been added to enable countries to make a rapid comparison of measures being adopted by other countries and ultimately help them to shape the responses that best fit their own institutional context.

A novelty of the new edition of the Compendium is that it integrates a number of specialized thematic modules – as addenda – focusing on the protection of so-called "soft targets".[3] In doing so, the Compendium seeks to expand the understanding of critical infrastructure protection efforts by identifying the points of contact with a specific type of vulnerable sites (soft targets) and encouraging countries to develop synergies between policies and operational measures in both areas.[4]

Although the Compendium focuses on the protection of CI from terrorist attacks, it recognizes that a number of Member States have chosen to adopt broad strategies that take into account the need to enhance CI resilience against all hazards, whether human-made or natural. In the light of this recognition, the Compendium provides the conceptual tools to enable Member States to adopt, if they so wish, all-encompassing strategies paying special attention to the terrorist threat and related assessment and mitigation mechanisms.

In line with resolution 2341 (2017), the Compendium deals with CI without focusing on any specific infrastructure type. This transversal approach aims to highlight the common principles, processes and methodologies that Member States are encouraged to translate into tangible strategies, actions plans and measures. At the same time, examples of sector-specific mitigation measures are offered throughout the document. In addition, chapter 9 provides an overview of the main initiatives taken by leading international agencies in selected sectors.

Lastly, in providing guidance to Member States, the Compendium supports the principle that human rights and gender issues shall be given due consideration and be effectively mainstreamed into all CI protection measures and related strategies.

[3] The four sector-specific modules are introduced by a general module and deal with the protection of religious and tourist sites, urban centres and the threats posed by unmanned aircraft systems.

[4] The Compendium and its related modules follow the terminological approach adopted by the General Assembly on the occasion of the seventh review of the United Nations Global Counter-Terrorism Strategy. Resolution 75/291, in particular, views "soft targets" as one of two subsets of vulnerable targets, the other being "critical infrastructure".

1. Understanding the challenge

Security Council resolution 2341 (2017)

The Security Council

...

1. *Encourages* all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure

Addendum to the guiding principles on foreign terrorist fighters (Madrid Guiding Principles)

Guiding principle 50

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

(a) Identify, assess and raise awareness of the relevant risks and threats of terrorist attacks on critical infrastructure and soft targets

1.1 Terrorism as a distinctive threat to CI

While CI has always been exposed to multiple hazards, including natural events, human error, technical failure and criminal acts in a broad sense, the emergence of CI protection as a distinctive policy area was a direct consequence of the events of 11 September 2001.

Over the past few decades, terrorists have regularly shown interest in CI as targets to advance their goals. As early as 2002, there were already clear indications that Al-Qaida was seeking to exploit vulnerabilities in United States public and private utilities. The discovery in Afghanistan of a computer containing structural analysis programs for dams prompted the United States National Infrastructure Protection Center to issue an information bulletin giving warning of the danger.[5]

Crucially, hardly any sector has escaped from terrorist activity or at least sustained attention on the part of terrorist groups. On a number of occasions, CI has been targeted with the specific goal of disrupting the delivery of essential services and thereby causing negative impacts on local or global communities.[6] Examples abound.

The energy sector has witnessed sustained terrorist activity through attacks perpetrated by Al-Qaida and affiliates on the facilities and staff of oil companies in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen. As case study 1 shows, the increasingly frequent terrorist attacks on energy infrastructure recorded between 1970 and 2011 have emerged as one of the major causes of energy disruption, with consequences for all countries in the entire energy supply chain.

5 See http://lists.jamed.com/crime/2002/01/0055.html.

6 In other cases, terrorist attacks or plans involving CI have not been carried out with the specific objective of hampering CI operations themselves, but rather to maximize civilian casualties by exploiting the presence of large crowds of people within or around CI. The transport sector has been particularly hit by this type of terrorist activity, starting with the sarin attack on the Tokyo metro in 1995. Another example is the 2016 simultaneous attacks on Brussels airport and metro system by two teams of Da'esh operatives. Overall, 32 people were killed and some 300 were injured.

Box 1
Terrorist threats and CI: nature and impacts on the energy sector

A study on terrorist attacks perpetrated globally against energy infrastructure between 1970 and 2011[7] has concluded that:

- The increasing frequency of terrorist attacks on energy infrastructure in the period under consideration has emerged as one of the major causes of energy disruption, with consequences for all countries in the entire energy supply chain.
- In today's globalized world, all countries, including producer countries, have become interdependent in terms of their energy security. Terrorists can achieve global impacts with minimal efforts. For this reason, any interruption to the aforementioned systems or infrastructure network could potentially affect the entire energy supply chain.
- Electricity disruption can be caused not only by attacks on large-scale energy infrastructure facilities such as oil terminals, refineries and pipelines, which are often the focus of media attention, but also by attacks on minor targets such as electrical transformers or high-tension lines.
- The ten countries that were exposed to the greatest number of energy infrastructure attacks in the period under consideration were Angola, Chile, Colombia, El Salvador, Iraq, Pakistan, Peru, Philippines, South Africa and Spain. These countries were victims of 3,801 out of the 4,653 incidents of energy infrastructure attacks experienced worldwide, accounting for 82 per cent of all recorded attacks.
- Terrorist attacks not only target energy facilities in producing countries such as Angola, Colombia and Iraq, but also in transit countries such as Afghanistan, Pakistan and Türkiye, and in consumer countries such as El Salvador, Peru and Spain. Wherever there is insurgency, political unrest or civil war, energy infrastructure seems an important target owing to the immediate impact of such attacks. It is therefore vital for Governments to include this issue in their energy policymaking, especially in risk management strategies.
- There is a general tendency in all countries for terrorist organizations to favour attacks of the bombing or explosive type, which is responsible for 4,177, or 90 per cent, of the 4,653 attacks. This demonstrates the very strong preference for this method of attack on energy infrastructure.

Most recently, the Office of Intelligence and Analysis of the United States Department of Homeland Security issued an alert to the electric sector following requests from power companies to take stock of increased threats from domestic violent extremists (also referred to as "DVEs") in 2020 and 2021. According to the Department of Homeland Security, "DVEs have developed credible, specific plans to attack electricity infrastructure since at least 2020, identifying the electric grid as a particularly attractive target given its interdependency with other infrastructure sectors."[8]

Threats against energy infrastructure have also materialized in the form of unmanned aircraft systems (sometimes referred to as "UAS"). According to a Joint Intelligence Bulletin from the Department of Homeland Security, the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center, on 16 July 2020, a small, four-rotor off-the-shelf drone was discovered on the top of a building next to a power substation. Nylon ropes hanging from the drone dangled a two-foot curved piece of copper wire, and analysis of the device indicated that this was likely intended to short circuit the substation, in the first known instance of a modified unmanned aircraft system apparently being used in the United States specifically to target energy infrastructure. The operator of the drone still has not been identified; the system's camera, memory storage card, and all identifiable markings had been removed, indicating that the operator was trying to avoid identification and was also in all probability within visual line of sight of the intended target while flying the drone.[9]

Key water infrastructure has been the object of special attention on the part of Da'esh. Between 2013 and 2015, Da'esh launched some 20 major attacks against Syrian and Iraqi targets. In addition to destroying pipes, sanitation plants and bridges, Da'esh has used water infrastructure strategically, for example by closing dams and cutting off water supplies.[10]

---

7 Mehmet Biresselioglu and Isik Yumurtaci, "Evaluating the nature of terrorist attacks on the energy infrastructure: The periodical study for 1970-2011", *International Journal of Oil Gas and Coal Technology*, vol. 10, No. 3, pp. 325–341 The study considers a wider range of events, including minor-scale ones. The underlying reasoning is that minor attacks are equally likely to cause a disruption in energy supply, and thus undermine the availability and accessibility of existing energy services, directly affecting domestic use and industrial productivity. Data for the study were retrieved from the target type of utilities from the Global Terrorism Database, an open-source database managed by the University of Maryland and including information on terrorist events around the world. The study is available at www.researchgate.net/publication/282446687_Evaluating_the_nature_of_terrorist_attacks_on_the_energy_infrastructure_The_periodical_study_for_1970-2011.

8 See https://www.thedailybeast.com/dhs-warns-that-right-wing-extremists-could-attack-power-grid.

9 See https://www.hstoday.us/featured/physical-attacks-on-electricity-infrastructure-extremist-messaging-plots-and-action/.

10 See https://worldview.stratfor.com/article/water-wars-waged-islamic-state.

In February 2021, an unidentified computer hacker attempted to poison the water supply of a city in Florida by remotely increasing the amount of sodium hydroxide.

The telecommunications sector has also been targeted. For example, in 2012, Boko Haram mounted a coordinated two-day attack on telecom infrastructure belonging to several operators across five cities in northern Nigeria. This example is interesting as Boko Haram appears to have drawn inspiration for this attack from similar acts perpetrated by terrorist groups in Afghanistan a few years earlier, suggesting that, in the CI domain, terrorist groups active in different parts of the world are ready and willing to imitate one another in terms of their chosen targets and attack methodologies.

In some cases, terrorist attacks have been perpetrated on infrastructure containing dangerous materials. On 26 June 2015, an individual crashed a car through the site of a chemical plant near Lyon and into gas canisters, provoking an explosion. In 2016, two nuclear power plants in Belgium were locked down under suspicion of an attempt by Da'esh to attack, infiltrate or sabotage the facilities to obtain nuclear and radioactive materials.

While, to date, there have not been any massive attacks against CI involving significant cascading effects, or failures, the threat posed by this type of scenario is still very much present and compels countries to set up adequate preventive and contingency plans. Indeed, terrorist actions perpetrated so far have revealed the intrinsic vulnerabilities of a number of CIs. It is also likely that new generations of terrorists will become more and more familiar with ICT. Although cyberattacks involving mass casualties – which may be qualified as "cyberterrorist attacks" – have not yet materialized, rising levels of ICT knowhow will arguably make them more likely to occur. According to the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security".[11]

[11] See https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/227/92/PDF/N1522792.pdf?OpenElement.

Box 2
Terrorist threats against aviation-related CI

Although threats to CI related to civil aviation have not changed significantly over the past few years, an increase may currently be observed in some threat vectors, such as the threat posed by cyberattacks, attacks conducted from a distance, and insiders.

Overall, airports and other aviation-related critical facilities remain an attractive target for criminal activities. Among the recorded attacks on aviation facilities, many can be categorized as burglary, armed robbery or larceny perpetrated by offenders seeking to obtain valuable goods or cash usually stored in cargo facilities or airside warehouses or carried on commercial aircraft. While none of those events involved individuals associated with terrorist groups, they demonstrate how vulnerable certain areas of airports might still be and how difficult they are to secure. in addition, since the mid-2010s, a number of events have been recorded involving unauthorized vehicles or persons forcing entry into the airside and runways of airports.

The risk associated with improvised explosive devices (IEDs) remains at the highest level and is becoming more and more geographically dispersed. The aviation plot uncovered in Australia in July 2017 showed that, by using the aviation system to spread materials and the Internet to distribute knowledge, sophisticated attacks could be launched from locations where just a small number of motivated individuals are present. So-called "lone wolf" attacks are also becoming more common, and while they are mostly currently at a low level of sophistication, this phenomenon, sometimes referred to as "mail-order terrorism", may increase the sophistication and impact of such attacks in the future.

In March 2019, IEDs in suspicious postal packages were intercepted by the police in London, allegedly as part a terrorist group operation. One of those devices was found near Heathrow Airport and was successfully deactivated. Similarly, in April 2019, the Kuwaiti authorities discovered an IED concealed in a hollowed-out book inside a cargo parcel after air cargo screeners identified the object as suspicious.

In addition to IEDs, cyber-related attacks (as reviewed in section 1.2.1) remain an important concern to civil aviation. While in 2021 there were no reports of cyberattacks endangering aviation safety or security directly, the number of such attacks on civil aviation infrastructure has been steadily increasing yearly. The main types of cyberattacks witnessed in 2021 included the use of fraudulent websites (for example, impersonating aviation entities to lure users into providing information or payment), data theft (for example, of passengers or employees' personal information), phishing and ransomware.

The threat of attacks from a distance, which include missile attacks and weaponized unmanned aircraft systems, remains of concern to aviation operations, both inside and outside of conflict zones. While most terrorist incidents against civil aviation worldwide continue to be against airports in conflict zones, attacks on airports outside conflict zones do occur and are typically mounted against dual-use facilities used by both civilian and military aviation. Most attacks against airports employ stand-off weapons, including missiles such as mortars and rockets, and also weaponized unmanned aircraft systems that enable attacks to be launched remotely.

UAS sightings around airports and above runways are also a growing concern as they jeopardize the safety and security of people and infrastructure, not to mention the risk posed to approaching aircrafts and the often-inevitable halting of operations while the threat is being resolved.

Another significant type of threat affecting civil aviation is that posed by insiders (for further details, see box 4).

Source: ICAO representative.

1.2. Nature of terrorist threats to CI

Terrorism-related threats to CI have multiple dimensions. The following sections break down such threats depending on their nature (physical versus cyber), their origin (Insider versus external) and the context in which they occur (isolated versus multiple targets). Understanding the types of threat to which CI is exposed is the first step in the process of designing adequate protection strategies, as discussed in chapter 2.

1.2.1. Physical threats versus cyberthreats

Physical threats to CI may take a variety of forms. Their common characteristic is that they are aimed at destroying infrastructure, weakening it or rendering it inoperative in full or in part by compromising its physical structure, mechanical components, and other attributes.

The most intuitive physical threats to CI involve the use of improvised explosives or incendiary devices, means of transport, rockets, man-portable air defence systems (known as "MANPADS"), grenades and even simple tools (such as matches or lighters, used in arson attacks), and so forth, to achieve the total or partial collapse or destruction of a facility. Attacks may also involve the intentional modification or manipulation of systems and CI processes (such as switching facilities on and off, triggering or releasing closures in piping systems, suppressing process signals, fault signals or alarms).

The deployment of chemical, biological, radiological or nuclear (CBRN) weapons or substances represents another distinctive type of threat to CI. CBRN attacks may be conducted by spreading infectious pathogens into food supply chains,[12] water pipes, the use of poison gas at key traffic junctions and crossroads, and similar acts. An attack on a critical facility containing CBRN materials may also result in the facility itself releasing such materials.

Although cyberthreats differ from physical threats in nature, the end result may be the same. Cyberthreats vary but may include, for example, attacks that result in:

- Systems or data manipulation – such as malware that exploits vulnerabilities in computer software and hardware components necessary for CI operation
- Shutting down of critical systems – such as denial-of-service (also referred to as "DoS") attacks[13]
- Limitation of access to critical systems or information – such as through ransomware attacks[14]

As shown in section 2.4.2, while interconnected and integrated computerized control systems have significantly streamlined the way in which CI operates and have created market efficiencies, increased connectivity may also increase the attack surface and therefore expose CI to a high risk of manipulation.

According to a private-sector survey of 200 industry executives working in critical facilities for the electricity sector in 14 countries, "[in 2010] nearly half of the respondents said that they had never faced large-scale denial of service attacks or network infiltrations. By [2011], those numbers had changed dramatically; 80 per cent had faced a large-scale denial-of-service attack, and 85 per cent had experienced network infiltrations".[15]

[12] In 1984, the salad bars of ten restaurants in Oregon, United States, were contaminated with salmonella. The attack was orchestrated by a group of people seeking to influence a local election. The incident illustrates the relative ease with which a bioterrorist attack can be perpetrated on a critical sector such as the food supply chain.

[13] A recent example of a denial-of-service attack directly affecting CIs was the attack perpetrated against the Danish railway ticket booking system on 14 May 2018.

[14] SecurityWeek reports that, between November 2013 and 31 January 2022, there were, in total, 1,137 ransomware attacks against CI organizations, according to the latest version of the Temple University CI ransomware attacks database. Researchers found that health care, government, and education were the sectors most widely targeted over the past four years. For further details, see https://www.scmagazine.com/brief/ransomware/more-than-1k-ransomware-attacks-reported-against-critical-infrastructure.

[15] McAfee, "In the dark: critical industries confront cyberattack. McAfee's Second Annual Report on Critical Infrastructure", 18 July 2011, p. 6. Available at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx.

Box 3

Cyberthreats against critical information infrastructure: conclusions by the open-ended working group on developments in the field of information and telecommunications in the context of international security

Established pursuant to General Assembly resolution 73/27, the open-ended working group on developments in the field of information and telecommunications in the context of international security provides a transparent and inclusive platform for all Member States to express their views and extend cooperation on the international security dimension of ICT.

On six occasions since 2003, groups of governmental experts have been established to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. Through three consensus reports drafted in 2010, 2013 and 2015, these groups recommended 11 voluntary norms of responsible State behaviour and recognized that additional norms could be developed over time. Building on this foundation, the open-ended working group has sought common ground and mutual understanding among United Nations Member States on a subject of global consequence. With specific reference to threats to critical information infrastructure (CII), the open-ended working group reached the following conclusions:

- There are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on CI and CII supporting essential services to the public. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern.
- ICT activity contrary to obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public, could pose a threat not only to security but also to State sovereignty, as well as economic development and livelihoods, and ultimately the safety and well-being of individuals.
- As all States are increasingly reliant on digital technologies, a lack of awareness and adequate capacities to detect, defend against or respond to malicious ICT activities may make them more vulnerable. As witnessed during the current global health emergency, existing vulnerabilities may be amplified in times of crisis.
- Threats may be experienced differently by States according to their levels of digitalization, capacity, ICT security and resilience, infrastructure and development. Threats may also have a different impact on different groups and entities, including on youth, the elderly, women and men, people who are vulnerable, particular professions, small and medium-sized enterprises, and others.

Source: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Table 1
Top 10 threats to industrial control systems (ICS)

No.	Threat	Explanation
1	Unauthorized use of remote maintenance access points	Maintenance access points are deliberately created external entrances to the ICS network and are often insufficiently secure.
2	Online attacks via office or enterprise networks	Office information technology (IT) is usually linked to the network in several ways. In most cases, network connections from offices to the ICS network also exist, so attackers can gain access via this route.
3	Attacks on standard components used in the ICS network	Standard IT components (commercial off-the-shelf) such as systems software, application servers or databases often contain flaws or vulnerabilities, which can be exploited by attackers. If these standard components are also used in the ICS network, the risk of a successful attack on the ICS network increases.
4	DoS attacks	(Distributed) denial-of-service attacks can impair network connections and essential resources and cause systems to fail – in order to disrupt the operation of an ICS, for instance.
5	Human error and sabotage	Intentional deeds – whether by internal or external perpetrators – are a massive threat to all protection targets. Negligence and human error are also a great threat, especially in relation to the protection targets confidentiality and availability.
6	Introducing malware via removable media and external hardware	The use of removable media and mobile IT components of external staff always entails great risk of malware infection.
7	Reading and writing news in the ICS network	Most control components currently use clear text protocols, so communication is unprotected. This makes it relatively easy to read and introduce control commands.

8	Unauthorized access to resources	Internal perpetrators and subsequent attacks following initial external penetration have it especially easy if services and components in the process network do not utilize authentication and authorization methods or if the methods are insecure.
9	Attacks on network components	Attackers can manipulate network components in order to carry out man-in-the-middle attacks or to make sniffing easier, for example.
10	Technical malfunctions or force majeure	Outages resulting from extreme weather or technical malfunctions can occur at any time – risk and potential damage can only be minimized in such cases.

Source: OSCE, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, Vienna, 2013, p. 34. Available at www.osce.org/files/f/documents/4/b/103500.pdf

1.2.2. Insider threats versus external threats

While the protection of CI from outside attacks benefits from a significant amount of guidance from national and international regulatory agencies, insider threats have received comparatively little attention. In comparison with external entities, who can only gain access to CI by means of violent acts or subterfuge, people acting from inside, so to speak, have distinctive advantages. They are often company employees or suppliers. They can either be the main conspirators or act as accomplices (such as informants) to outside agents. They are often in a position to observe processes undisturbed over a period of time. Their knowledge (or the ease with which they can acquire knowledge) of the relevant facility can be readily exploited for criminal purposes.

Section 2.6.2.2 provides some examples of measures to secure CI against this type of threat. In this area, a key preventive role can be played by CI operators, starting from the implementation of effective personnel selection and vetting procedures.

Box 4
Insider threat dynamics in the civil aviation sector

The threat posed by insiders remains a great concern to the civil aviation sector, exacerbated by circumstances brought about by the coronavirus disease (COVID-19) pandemic. While it is not a new threat, the pandemic has strained many aviation resources and upended normal life routines, possibly rendering more likely the materialization of this particular type of threat. Insider threat events recorded to date, such as criminal activities facilitated by aviation employees, have been on the rise, as evidenced by the discovery of guns concealed in luggage by airline employees or a drug-related money-laundering scheme facilitated by airport staff. In addition, some of the armed robberies and other similar crimes mentioned above may have been facilitated by insiders and people with privileged access. Individuals with links to terrorist groups have attempted to gain airport employment, and also employment in other parts of the aviation-related transport system. This tactic contrasts with the more common approach followed in the past, whereby efforts were made to influence insiders already within the organization, rather than attempting to place potential operatives within the system. In spite of this, the risk posed by insiders without any affiliation to terrorism should not be overlooked, such as the case of an American Airlines mechanic who tampered with an aircraft in service by gluing a piece of foam inside an inlet on the air data module, which could have led to a catastrophic event. The mechanic was allegedly upset about union contract negotiations.

Source: ICAO representative.

1.2.3. Isolated targets versus multiple targets

Threats against CI may be either isolated and sporadic acts, or part of a broader plan to attack infrastructure in the same sector (such as energy, transport, telecommunications), belonging to the same owner or operator, or located in the same geographical area. Terrorism-motivated actions targeting CI may be perceived in much the same way as cases of industrial espionage, in which cyberattacks are often launched as campaigns, or serial attacks. For example, in 2011 the so called "Lurid" malware attack targeted, among others, the ICT systems of a number of diplomatic missions and space-related government agencies. Other attacks may encompass infrastructure based in multiple countries and belonging to

various critical sectors. The most extensive attack ever orchestrated to date, in terms both of its geographical reach and the disruption caused, is that of the WannaCry crypto-worm, which in May 2017 disabled rail systems in Germany and the Russian Federation, blocked hospitals in the United Kingdom, interfered in telecommunications networks in Portugal and Spain and blighted petrochemical companies in Brazil and China.

The identification of patterns in similar complex scenarios requires strong analytical tools and the processing of information from vast and heterogeneous sources. To complicate matters further, as the Organization for Security and Cooperation in Europe (OSCE) has highlighted with reference to the energy sector, most cyberattacks are not publicized because the relevant operators are reluctant to make those incidents known. At the same time, the ability to recognize underlying dynamics and methods as early as possible is key to enabling authorities to share live information. This strengthens the capacity to respond more effectively to current attacks and to pre-empt imminent attacks against likely victims.[16]

In some cases, what appears to be an isolated attack, aimed at relatively unimportant targets, may in fact be part of a more ambitious and incremental criminal strategy.[17] It is crucial to be able to identify as early as possible whether an attack is a sporadic act mounted against one piece of infrastructure or is part of a series of planned attacks against other infrastructure. Developing such advance knowledge is essential for preventive purposes.

1.3 Terrorist motivations to attack CI

The heterogeneous nature of CI, together with the different geographical and institutional contexts in which it is located and operates, renders it extremely difficult to reach general conclusions as to what motivates terrorists to carry out their attacks on CI, as opposed to non-critical targets. An analysis of terrorist motivations may still, however, provide useful pointers as part of the broader threat assessments required under critical infrastructure protection (CIP) national strategies.

From the limited empirical research carried out in this field, it emerges that CI is attractive for a variety of reasons. First, some critical facilities may represent an appealing target because of their strategic value for societies, in particular in highly industrialized countries of the West. Interfering in their functioning, ideally with the possibility of generating cascading effects, will enable terrorists to maximize damage and the impact of their action in just one shot and to instil fear at levels that would not be so easily attainable by attacking less critical targets. It was to this end, for example, that Al-Qaida operatives reportedly devoted a considerable amount of time to surveillance of the headquarters of various United States-based financial firms and international organizations. Arguably, this meticulous activity was mounted in response to Osama bin Laden's 2001 edict urging his affiliates to "concentrate on hitting the United States economy through all possible means".[18]

Other critical facilities may be targeted to show the impotence of State institutions. For example, terrorist organizations may decide to attack power-generating facilities, oil pipelines and other such installations in order to cut off the supply of basic services and reveal the fragility of public bodies and related government policies.

---

16 OSCE, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, Vienna, 2013. Available at https://www.osce.org/files/f/documents/4/b/103500.pdf.

17 A joint Department of Homeland Security-FBI report issued in 2017 noted that certain United States government networks in the energy, nuclear, water, aviation, and critical manufacturing sectors were at risk of targeted advanced persistent threat actions. The Department assessed this activity to be a "multi-stage intrusion campaign by threat actors targeting low security and small networks to gain access and move laterally to networks of major, high value asset owners within the energy sector." According to the report, the "threat actors [were] actively pursuing their ultimate objectives over a long-term campaign", with companies like third-party suppliers being initially targeted as staging targets. (See: Department of Homeland Security, "Advanced persistent threat activity targeting energy and other critical infrastructure sectors", 20 October 2017, available at www.us-cert.gov/ncas/alerts/TA17-293A. See also Conner Forrest, "DHS, FBI warn of cyberattacks targeting energy infrastructure, government entities", TechRepublic, 23 October 2017. Available at https://www.techrepublic.com/article/dhs-fbi-warn-of-cyberattacks-targeting-energy-infrastructure-government-entities/.

18 Gary Ackerman and others, *Assessing Terrorist Motivations for Attacking Critical Infrastructure*, Center for Nonproliferation Studies, Monterey Institute of International Studies, 2007. Available at https://digital.library.unt.edu/ark:/67531/metadc887957/m2/1/high_res_d/902328.pdf.

A third possible motivation, connected to the two previous ones, is the desire to obtain a higher degree of publicity than would be possible by focusing on lower-profile targets.

Paradoxically, terrorists may seek control of CI not to cause damage or intimidate, but for the opposite reason: with the aim to establishing their own legitimacy and social acceptability. As has been noted, while most operations carried out by Da'esh using water-related infrastructure were aimed to disrupt troop movements and fight the military, "such efforts also often [had] the added benefit of enhancing recruitment efforts; by allowing water to flow to towns sympathetic to the Islamic State's cause, or even by simply doing a better job of providing necessary services, the group [could] attract more men and women to its ranks".[19]

In many cases, there is probably a combination of factors prompting terrorist groups to perpetrate attacks involving CI. These incentives will also have to be balanced with a number of constraints. The final decision as to which infrastructure to strike and the modus operandi to be employed will depend on factors such as the characteristics of the targeted sector and the vulnerability of individual infrastructure. It will also hinge on the operational and financial capabilities of the terrorist group to launch a particular attack. The robustness of physical protection measures in place at a certain critical facility will naturally influence such decision. Similarly, the strength of the procedures applied by the infrastructure's management to mitigate the insider threat will also play a role. This is not to say that terrorist groups will only attack CI when they are sure of being able to interfere in its operations. A simple attempt, even a failed one or one that causes very limited damage, might provide the desired level of media resonance, in particular when the target is chosen for its symbolic value.

1.4 Countering terrorist threats to CI through a human rights-compliant and gender-responsive approach

Terrorism poses a serious challenge not only to international peace and security, but to the very tenets of the rule of law and to the protection of human rights. Member States take steps to effectively counter and prevent terrorism as part of their obligations under international human rights law. This obligation is of particular importance in view of the potential impact that attacks on CI may have on populations, given the role that such infrastructure frequently plays in delivering vital social functions. Damage to or the disruption or destruction of critical infrastructure can result in far-reaching impact on a wide range of human rights, from the right to life and security of person to the right to health and a healthy environment, the right to education, and the right to water, sanitation and other prerequisites of an adequate standard of living.

The duty of States to safeguard human rights entails the obligation to take necessary and adequate measures to prevent, combat and prosecute activities that endanger these rights, such as threats to national security or violent crime, including terrorism. In this respect, States should be guided, among others, by the United Nations Global Counter-Terrorism Strategy, which emphasizes that effectively combating terrorism and ensuring respect for human rights are not competing but complementary and mutually reinforcing goals. While the promotion and protection of human rights may constitute an independent pillar of the Strategy, they are also essential to the successful delivery of all four of its components.

The Security Council has also consistently and repeatedly affirmed that States should ensure that any measures taken to counter terrorism comply with all their obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law. Moreover, in its resolution 2178 (2014), the Security Council stated that failure to comply with these and other international obligations, including under the Charter of the United Nations, fosters a sense of impunity and is one of the factors contributing to increased radicalization. Counter-terrorism

19 Ambika Vishwanath, "The Water Wars Waged by the Islamic State", Stratfor, 2015. Available at https://worldview.stratfor.com/article/water-wars-waged-islamic-state.

strategies, including those adopted to protect CI, should also take into account gender and age sensitivities, the best interests of the child and the differential impact of terrorism and violent extremism conducive to terrorism on the human rights of women and girls.[20]

In the interest of addressing terrorist threats to CI, State authorities may temporarily take measures that result in the limitation of certain rights, provided that these restrictions comply with the conditions set out in international human rights law. Measures taken in this regard need to be in genuine response to the threat at hand, made necessary by the exigencies of the situation, have a clear legal basis, and be proportionate to the pursuance of legitimate aims. States have to ensure that satisfactory safeguards are set up to protect against arbitrary and disproportionate interference with human rights in this context.

To meaningfully comply with these obligations, States need to conduct regular human rights assessments of measures taken to tackle the terrorist threat to CI and ensure that such measures are evidence-based and therefore efficient, and do not reinforce exclusion, prejudice or biases, nor hinder access to or use of the space by certain groups or populations. Likewise, integrating gender perspectives in CIP is integral to effective and efficient risk mitigation strategies, as it considers not only the gender-specific security needs of women, men, boys and girls, but also how the underlying gendered relationships, stereotypes and dynamics influence security patterns and vulnerabilities.

[20] Addendum to the Madrid Guiding Principles (S/2018/1177).

2. Developing national strategies for CIP against terrorist attacks

Security Council resolution 2341 (2017)

The Security Council

...

2. *Calls upon* Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management, and facilitating effective interaction of all stakeholders involved

Addendum to the Madrid Guiding Principles

Guiding principle 50

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

...

(c) Develop, implement and practise strategies and action plans for reducing the risks of terrorist attacks on critical infrastructure … that integrate and leverage the capabilities of relevant public and private stakeholders

2.1 Why a national strategy?

Most Member States have been providing safety and security measures for their CI long before CIP established itself as a policy field in its own right. Protective measures were mostly adopted in an incremental and piecemeal fashion, in the form of regulations covering specific sectors or threats, or focusing on certain parts of risk and crisis management processes. In some cases, State policies have reached a significant level of sophistication and conform to the highest international standards.

As a result, it may be asked why Member States should design general nationwide CIP strategies when they already have detailed regulations, policies and practices in place covering most, if not all, critical sectors. The most compelling reason is that, in modern societies, the protection of CI is an increasingly transversal and multidisciplinary task. The interdependence between sectors, with the potential for cascading effects in the event of accidents (whether of natural origin or human-caused) requires the ability to see the big picture, so to speak, as a condition for the effective coordination of prevention, response and recovery actions across sectors. In addition, relying on purely sectoral – or so-called "vertical" – approaches would appear to unduly multiply involved agencies, cause the duplication of effort and waste of resources. A comprehensive CIP strategy thus aims to rationalize workstreams, produce economies of scale and better allocate financial and human resources around a set of predetermined objectives.

This is not to suggest that nationwide CIP strategies should replace existing sector-specific protection measures, in particular when these measures have proved successful or conform to international regulatory frameworks or recognized best practices. What is needed, however, is for Member States to bring the various pieces of the mosaic together,

and to make them part of a coherent system of governance. CIP strategies should be tailored to suit the specific needs and approaches of individual countries.

As shown in section 2.5, Member States have adopted a variety of institutional models reflecting not only their specific legal traditions, but also the relationship between the Government, citizens and the private sector. Countries have considerable room for manoeuvre in determining the modalities for protecting their CI. They all need, however, to have in place the conceptual building blocks (a strategy) to connect the dots and ensure smooth working relationships among all stakeholders. With this in mind, the overarching objectives of a nationwide, cross-sectoral strategy should be:

- To define the sectors to be regarded as critical and lay out a methodology for identifying specific assets and processes as critical (see section 2.4.1)
- To identify and empower a governmental entity in charge of coordinating and managing the protection effort at the national level, which includes promoting and sustaining the implementation of the strategy by the various stakeholders involved (see section 2.5)
- To allocate the institutional responsibilities at the level of each critical sector and the various levels of government (local, state, federal) (see chapter 5)
- To define methodologies for the prevention of and response to terrorist attacks against CI following a risk and crisis management approach (see section 2.6)
- To outline the forms, channels and procedures for sustained information-sharing and coordination between the competent government agencies and the private sector, notably CI owners and operators (see section 2.5.2)

Tool 1
OECD Recommendation on the Governance of Critical Risks

www.oecd.org/gov/risk/recommendation-on-governance-of-critical-risks.htm

Adopted by the Council of the Organisation for Economic Co-operation and Development (OECD) in 2014, the Recommendation proposes a fundamental shift in risk governance towards a whole-of-society effort. By introducing the notion of "critical risk", it proposes a set of actions that Governments can take at all levels of government, in collaboration with the private sector and with each other, to better assess, prevent, respond to and recover from the effects of extreme events (both natural and human-induced), as well as take measures to build resilience to rebound from unanticipated events.

The Recommendation identifies four overarching considerations that Governments should take into account with a view to making society more resilient to critical risks:

- Identification and assessment of risks should take interlinkages and knock-on effects into account. This helps set priorities and inform allocation of resources.
- More investment should be made in risk prevention and mitigation – such as investments in protective infrastructure – but also non-structural policies such as land-use planning.
- Flexible capacities for preparedness, response and recovery should be developed to help manage unanticipated and novel types of crises.
- Transparent and accountable risk management systems should learn continuously and systematically from experience and research.

Tool 2
OECD, Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies, 2019

www.oecd.org/gov/risk/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm

Acknowledging the global increase in infrastructure investment and the digital transformation of infrastructure services, this report takes stock of the changing context and examines the policy options and governance models for making upfront investment in resilience. Based on a cross-country survey, it analyses the progressive shift of CI policies from asset protection to system resilience.

A system approach is understood as one in which Governments and infrastructure operators address asset interdependencies and prioritize resilience measures for critical hubs and nodes whose failure would cause the most damage.

The report includes a policy toolkit for the governance of CI resilience. The toolkit identifies the steps that countries are recommended to take to design an appropriate governance model for today's CI resilience challenges. This toolkit complements the OECD Recommendation on the Governance of Critical Risks (see Tool 1), contributes to international discussions in the Group of 20 on quality infrastructure, and supports the implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030.

Tool 3
Cybersecurity and Infrastructure Security Agency (CISA), United States: Guide to Critical Infrastructure Security and Resilience

www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

The Guide provides an overview of the approach to critical infrastructure security and resilience adopted in the United States. Rather than to promote specific approaches, the intent is to share basic information and lessons learned over the past 15 years. Information may apply to other countries, in particular those that are considering developing or refining their own voluntary and regulatory-based infrastructure security and resilience programmes. Each section of the Guide provides additional resources for more detailed information on specific topics.

2.2 All-hazards versus specific-risk approaches

The threats faced by CI are polymorphous in nature. They may be natural: thus, on 11 March 2011, an earthquake followed by a tsunami provoked a major nuclear accident in Fukushima, Japan. They may have their origin in negligent human behaviour. In 2006, a blackout affected 10 million people across Europe following action by an electricity transmission operator who had switched off a power cable across the River Ems to allow a cruise ship to pass.

Other threats may be the direct result of human behaviour intended to pursue terrorism-related or other criminal objectives. Cyberattacks for ransom offer an increasingly common example of profit-making activities that may severely affect CI by encrypting users' data and demanding payment in exchange for unlocking the data. Threats to CI may also be linked to criminal behaviour in more subtle and indirect ways. In Europe, the French building association Fédération française du bâtiment has repeatedly warned against criminal networks' involvement in the trafficking of counterfeit and substandard construction materials. Reportedly, many companies in the construction sector have purchased non-compliant, poor-quality materials compromising the solidity of critical assets and exposing them to a higher risk of collapse.

As Member States are called upon to protect CI from multiple types of risk, a key question is: Should Governments adopt one single plan covering all possible threats, or rather envisage the adoption of hazard or risk-specific strategies? In principle, either approach is consistent with the international legal framework, including resolution 2341 (2017).

Among the Member States that have adopted CIP strategies, the majority follow an all-hazards approach.[21] This means that strategic objectives and organizational structures are shaped in such a way as to take into account accidental, intentional and natural threats to CI in a holistic manner. An all-hazards approach is often seen as a prerequisite to making the best use of limited available resources and avoiding needless duplication. The underlying rationale is that the same risk management and collaborative processes, and also crisis response mechanisms, can be broadly used to respond to all types of threats indistinctively. All-hazards approaches are implemented by such countries as Canada and the United Kingdom.

Other countries adopt a mixed approach. Australia, for example, has elaborated specific guidelines on the protection of CI against terrorist attacks.[22] The guidelines complement the country's general strategy on CIP, which extends its reach to other hazards. In Spain, the institutional architecture for CIP is set out in Act 8/2011, establishing measures for the protection of CI. Unlike other countries, the Spanish law is focused on countering the terrorist threat, although it applies to other – unspecified – risks.

The imperative set out by resolution 2341 (2017) is for the terrorist threat to be comprehensively reflected in the preparation of Governments' strategic plans to protect CI. With this in mind, each Member State is encouraged to determine, as a matter of national policy, the most effective forms and modalities for protecting CI against terrorist acts within a multi-threat type of environment.

2.3 CIP strategies vis-à-vis other national policies

Most Member States, including those that have not enacted dedicated CIP strategies, address CIP-related issues in practice through a variety of policy instruments elaborated by different government agencies. These documents typically take the form of national security (including cybersecurity) strategies, policies on counter-terrorism and soft target protection. While these various policies may have been adopted at different times and by multiple government agencies, it is vital that their CIP-related components be part of a coherent message and strategy. This requires, in particular, that Member States determine:

- The interplay between existing policies (on counter-terrorism, national security and other such matters) and a dedicated CIP strategy
- The extent to which existing policies and the CIP strategy should be adjusted and streamlined in order to avoid conflicting outcomes that would make implementation difficult or impossible

When a national strategy on CIP is being designed, it is important to make an inventory of all national policies that may have an impact on or intersect with CIP issues. If they impinge on CI-related issues in substance, they should be subject to close scrutiny for the purpose of ensuring their compatibility with and complementarity to newly designed CIP national strategies.

2.3.1. Policies on soft targets

As amply illustrated by the specialized thematic modules which complement this Compendium, soft targets are types of vulnerable sites (such as religious, tourist and urban sites, museums, cinemas, shopping malls, landside and public areas of an airport, sports facilities, and so forth) whose open nature and high degree of accessibility make them especially vulnerable to terrorist attacks. Often, soft targets offer terrorists an ideal ground to strike with little planning effort while still causing mass casualties.[23]

21 In the context of aviation, ICAO applies the word "hazards" to refer to safety-related issues. Security-related events are more accurately defined as "incidents".

22 See the National Guidelines for Protecting Critical Infrastructure from Terrorism, available at www.police.vic.gov.au/sites/default/files/2019-03/NationalGuidelinesForProtectingCriticalInfrastructureFromTerrorismNovember2015.pdf.

23 The specialized thematic modules provide extensive analysis of the features and characteristics of soft targets, along with guidance and good practices on policies and operational actions to address their vulnerabilities and increase their resilience in the face of terrorist acts.

The notion of soft targets is conceptually distinct from that of CI, which broadly refers to assets, systems and processes that are vital for the provision of essential services and whose disruption has the potential to cause extensive negative impacts to the security, social and economic well-being of a community.

A key element of distinction between soft targets and CI thus resides in their degree of "criticality". Soft targets are not per se critical to the delivery of essential social services. Moreover, a soft target is typically a physical site, while critical infrastructure may also be a process, including information systems and networks (see section 2.4.2). In addition, unlike soft targets, a notable feature of CI is the ability to generate so-called "cascading effects", whereby disruptions in one sector have a potential domino effect by striking other sectors and leading to system-wide paralysis (see section 2.4.3). The criteria employed by countries to identify infrastructure meriting a special level of protection – based on prediction models about the severity, duration, geographical scope and economic consequences of disruptive events – are hardly suitable for the determination of what constitute a soft target.

A major consequence of these differences is that Member States' policies and frameworks dealing with soft targets do not automatically satisfy conditions and requirements for the protection of CI. This does not imply, however, that the two areas need to be handled in silos. On the contrary, logic and experience show the usefulness for countries to avoid a compartmentalized approach and, instead, develop synergies as part of their overall protection policies against terrorist acts. While keeping in mind the differences in the conceptual and normative frameworks applicable to soft targets and CI, the potential for complementarity should be systematically explored. The rationale for a coordinated approach stems from a number of considerations, including the following:

- The same public agencies often have institutional and operational responsibilities in both areas.
- Successful measures designed and implemented in the field of CIP can also be applied to the protection of soft targets and vice versa. For example, various measures adopted to ensure the physical security of CI are also typically used to control access to soft targets (such as guard posts, fences, metal detectors and so forth).
- Lessons learned in one area may be easily – albeit not automatically – transferred to the other one, including on achievements and failures observed in risk mitigation and crisis management.
- Both critical infrastructure and soft targets are typically owned and operated by private entities, making the development of public-private partnerships (PPP) a central feature of preparedness and protection efforts for both.

Box 5
Disruptions to CI and soft targets: the interplay

CI is often crucial to the functioning of soft targets. For example, uninterrupted electricity supply is needed for a sporting event to take place. At the same time, a disruption to the provision of basic services, such as electricity, may not simply leave those present in a concert hall in the dark and interrupt the performance, but could be part of a strategy to make evacuation efforts more difficult during a terrorist attack. At the same time, a successful terrorist attack against a crowded tourist or religious site may cause CI – and even an entire critical sector – to collapse. For example, hospitals may rapidly fill beyond their capacity and communication networks stop working as they are overwhelmed with users' requests. Attacks on soft targets may have particularly severe effects on CI when they occur in urban areas, where the two coexist and interact in complex and densely populated spaces, underlying the need for an approach that considers both as part of a single multifaceted system.

The above-mentioned examples show that protection efforts for CI and soft targets require close policy, institutional and operational coordination.

CASE STUDY 1
Integrating CI and soft target protection frameworks: Belgium and Germany

Belgium's "federal points of interest"

The Belgian Protection of Critical Infrastructure Act of 1 July 2011 incudes the notion of "federal points of interest" ("points d'intérêt fédéral"). These are defined as "places not designated as critical infrastructure, but of particular interest to public order, for the special protection of persons and property, for the management of emergency situations or for military interests, and which may require protective measures taken by the Crisis Centre General Directorate".

The Belgian law offers an example of a single normative framework taking into account both CI and soft targets. Although the so-called "federal points of interest" do not meet the conditions to be regarded as CI, they are still considered worthy of particular attention and protection.

Systemic versus symbolic criticality in Germany

The German National Strategy for Critical Infrastructure Protection distinguishes between criticality of a systemic nature and that which is merely symbolic. Infrastructure is considered to be of "systemic criticality" whenever – owing to its structural, functional and technical position within the overall system of infrastructure sectors – it is highly relevant in view of its interdependencies. Examples are electricity and IT infrastructure, which, on account of the size and density of their network, may cause serious disruptions of community life and processes whenever there is a widespread and prolonged outage. By contrast, infrastructure may be of "symbolic criticality" if its loss might, on account of its cultural significance or its important role in creating a sense of identity, have an emotional impact and a lasting and psychologically unbalancing effect on society.

Sources: www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf;jsessionid=C71D9BB-5FA7E4A7115D27E77116449A3.1_cid287?__blob=publicationFile&v= and www.nbb.be/doc/cp/fr/2018/20180925_loi_du_1juillet2011.pdf

2.3.2. National security policies

National security is a fluid concept. Member States translates this concept into different sub-items and approaches depending on a number of factors and perceptions rooted in their specific history, geographical situation or geopolitical context. In most cases, national security encompasses principles, policies, procedures and functions which aim to guarantee a country's independence, sovereignty and integrity, and also the rights of its citizens.

Some countries explicitly include CIP among their national security priorities. Linking CIP firmly to the realm of national security objectives may help to ensure enhanced political backing for the subsequent elaboration of dedicated CIP strategies and facilitate their implementation.

CASE STUDY 2
Integrating CIP into national security strategies: Poland and Spain

Poland

The 2020 National Security Strategy makes explicit reference to CIP under its pillar dealing with "Resilience of the state and common civic defence". Section 2.8 of the Strategy envisages the implementation of a "model of critical infrastructure protection, ensuring its continued operation and uninterrupted provision of services". The Strategy also contains guidelines for CIP in specific sectors such as health, economic and energy security.

Spain

The 2021 National Security Strategy identifies CI as the axis on which the physical resilience of a country is articulated. The Strategy focuses on the need to promote the preventive dimension of the national system for CIP, with special emphasis on the protection of CI computer systems and operators of essential services against cyberthreats.

Sources: www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf and www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021.

2.3.3 Counter-terrorism policies

While most counter-terrorism strategies do not specifically mention CI, a number of the objectives and institutional arrangements set forth in those strategies are instrumental in preserving the integrity of CI and the vital social functions that it performs. For example, counter-terrorism strategies implicitly address CIP issues when they set forth procedures for general crisis management following a terrorist attack. Moreover, counter-terrorism strategies often set out broad frameworks for preventing the commission of terrorist offences (for example, by addressing preparatory acts, creating synergies between intelligence and law enforcement communities, and other such measures).

CIP strategies should integrate concepts and procedures set forth in counter-terrorism policy frameworks by adapting them to specific CIP needs and contexts.

CASE STUDY 3
Protecting CI through counter-terrorism legislation: Republic of Moldova and Portugal

Republic of Moldova

The regulation on the protection of critical infrastructure against terrorism (government decision No. 701) establishes the process for planning, organizing and implementing the counter-terrorism protection measures of CI facilities by streamlining the use of available human, financial and material resources and taking into account the specific vulnerabilities of CI.

The regulation was adopted in the framework of Act No. 120 on preventing and combating terrorism, which provides the normative and organizational framework for the competent authorities to coordinate law enforcement measures. It also sets forth the responsibilities of those that directly participate in counter-terrorist operations and outlines the rights of victims of terrorist attacks.

Portugal

The protection of CI is part of the country's National Counter-Terrorism Strategy, which is based on five pillars: "detect, prevent, protect, pursue and respond". The purpose of the "protect" pillar is to strengthen the security of priority targets and, in that regard, protection takes the form of increasing the security of people, borders, the movement of capital, goods, transport, energy and critical infrastructure, both national and European.

The National Counter-Terrorism Strategy mentions the development of an action plan for the protection of CI and enhancement of its resilience. The preparation of security plans is under the responsibility of individual CI operators, while the external security plans fall within the mandate of the armed forces, security services and the National Civil Protection Authority.

In addition, in 2016, a working group on the protection of CI was established under the auspices of the country's Internal Security System. It thus became possible to harmonize procedures for the analysis of the security component of operators' security plans. The working group has been meeting periodically and implementing its mandate, ensuring critical infrastructure protection in the energy and transport sectors.

Source: Information provided by the Permanent Missions of the Republic of Moldova and Portugal to the United Nations.

2.3.4. Cybersecurity policies

Cybersecurity is defined by the Global Forum on Cyber Expertise (GFCE) as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets".[24] Cybersecurity policies have a central place in the protection of CI as they provide the framework where countries define the objectives and means for protecting Critical Information Infrastructures (CII). This concept is further examined in section 2.4.2.

A number of regional instruments explicitly associate cybersecurity concepts with CI. For example, the African Union Convention on Cyber Security and Personal Data Protection (2014) demands that States Parties "undertake to develop, in

[24] Global Forum on Cyber Expertise (GFCE) Foundation, *GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers*, GFCE-Meridian, 2016. Available at https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

collaboration with stakeholders, a national cybersecurity policy which recognizes the importance of Critical Information Infrastructure (CII) for the nation, identifies the risks facing the nation in using the all-hazards approach and outlines how the objectives of such policy are to be achieved" (art. 24, "National cyber security framework")

With this in mind, not all national cybersecurity strategies accord the same place and weight to CI and there are significant differences among countries. As noted in the GFCE-Meridian Good Practice Guide, "some strategies have been written from a cybercrime perspective only or an internet-only perspective. They tend to overlook (national) disruption and crisis management for CII as well as cross-sectoral impacts. Strategies written from cybersecurity perspective based on a national risk assessment will adopt a broader perspective that will give room for CIP and CIIP" (p. 8).

Box 6
European Union approach to cybersecurity

The European Union has constructed its cybersecurity policy around three main pillars that are directly relevant for the protection of CI: a cybersecurity strategy; a legislative framework; and a sanctions regime against cyberattacks.

Cybersecurity strategy

In December 2020, the European Commission and the European External Action Service presented a new European Union cybersecurity strategy. The document sets out proposals for deploying new regulatory, investment and policy instruments. On 22 March 2021, the European Council adopted conclusions on the cybersecurity strategy, setting as a key objective the achievement of strategic autonomy while preserving an open economy. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity, with the aim of strengthening the European Union's digital leadership and strategic capacities.

Legislative framework: Cybersecurity Act

The European Union Cybersecurity Act, which entered into force in June 2018, introduced the following:

- European Union-wide certification scheme: This scheme was established in recognition of the fact that the different security certification schemes currently in use by different European Union member States generate market fragmentation and regulatory barriers. The European Union-wide certification scheme is expected to play a critical role in ensuring high cybersecurity standards for ICT products, services and processes.
- New and stronger mandate for the European Union Agency for Cybersecurity: Building on structures of its predecessor, the European Union Agency for Network and Information Security, the Agency supports member States, European Union institutions and other stakeholders in dealing with cyberattacks.

Legislative framework: Network and Information Systems (NIS) Directive

The NIS Directive was introduced in 2016 as the first ever European Union-wide legislative measure with the purpose of strengthening cooperation between member States on cybersecurity. It laid down security obligations for operators of essential services (in critical sectors such as energy, transport, health and finance) and for digital service providers (online marketplaces, search engines and cloud services). In December 2020, the European Commission proposed a revised NIS directive (NIS2) to replace the 2016 directive. The new proposal responds to the evolving threat landscape and takes into account the digital transformation, which has been accelerated by the COVID-19 crisis.

The new rules, for which the Council devised a general approach in December 2021, aim, among other objectives, to strengthen security obligations for businesses and supply chains, introduce more stringent supervisory measures for national authorities and increase information-sharing and cooperation.

Sanctions regime against cyberattacks

In May 2019, the Council established a framework enabling the European Union for the first time to impose sanctions on persons or entities are responsible for cyberattacks or attempted cyberattacks, that provide financial, technical or material support for such attacks or that are involved in other ways. Restrictive measures include a ban on persons travelling to the European Union and an asset freeze on persons and entities. The first ever sanctions for cyberattacks were imposed on 30 July 2020.

Source: https://www.consilium.europa.eu/en/policies/cybersecurity/.

2.4 Which infrastructure is critical?

Addendum to the Madrid Guiding Principles

Guiding principle 50

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

...

(b) Determine what constitutes critical infrastructure … in the national context, on the basis of ongoing analysis of terrorist capabilities, intentions and past attacks

Security Council resolution 2341 (2017) explicitly recognizes, in its preamble, that "each State determines what constitutes its critical infrastructure". It does not specify, however, which specific criteria Member States should use to select certain assets and processes among the myriad located in their territories. Nor is any guidance in this regard provided by other international instruments.[25]

Member States are thus left with significant discretion in choosing the criteria for identifying which infrastructure operating in their territory satisfies the "criticality" threshold. The task is not a trivial one: the singling out of infrastructure that should acquire "critical" status is key to being able to prioritize scarce resources on the protection of several assets, systems and processes. On the one hand, the inclusion of too many objects in the "critical" category may become unmanageable (in addition to being financially unsustainable). On the other hand, too restrictive an approach runs the risk of leaving a number of key assets and processes unprotected with potentially catastrophic consequences in the event of an accident. As has been noted, Governments have a tendency to expand rather than narrow down their national lists of CI. This occurs because, as noted by the United Kingdom Chatham House International Security Department, "too few decision-makers are willing to accept the political risk that might come with removing an item from the 'critical' list, and the temptation is to continually expand the circle of things that are considered critical. This level of ambiguity is wasteful as resources are not directed to where they can have the most impact.".[26]

Member States planning to adopt policies or regulatory framework for the identification of their own CI can draw inspiration from the methodologies employed by other Member States. The following subsections reference some commonly used methodologies and illustrate the three basic steps that Governments should consider taking.

---

[25] The African Union Convention on cybersecurity, for example, limits itself to requesting that "each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure" (art. 25, "Legal measures", para. 4, "Protection of critical infrastructure").

[26] Dave Clemente, Cyber Security and Global Interdependence: What Is Critical? Chatham House, London, 2013, p. ix. Available at https://www.brookings.edu/book/cyber-security-and-global-interdependence-what-is-critical/.

2.4.1. Determining "criticality"

2.4.1.1 Step 2: Identifying certain sectors as critical"

The first basic step in the CI identification processes is determining what is meant by CI in general. This is useful in defining the arena in which further policy and regulatory frameworks will be crafted.[27] Typically, national definitions combine two elements: they highlight the finality or purpose of the infrastructure (linking criticality to the performance of essential social functions) and emphasize the effects of disruption or destruction (in other words, linking criticality to the estimated consequences of service interruption).[28]

CI may be defined by taking into account the role that it plays in the promotion and protection of human rights (for example, infrastructure that is vital to the functioning of health-care delivery systems, emergency services systems, water and wastewater systems, and others), as well as the human rights impact that the disruption or destruction of the infrastructure would likely cause (for example, inability to deliver adequate or even life-saving health services; environmental damage that may result in loss of life; forced displacement with a negative impact on the right to health, and others). Such an approach is reflected in various existing definitions, including in the European Union definition set out below. In the same vein, the law of armed conflict bestows special protection on infrastructure that is indispensable for the survival of the civilian population or the destruction of which may cause severe casualties or prejudice the health and survival of the population (First Additional Protocol to the 1949 Geneva Conventions, arts. 54–56).

Box 7
European Union definition of critical infrastructure

The European Union defines "critical infrastructure" as an "asset, system or part thereof" which is "essential for the maintenance of vital social functions, health, safety, security, economic or social well-being of people", and the disruption or destruction of which would have a significant impact "as a result of the failure to maintain those functions."

Source: Council Directive 2008/114/EC, art. 2.

Table 2
National definitions of CI

Argentina	CI is that which is essential for the proper functioning of essential services of society, health, security, defence, social welfare, the economy and the effective functioning of the State, whose destruction or disruption, in whole or in part, affects and/or impacts them significantly (resolution 1523/2019, annex 1).
Austria	Infrastructure or parts thereof which are of crucial importance for ensuring important social functions and the failure or destruction of which has severe effects on the health, security or the economic and social well-being of the population or the functioning of government institutions (Strategy for Cybersecurity, 2013)
Belgium	Facility, system or part thereof, of federal interest, which is essential to the maintenance of vital functions of society, the health, safety, security and economic or social well-being of citizens, and whose interruption of operation or destruction would have a significant impact due to the failure of these functions (2011 Act on the Security and Protection of Critical Infrastructure)
Canada	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 (Public Safety Canada)

27 The international law of armed conflict bestows special protection on infrastructure that is indispensable for the survival of the civilian population or the destruction of which may cause severe casualties or prejudice the health and survival of the population (First Additional Protocol to the 1949 Geneva Conventions, arts. 54–56).

28 Guidance may also be found through work carried out by some international organizations and treaties. For example, while ICAO instruments do not define "critical infrastructure" as such, the ICAO Aviation Security Manual refers to the notion of "vulnerable point" as "any facility on or connected with an airport, which, if damaged or destroyed, would seriously impair the functioning of the airport. Air traffic control towers, communication facilities, radio navigation aids, power transformers, primary and secondary power supplies and fuel installations, both on and off the airport, should be considered vulnerable points. Communication and radio navigation aids that could be tampered with should be afforded a higher level of security" (Aviation Security Manual (Doc 8973 – Restricted), para. 11.2.4.9).

China	Critical information infrastructure refers to important network infrastructure, information systems and other facilities in important industries and sectors such as public telecommunications and information services, energy, transport, water, finance, public services, e-government, national defence, science, technology and industry, as well as where their destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people's livelihood, or the public interest (Critical Information Infrastructure Security Regulations, 2021)
France	Vital infrastructure is any establishment, facility or structure for which the damage, unavailability or destruction as a result of a malicious action, a sabotage or terrorism action could directly or indirectly: if its activity is difficultly substitutable or replaceable, severely burden the war potential or economic potential, the national security or the survivability of the nation, or to seriously affect the population's health or life (General Inter-Ministerial Instruction on the Security of Vital Activities, General Secretariat on Defence and National Security, 2014)
Germany	CI refers to organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruptions of public safety and security, or other dramatic consequences (Federal Office for Information Security)
Italy	Material resources, services, IT systems, networks and infrastructure assets which, if damaged or destroyed, would have serious repercussions for crucial functions of society, including the supply chain, health, security and the economic or social well-being of the State and the population (Ministry of the Interior)
Kenya	CI describes assets that are essential for the functioning of a society and economy (such as the electrical grid, telecommunications, water supply) (National Cybersecurity Strategy)
New Zealand	Physical and digital assets, services and supply chains, the disruption (loss, compromise) of which would severely impact the maintenance of national security, public safety, fundamental rights, and well-being of all New Zealanders (Draft Infrastructure Strategy, 2021)
Pakistan	Critical elements of infrastructure, namely assets, facilities, systems, networks or processes the loss or compromise of which could result in: first, 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; or, second, significant impact on national security, national defence, or the functioning of the State (Prevention of Electronic Crimes Act, 2016)
Portugal	CI is defined as a component, system or part thereof that is essential for the maintenance of vital functions for society, health, safety and economic or social well-being, and the disruption of its operation or its destruction would have a significant impact, as it would be impossible to continue to guarantee these functions (Act No. 20/2022)
Qatar	Physical assets, systems or installations which, if disrupted, compromised or destroyed, would have a serious impact on the health, safety, security, or economic well-being of Qatar or the effective functioning of the Qatari Government (Cybersecurity Strategy, 2014)
Russian Federation	CI of the Russian Federation refers to facilities the disruption or discontinuation of whose operation leads to a loss of control, destruction of infrastructure, irreversible negative changes (or failure) of the economy, of a constituent entity of the Russian Federation or its administrative and territorial units or a significant deterioration in the health and safety of people living in these areas over the long term (National Security of Russia – Information 2012)
Saudi Arabia	Infrastructure whose loss or susceptibility to security violations may result in significant negative impacts on the availability, integrity or delivery of basic services or may have a significant impact on national security, national defence, the Saudi Arabian economy or Saudi Arabian national capabilities (Cybersecurity legislation) (Ministry of Foreign Affairs)
South Africa	Means any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, and includes any transport network or network for the delivery of electricity or water (Critical Infrastructure Protection Act, 2019)
Spain	Strategic infrastructure whose operation is essential and does not allow alternative solutions, so that its disturbance or destruction would have a serious impact on essential services (Act 8/2011)
Switzerland	Processes, systems and facilities that are critical to the functioning of the economy and the well-being of the population (National Strategy on the Protection of Critical Infrastructure 2018–2022)
Trinidad and Tobago	CI means computer systems, devices, networks, computer programs and computer data so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, defence or international relations of the State; or provision of services directly related to national or economic security, banking and financial services, communications infrastructure, national public health and safety, public transport, public key infrastructure or any combination of those matters (National Cyber Security Strategy, 2012)
Ukraine	Functions and/or services, the performance of which is ensured by public authorities, local government bodies, institutions, business entities and organizations of any form of ownership, and failures, interruptions and disruptions to the provision of which will have rapid negative consequences for national security (Critical Infrastructure Act, 2021)
United Kingdom	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 (Centre for the Protection of National Infrastructure)
United States	Physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety (CISA)

2.4.1.2 Step 2: Identifying certain sectors as critical

The second step in the CI identification process aims to determine the sectors and subsectors regarded as "critical". A number of sectors are likely to be regarded as critical by all or most Member States. The energy sector is a prime example, as countries are dependent on the provision of electricity for the performance of almost all social and economic functions, from telecommunications and water pumping to the supply of life-saving medical care. At the same time, a certain sector or subsector might be regarded as vital by some Member States only. The size, structure and features of a certain national economy might determine what is critical and what is not. For example, some countries may be heavily dependent on the tourism industry for revenue generation and as a precondition for the maintenance of social cohesion and internal stability. For these countries, designating the tourism industry as "critical" may be necessary to ensure the delivery of essential services to society.

Crucially, the fact that a certain sector is identified as critical does not automatically imply that all underlying services should be critical. For example, in the energy sector a district heating service would most likely not be included as critical at the national level, but the delivery of electrical power would.

2.4.1.3 Step 3: Subsuming specific assets, systems and processes under each critical sector

The third step in the CI identification process links the sectors and subsectors which have been determined as "critical" to a list of individual assets, systems and processes. Numbers can greatly vary from just a few to several thousand, depending on countries' size, level of economic development, and other factors. Some Member States have elaborated sets of indicators which aim to measure the effects of infrastructure breakdown or functional failure. They normally feature a combination of the following:

- Geographical scope of the effect
- Duration of the effect
- Severity of the potential or estimated effects in terms of:
- Economic consequences (impact on GDP, number of employees affected, loss of tax revenue)
    - Number of victims and extent of evacuated population
    - Loss of authority by the Government or disruption of public administration
    - Damage to the environment

A variety of approaches can be used with a view to subsuming specific assets, systems and processes under each critical sector. A consortium led by the Netherlands research organization TNO has sought to group these schematically into three main types:[29]

- First, a service-based approach (such as in Switzerland) where the Government identifies critical assets based on sector-specific criteria defining service-level thresholds and the quantifiable output of the assets (such as the number of megawatts delivered)
- Second, an operator-based approach (such as in France), where the task of determining which assets or services are critical is left to individual CI operators
- Third, an asset or hybrid-based approach (such as in. the United Kingdom), which employs elements of both the service oriented and operator-oriented approaches.

29 European Commission, *Good Practices Manual for CIP Policies for Policy Makers in Europe*, Recommended Elements of Critical Infrastructure Protection for Policy Makers in Europe (RECIPE), 2011. Available at https://repository.tno.nl/islandora/object/uuid:29f15365-8885-4278-82fe-996567858ae9.

CASE STUDY 4
Indicators for qualifying infrastructure as critical: Argentina and South Africa

Argentina

Resolution 1523/2019 has established and defined the criteria for identifying infrastructure as critical with special reference to CII. Those criteria are based on the prospective impact resulting from disruptive conduct, as follows:

- *Impact on human life*: The disruption of a computer system generates a risk of loss of life or serious threat to the health and physical integrity of people.
- *Economic impact*: The disruption of a computer system generates damage or the threat of serious damage to the productive and/or financial structure of the country.
- *Impact on the environment*: The disruption of a computer system negatively affects or seriously damages the space in which living beings develop.
- *Impact on the exercise of human rights and individual freedoms*: Any action carried out through a computer system unduly restricts or curtails the full and collective exercise of the rights enshrined in international treaties, the National Constitution or laws.
- *Public or social impact:* The disruption of a computer system is likely to cause serious shock in a significant part of the population.
- *Impact on the exercise of State functions*: The disruption of a computer system substantially affects the normal functioning of the organs of the executive, legislative or judicial powers.
- *Impact on national sovereignty*: The disruption of a computer system places in jeopardy or restricts the power of the State within the national territory.
- *Impact on maintenance of the national territorial integrity*: The disruption of a computer system leads to the violation of the terrestrial, air or maritime borders of the State.

South Africa

According to the 2019 Critical Infrastructure Protection Act, one or more of the following criteria must be applied in determining whether the qualifying requirements for CI are met:

- The infrastructure must be of significant economic, public, social or strategic importance.
- The country's ability to function, deliver basic public services or maintain law and order may be affected if a service rendered by the infrastructure is interrupted, or if the infrastructure is destroyed, disrupted, degraded or caused to fail.
- Interruption of a service rendered by the infrastructure, or the destruction, disruption, degradation or failure of such infrastructure, will have a significant effect on the environment, the health or safety of the public or any segment of the public, or any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question.
- There are reasonable grounds to believe that the declaration as critical infrastructure will not have a significantly negative effect on the interests of the public.
- The declaration as critical infrastructure is in pursuance of an obligation under any binding international law or international instrument.
- Any other criteria which may, from time to time, be determined by the Minister by notice in the Gazette, after consultation with the Critical Infrastructure Council.

Sources: www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf and www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918.

CASE STUDY 5
Methodologies for CI identification: Australia, France, Germany, Netherlands, South Africa, United Kingdom and European Union

Australia

The criteria and procedures for identifying assets as critical are set out in the 2018 Security of Critical Infrastructure Act. The Act defines what is meant by "critical infrastructure asset" in the various sectors by reference to criteria such as the production capacity of certain assets. For those assets that do not comply with the set criteria, the Minister may privately declare an asset to be a critical infrastructure asset if he or she is satisfied that:

- The asset is critical infrastructure that affects national security.
- There would be a risk to national security if it were publicly known that the asset is critical infrastructure that affects national security.
- The Secretary shall keep a Register of Critical Infrastructure Assets, containing information in relation to those assets. The Register must not be made public.

France

In France, the Government does not identify individual CI assets directly. Instead, it designates so called "vital operators" (referred to as "OIV") in charge of identifying individual assets. According to the Defence Code, a vital operator is identified by the minister in charge (referred to as the "coordinating ministry") of a given sector of activity in consultation with other relevant ministries. The coordinating minister notifies the operator of his or her intention to designate it as a vital operator. The notification process also represents an opportunity for initial consultation between the Government and the operator.

To be designated as a vital operator, operators must fulfil two conditions:

- Their activity is carried out wholly or partly in a sector of vital importance.
- They manage or use at least one establishment, structure or facility whose damage, unavailability or destruction as a result of malicious acts, sabotage or terrorism may have major consequences for the survival capacity of the Nation or the health or life of the population.

The status as vital operators can be acquired by:

- Corporations
- Associations, foundation or international organizations
- State services, local authorities, groups of local authorities, public establishments, independent administrative authorities

In the case of a corporation, a vital operator may be a parent company or a subsidiary. The choice is made after consultation with the relevant operator. Several subsidiaries of the same group may potentially be designated. When an operator is designated by several ministers simultaneously, a consultative process is undertaken to identify which minister will act as the coordinating one. To the extent possible, the coordinating ministry should be the one responsible for the sector of vital importance in which the vital operator carries on its main activity.

As part of its normal activity, a vital operator may have subcontracted or outsourced one or more functions contributing to the achievement of the activity of vital importance. In this case, it is up to the vital operator to take the necessary measures vis-à-vis its subcontractor or its supplier, so that this latter contributes to the achievement of the CIP security and safety objectives.

Following their designation, vital operators elaborate their "operator's security plans". The risk analysis conducted during the elaboration of these plans enables them to propose, as an appendix to their plan, the list of installations, establishments or systems that they consider relevant to be designated as "vital points" (referred to as "PIV").

Germany

The German Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz ("Regulation on the Identification of Critical Infrastructure", known as the "BSI-KritisV") determines which facilities qualify as critical infrastructure in Germany. Classification as "critical infrastructure" depends on two conditions:

- The infrastructure in question must fall into a certain category of the energy, water, food, IT and telecommunications, health, finance and insurance, or transport and traffic sectors;
- The facilities in question must meet certain thresholds in terms of size and importance.

When infrastructure qualifies as critical, two main consequences apply:

- CI operators face a number of obligations, which include, among others, the requirement to report any disruptions or significant impairments, and the implementation of state-of-the-art security.

- Investments by non-European Union or European Free Trade Association (EFTA) investors in companies operating CI are subject to German foreign direct investment (FDI) screening. Investments of 10 per cent or more in a business considered to be CI are subject to mandatory FDI filing as well as a standstill obligation.

On 1 January 2022, the second amendment to the Regulation entered into force. The amendment has had the following effects:

- Broadened the definition of CI, particularly in the IT services and energy sectors by lowering the thresholds for assets to be considered CI.
- Extended the scope of CI in the health sector by introducing the new category of "laboratory information networks", in other words, networks of laboratories in which one laboratory provides IT services for the other laboratories from the same network.
- Added several CI categories in the transport sector, including airport and port operation companies as well as so-called intelligent transportation systems.
- Clarified the concept of "joint infrastructure" as several infrastructure facilities that are necessary for the provision of the same critical service. This can be assumed, for example, if a disturbance of the availability or integrity of one facility could lead to a disturbance of the other facility. If qualified as joint infrastructure, the volume of all joint facilities is aggregated, making it more likely that thresholds are met.

As a result of the recently expanded scope of the CI normative framework, the number of CI facilities in Germany is expected to increase by approximately 15 per cent.

South Africa

The CI identification process starts with the person in control of infrastructure lodging an application with the National Commissioner of the South African Police Service to have such infrastructure declared as critical. The application must include certain information, including the sector in which the primary functions of the infrastructure in question takes place, the resources available to the person in control of the infrastructure to safeguard it against disruptions and to ensure its recovery in case of incidents, the level of risk to which the infrastructure in question is exposed, and the extent to which the declaration as critical infrastructure will promote the interests of the public.

As a general rule, the National Commissioner must publish a notice of the application in the Gazette, conduct a security assessment of the infrastructure in question and submit its evaluation to the Critical Infrastructure Council, which is the inter-agency governmental entity in charge of coordinating CIP-related actions at the national level.

Upon the Council's recommendation, the Minister takes the formal decision as to whether or not the infrastructure in question qualifies being declared as critical. Where infrastructure is declared to be critical, the Minister issues a "certificate of declaration" setting out: first, the risk categorization as determined by the Minister; second, the premises or complex where the critical infrastructure is located; third, the conditions which the Minister may deem necessary to impose for purposes of securing the critical infrastructure; and, fourth, whether information regarding security measures will be restricted.

Netherlands

In 2014, the CI policy of the Netherlands underwent significant reform. This led to a shift from the notion of "critical sectors" to that of "critical processes". Critical processes are those that could result in severe social disruption in the event of their failure or disruption. Since not all processes in a sector are critical, the current focus is on critical processes rather than critical sectors. Identifying critical processes enables the use of tools and scarce resources in a more efficient and targeted manner. The assessment of the level of criticality is performed on the basis of established impact criteria, such as economic damage and physical consequences. The assessment distinguishes between two critical categories, A and B. The failure of A-critical processes has greater potential effects than the failure of B-critical processes. The distinction between A-critical and B-critical can be helpful in prioritizing interventions during incidents and adopting custom solutions for resilience-enhancing measures.

Category A: This includes infrastructure for which disruption, damage or failure meets at least one of the three impact criteria and meets the criterion of cascade effects.

- Economic impact: more than approximately €50 billion in damage or an approximately 5 per cent drop in real income.
- Physical consequences: more than 10,000 dead, seriously injured or chronically ill.
- Social impact: more than one million afflicted by emotional problems or serious problems with basic survival.
- Cascade effects: failure results in the breakdown of at least two other sectors.

Category B: This category includes infrastructure for which disruption, damage or failure meets at least one of the three impact criteria:

- Economic impact: more than approximately €5 billion in damage or an approximately 1 per cent drop in real income.
- Physical impact: more than 1,000 dead, seriously injured or chronically ill.
- Social impact: more than 100,000 people afflicted by emotional problems or serious problems with basic survival.

CASE STUDY 5
Methodologies for CI identification: Australia, France, Germany, Netherlands, South Africa, United Kingdom and European Union (con't)

Each ministry is responsible for performing the assessment of the critical processes that fall under its responsibility. The coordinating ministry, the Ministry of Justice and Security, will regularly examine the methodology to ascertain whether it is up-to-date and will identify if there are indications of possible, new critical processes.

United Kingdom

The United Kingdom has identified 13 national infrastructure sectors. For each sector, one or more lead government departments ensures that protective security is in place for the corresponding critical assets. The so-called "criticalities process" gives each sector's lead government department a common approach to collect and structure data on the critical infrastructure for which it is responsible. The process supports the systematic identification of the essential functions, the critical systems that provide them (and their interdependencies), and the organizations that operate those systems. This information is tied to the impacts that a system's failure would have (both within and across sectors). The criticalities process, in particular, envisages the following steps:

- Step 1: map essential functions
- Step 2: determine systems
- Step 3: assess sector impact
- Step 4: identify supporting systems, relationships and organizations
- Step 5: assess cross-sector impacts

Sources: www.legislation.gov.au/Details/C2018A00029/Html/Text; www.legifrance.gouv.fr/download/pdf/circ?id=37828; www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf; https://english.nctv.nl/topics/critical-infrastructure-protection; and www.cpni.gov.uk/critical-national-infrastructure-0.

CASE STUDY 6
Identifying CI under the Presidential Programme to Counter Urban Terrorism: Colombia

Established in 2017 by Instruction 0002 of 24 March from the Police Intelligence Directorate, the integrated information and intelligence centres (known as "CI3") represent an inter-institutional mechanism for the exchange of information and formulation of strategic courses of action in the face of phenomena and threats that affect citizens' security and coexistence.

Within this organizational model, the unit known as CI3-T focuses on counter-terrorism. Within Ci3-T, the Presidential Programme to Counter Urban Terrorism has been developed under the leadership of the Police Intelligence Directorate and with the support of the Presidential Council for National Security and the Ministry of National Defence. The Programme comprises 16 lines of action, one of which deals with the mapping of critical infrastructure and protection measures and is designed to prevent and avoid the commission of terrorist attacks on strategic assets in Bogotá.

The city of Bogotá currently has 120 critical points, which were selected in meetings of CI3-T. The selection took place through the assessment of compliance with the criteria established for the prioritization of strategic infrastructure that may be the object of potential terrorist actions. These criteria are the following:

- Presence of historical terrorist plans
- Presence of recent terrorist plans
- Presence of imminent terrorist plans
- History of recorded performance of terrorist actions
- Criticality level assessment – impact assessment
- Vulnerable zone: security perimeter, environment with massive presence of people and of places with capacity for high public influx

Based on the above, the infrastructure risk is classified as high, medium or low, and this in turn determines the prioritization guidelines for dealing with terrorist acts.

Source: Permanent Mission of Colombia to the United Nations.

Tool 4

Towards the identification of critical national infrastructure in the national cybersecurity strategy Process – GFCE white paper

https://cybilportal.org/wp-content/uploads/2022/03/White-Paper-Towards-Identifying-CNI-in-the-NCS-Process.pdf

This white paper proposes certain practical considerations and measures whereby countries can develop approaches for identifying CI and CII as part of their national cybersecurity strategy development and implementation processes.

The white paper addresses three foundational elements. A fourth section identifies areas where additional research is needed.

- Section I addresses potential approaches for identifying the ICT risk aspects of CI and CII.
- Section II discusses potential approaches for formalizing the identification of CI and CII in the national cybersecurity strategy and/or law and ways to build a national consensus around the need to protect the most important ICT assets.
- Section III identifies a range of potential governance structures for implementing CNI and CII protection as part of the implementation of the national cybersecurity strategy;
- Section IV identifies research needs for the protection of CI and national CI.

2.4.2. Critical Information Infrastructure

In modern economies, industrial production chains and the delivery of goods and services by both public and private entities are – to a great extent – managed by computer-controlled systems known as industrial control systems (sometimes referred to as "ICS"). Over the past few decades, industrial control systems have progressively gained connectivity to the Internet and to private enterprise networks. This change has streamlined production and service delivery. In addition, as noted by one researcher, "the networking of industrial control systems on a greater scale has led to increased synergy and efficiency, and, due to market needs, real time information for these systems is increasingly important for marketing purposes".[30]

The fact that industrial control systems are increasingly linked to companies' computer systems via the Internet makes them significantly more vulnerable to cyberattacks. Specific security challenges are posed by legacy systems – namely, those industrial control systems that were installed in the pre-Internet era and were not originally conceived for connectivity purposes.

Industrial control systems are used in virtually all CI sectors as they often govern non-stop operations in power plants, dams, bridges, telecommunication towers and other such facilities and are therefore key components of CII. There are a number of national definitions of CII. OECD, for example, defines CII as "those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy".[31]

It is essential that CIP strategies recognize and provide protection to CII on an equal footing to that provided to critical assets in the physical world, all the more so since, as noted by Clemente, "we may be nearing the point where distinctions between 'infrastructure' and 'information infrastructure' are irrelevant, as the two merge into one ever-expanding circle of critical 'stuff'".[32] As the dependence on cyber-enabled infrastructure increases, so too does the proliferation of so-called "critical nodes" – namely, points in a system where failure would significantly degrade the network.

[30] Dana Shea, "Critical infrastructure: control systems and the terrorist threat", Congressional Research Service, 14 July 2003, p. CRS-3. Available at https://digital.library.unt.edu/ark:/67531/metacrs5038/m1/1/high_res_d/RL31534_2003Jul14.pdf.

[31] OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35], OECD, 2008. Available at www.oecd.org/sti/40825404.pdf.

[32] Dave Clemente, *Cyber Security and Global Interdependence*, p. 17.

2.4.3 Interconnections and interdependencies

The delivery of essential goods and services to society is increasingly achieved through the interplay among multiple providers. These cut across all CI sectors and subsectors, forming complex interlinkages. While the interconnectedness of assets, systems and processes is predicated on a more effective management of resources, it increases dependencies. These may be broadly defined as "the relationship between two products or services in which one product or service is required for the generation of the other product or service".[33] For example, food supply relies on transport, the banking and financial sector relies on telecommunications to authenticate transactions and the telecommunications sector depends on the uninterrupted distribution of electricity. Most essential services depend on the simultaneous provision of services from multiple sectors. For instance, health care cannot be delivered in the absence of electricity, water and emergency services at the same time.

- Dependencies can produce effects of varying intensity and can be of different types:
- Physical dependencies: the functioning of one piece of infrastructure depends on the supply of material outputs from another piece of infrastructure.
- Cyber dependencies: the functioning of one piece of infrastructure depends on information transmitted through an information infrastructure.

It is essential to understand that dependencies raise the vulnerability levels of assets. These, in turn, are made more acute by the extensive reliance by government agencies and the private sector on ICT, which exacerbate the effect of cross-sector and transnational dependencies. It has been observed, in this regard, that "the scenario which causes the highest degree of concern among experts is the combined use of a cyberattack on critical infrastructure in conjunction with a physical attack. This use of cyberterrorism could result in an amplification of the physical attack's effects. An example of this might be a conventional bombing attack on a building combined with a temporary denial of electrical or telephone service. The resulting degradation of emergency response, until back-up electrical or communication systems can be brought into place and used, could increase the number of casualties and public panic".[34]

When vulnerabilities turn into breakdowns as a result of a terrorist attack, dependencies may produce cascading effects. For example, the spreading of toxic substances in the water supply chain leads to failures in the health-care system.

It is critically important for CIP strategies to leverage the causal relationship that exists between CI interconnections, dependencies and vulnerabilities as a way to:

- Achieve an adequate level of understanding (on the part of all involved stakeholders, whether from the private or public sector) of systemic vulnerability points, which should be reflected in more accurate risk and crisis management. The task of integrating the concept of dependencies in risk and crisis management processes is made more complex by the fact that dependencies can change depending on the mode of operation of a certain piece of CI. For example, while normally a hospital does not rely on diesel fuel, following a breakdown in the electricity system it may become suddenly dependent on diesel supply to operate its emergency power generator. CIP strategies should frame dependencies in a non-static manner, but rather in terms of dynamic and rapidly shifting relationships.
- Raise awareness of mutual dependencies through inter-sectoral networking (based, for example, on the discussion of risk scenarios), in order to stimulate further cooperation between the various players.

Interconnections and dependencies often cut across borders, which entails the need for CIP strategies to also address their international dimension. This aspect is further examined in chapter 6.

---

[33] CIPRNet Project, https://ciprnet.eu/home.html.

[34] Dana Shea, "Critical infrastructure: control systems and the terrorist threat", p. CRS-8.

CASE STUDY 7
Interdependencies and the "vital zones": France

The French CIP strategy operationalizes the notion of dependencies by introducing the concept of "vital zone" ("zone d'importance vitale", or ZIV). A vital zone is an area in which several "vital points" ("PIVs") belonging to different "vital operators" ("Ds") are implanted, and for which a joint security assessment and management presents added value. In terms of security, there is interdependence between PIVs when:

- The carrying out of a threat on one of them would have consequences on the integrity or the activity of the others, or
- Security measures implemented for one vital point or across a shared area affect the security of one or more other vital points.

Three types of geographical areas exist:

- Case 1: An area consisting of neighbouring vital point, which are contiguous or located at a relatively small distance from one another.
- Case 2: An area consisting of enclosed vital points, such that a vital point "2" is found inside a vital point "1".
- Case 3: A zone combining the characteristics of the first two cases.

In any case, the creation of a vital zone must fulfil an operational need and contribute to improving the protection of vital points by pooling and streamlining resources. The concerned area should be understood as a zone with homogeneous characteristics, such as may be found in certain industrial zones, airports or sea or river ports.

Source: https://www.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf..

CASE STUDY 8
Intersectoral and knowledge-sharing workshops about dependencies: the Netherlands

Under its CIP strategy, the Netherlands ran a series of intersectoral workshops enabling CI sectors to gain insights into the effects of reciprocal dependencies. The participating stakeholders identified the technical and organizational networks in which critical sectors operate. This enabled a mix of public and private parties to anticipate and discuss threat scenarios. No specific models were used for examining dependency analyses, the underlying idea being that knowledge exchange through networking and expertise-sharing would allow sectors to become more aware of dependencies and how to address vulnerabilities. Moreover, the parties involved would become more acquainted with each other and their respective capabilities, thus increasing the potential for effective cooperation in the event of accidents. The scenarios were notably used to discuss:

- Effects of CI disruptions, for example whether direct or indirect, to the supply chain, affecting access, scarcity or integrity, the time period of disruption, sector characteristics and human factors
- Dependencies, redundancies and recovery
- Measures to reduce vulnerabilities

Source: https://www.researchgate.net/publication/261987293_RECIPE_Good_Practices_Manual_for_CIP_Policies.

2.5 Designing the CIP architecture

In the absence of an international legal instrument determining which institutional model Member States need to adopt to protect CI located on their territories, Governments are expected to choose the framework that best matches the size and structure of their economies, their public policy culture and established institutional practices. CIP governance architectures should notably take into account the basic constitutional structure of the country, in other words, whether they are unitary and centralized or federal and decentralized States. This is especially important in assigning roles and responsibilities to the various levels of Government.

2.5.1 Main governance models

CIP architectures fluctuate between two basic models. At one end of the spectrum, CI governance is based on principles of self-regulation, incentives and voluntary compliance. The so called "voluntary approach" underlines policies focusing on non-binding guidance. Under this model, all stakeholders (whether from the public or private sector) are encouraged to contribute to the definition and implementation of the CIP policy by way of recommendation, persuasion and the creation of a shared perception of pursuing a common goal. The binding force of legislation and regulatory schemes is used lightly and only as a complementary tool, except in certain sectors – such as the nuclear sector – where it may take a predominant role.

At the other end of the spectrum is the so called "mandatory approach", based on the premise that cooperation in the CIP field is best achieved through the establishment of binding legal frameworks accompanied by sanctions for CI operators that fail to comply with required security standards.

In practice, countries adopt elements of both approaches. Their systems can only be defined as being predominantly "voluntary" or "mandatory". Examples of the former are Canada, Switzerland, the United Kingdom and the United States. Examples of the latter are Belgium, Estonia, France and Spain,.

It may be difficult for countries to determine which model best fits their needs. When, in particular, they establish CIP policies for the first time, they might adopt structures and processes that eventually prove to be inadequate. For this reason, countries often set up mechanisms to ensure that strategies are periodically subject to revision. The United States offers an example of a country that started with a pure concept of voluntary participation of CI operators in the process. While its system is still based on this principle, over time it has increasingly seen the need to strengthen its legal framework for CIP protection. The lesson here is that countries should learn from experience.

Table 3
CIP institutional frameworks in selected Member States

Australia	A central pillar of CIP efforts in Australia is the 2018 Security of Critical Infrastructure Act, which provides a framework for managing risks to national security relating to CI, including by: • Improving the transparency of the ownership and operational control of CI in Australia in order to better understand those risks. • Facilitating cooperation and collaboration between all levels of government, regulators, CI owners and operators, in order to identify and manage those risks. In support of the above-mentioned objectives, the institutional framework consists of the following elements: • Maintaining a register of information in relation to CI assets (the register is not public). • Requiring certain entities relating to CI asset to provide information in relation to the asset, and to report if certain events occur in relation to the asset. • Allowing the competent minister to require certain entities relating to a CI asset to perform, or refrain from performing, an action or process if the minister is satisfied that there is a risk of an act or omission that would be prejudicial to security. • Allowing the Secretary of the Department of Home Affairs to require certain entities relating to a CI asset to provide certain information or documents. • Allowing the Secretary to undertake an assessment of a CI asset to determine if there is a risk to national security relating to the asset. In 2022, the Security of Critical Infrastructure Act was amended with the introduction of new provisions, which include: • Obligation for specified CI assets to adopt and maintain a CI risk management programme. • Additional cybersecurity obligations that may be applied in relation to systems of national significance. • Provisions whereby directions facilitating government assistance to industry in the event of a serious cybersecurity incident prevail over the requirements of a risk management programme. • Amended provisions authorizing the use and disclosure of protected information. • Provisions whereby the minister's authority to declare an asset as CI asset includes the power to require compliance with a risk management programme. • Power of the minister to declare a CI asset to be a system of national of significance.

Canada	The CIP architecture has a strong voluntary component. Responsibilities are shared by federal, provincial and territorial governments, local authorities, and CI owners and operators. All these entities are represented in national sector networks (for each of the 10 identified CI sectors) whose goals are to: • Promote timely information-sharing. • Identify issues of national, regional or sectoral concern. • Use subject-matter expertise from CI sectors to provide guidance on current and future challenges. • Develop tools and best practices for strengthening the resiliency of CI across the full spectrum of prevention, mitigation, preparedness, response and recovery. Participation in these networks is voluntary. Their members also direct sector-specific work plans. To maintain a comprehensive and collaborative approach to enhancing the resiliency of critical infrastructure, a National Cross-Sector Forum promotes information-sharing across the sector networks and address cross-jurisdictional and cross-sectoral interdependencies.
France	CIP coordination is ensured by the General Secretariat for Defence and National Security on behalf of the Prime Minister. The General Secretariat approves the national security directives drafted by the coordinating ministries in each critical sector. Those ministries are also the operators' points of contact. Zone and department prefects (in other words, the State's representatives in a department or region) act under the overall guidance of the Ministry of the Interior as the territorial coordinators of the CIP strategy. Once designated, operators shall take several steps, notably: • Appointment of a delegate for defence and security (privileged interlocutor with the administrative authority) • Drafting of an operator's safety plan which sets out the operator's safety policy • Drafting of a specific protection plan for each of the vital points identified
Germany	The country's CIP architecture is based on the identification of six work packages corresponding to different phases of the risk management cycle. The public sector (under the coordination of the Federal Ministry of the Interior and Community) takes the lead on the implementation of the first four packages with the collaboration of the private sector and CI operators. In the implementation of packages 5 and 6, the roles are inversed, with companies and operators acting as the lead entities. The work packages are the following: • Definition of general protection targets. • Analysis of threats, vulnerabilities and management capabilities. • Assessment of the threats involved. • Specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment; if and where required, legislation. • Implementation of goal attainment measures primarily by means of, first, association-specific solutions and internal regulations; second, self-commitment agreements by business and industry; and third, development of protection concepts by companies. • Continuous, intensive risk communication process (dialogue on analysis findings, assessments, protection targets, and action options). The system envisages a number of institutionalized platforms involving public authorities, companies and associations. While this overall architecture did not initially differentiate between institutional approaches to physical security and cybersecurity, the existing CIP architecture has been complemented by the German 2001 Cybersecurity Strategy. The Strategy describes the long-term cybersecurity policy objectives of the German Government (including to foster CI operators' business continuity) and digital sovereignty, and provides a strategic framework for the State, private sector and civil society through guidelines, operational and strategic goals.
Spain	Acting through the National Centre for the Protection of Critical Infrastructure, the Secretary of State for Security is the highest body of the Ministry of the Interior responsible for CIP. For each strategic sector, at least one entity of the General State Administration is designated with responsibilities to promote, within its scope of competence, the Government's security policies and for ensuring their application. In terms of engaging CI operators, Spain is a typical example of what may be called the "mandated approach". The system is based on detailed regulatory provisions requiring the adoption of various layers of strategic and security plans whose elaboration and approval rests with different entities within specific time frames. These include the following plans: • National plan for CI protection: this establishes criteria and guidelines to mobilize the operational capacities of public administrations in coordination with CI operators. • Sectoral strategic plans: these enable the scoping of the essential services in each of the identified sectors, system vulnerabilities, the potential consequences of inactivity and the strategic measures necessary for the system's resilience. • Operator's security plans: these define CI operators' general policies to ensure the security of the facilities or systems that they either own or manage. They must be submitted within six months of the notification of the operator's designation by the Ministry of the Interior. • Specific protection plans: these determine the specific measures to be adopted by CI operators to ensure the security of CI. They must be submitted within four months of the approval of the operator's security plan by the Ministry of the Interior. • Operational support plans: these set forth the specific measures to be implemented by the public administrations in support of CI operators.
Netherlands	Primary responsibility for the continuity and resilience of critical processes is borne by their actual operators. These are expected to gain insight into threats, vulnerabilities and risks, and also to develop and maintain capacities that increase and safeguard the resilience of critical processes. Responsible ministries establish general frameworks for the sectors that fall under their responsibility (via policy or regulatory instruments). The ministries, in association with the operators of critical processes, are responsible for safeguarding and inspecting capabilities related to CI. The National Coordinator for Security and Counterterrorism of the Ministry of Justice and Security is the entity responsible for overall coordination and management tasks.

Saudi Arabia	The High Commission for Industrial Security ensures the protection of critical infrastructure (oil, industry, and services) against terrorist attacks, primarily those carried out with the use of drones and small boats. In collaboration with different military and security institutions, the High Commission is in charge of elaborating counter-terrorism policies with regard to CIP. It also provides specific instructions, notably the following: • Industrial safety regulatory directives: published in Ministerial Decision 11131 11131 of 22 Dhu al-Qadah 1430 (10 November 2009), these include many administrative requirements to establish industrial security departments inside CI facilities to enhance capacities to resist and counter terrorist attacks. Such requirements include: security hierarchy and organizational structure; requirements for employment in industrial security; regulatory rules for industrial security. • Security directives: issued by Ministerial Decisions 5100 and 5101, 02/07/1438 (Arabic calendar), these include chapters dealing with building security systems to enhance the security and integration with different regulatory and security agencies: security systems at industrial facilities; security fencing systems; pipelines and pipeline corridors; facilities with a marine interface; security management at industrial facilities; security communications and data networks. • Safety and fire protection directives: issued by Ministerial Decisions 5098 and 5099, 02/07/1438 (Arabic calendar), these deal with: general requirements for safety fire protection directives; plant layout, spacing and access; onshore and near-shore well-site safety; pressure piping transport pipelines and pressure vessels; manufacture transport storage and use of explosive materials; mines and mineral processing plants; pre-incident planning and management of emergencies; Incident reporting and investigation. The above-mentioned directives form a homogeneous and integrated security management system under the supervision of the High Commission.
United Kingdom	The Civil Contingencies Secretariat, part of the National Security Secretariat, supports the Prime Minister and Cabinet, and leads the wider government effort on civil emergency planning and response. Particular policy responsibilities of the Secretariat are the following: • National Risk Assessment and National Risk Register (identifying and assessing risks to national safety and security arising from terrorism, major industrial accidents and natural hazards, over five years) • National Security Risk Assessment (identifying global risks to United Kingdom security interests, in a 5-to-20-year time frame) • Leading a cross-government resilience capabilities programme to improve public sector response to such emergencies • Contingency planning and capability building for the risks of catastrophic emergencies • Policy for secure and resilient national infrastructure, and corporate resilience in the private sector Working with CI owners and regulators, the government departments responsible for the 13 critical sectors are required to produce sector security and resilience plans on an annual basis. These plans, which are based on the risks identified in the National Risk Assessment, set out each department's understanding of the risks to its sectors and the key activities that it will undertake to address those risks during the year ahead. Several agencies provide central government, regulators and Infrastructure owners and operators with advice on Infrastructure risks and mitigation, notably the Centre for the Protection of National Infrastructure and the National Cyber Security Centre. No explicit sanctions or other consequences are set in the event that a CI operator fails to engage in cooperation with Government.
United States of America	The Secretary of Homeland Security provides strategic guidance and coordinates the overall federal effort. Sector-specific federal agencies lead collaborative processes for CI security within each of the 16 CI sectors. Each such agency is responsible for developing and implementing a sector-specific plan based on the unique characteristics of each sector. State, local, tribal and territorial governments ensure the security and resilience of CI under their control, as well as that owned and operated by other parties within their jurisdictions. The mechanisms for collaboration between private sector owners and operators and government agencies are articulated around several sector-specific and cross-sectoral coordination structures.

2.5.2 Public-private partnerships for CIP

Addendum to the Madrid Guiding Principles

Guiding principle 51

In their further efforts to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider:

...

(c) Establishing processes for exchanging risk assessments between Government, industry and the private sector, to promote and increase situational awareness and strengthen soft target security and resilience;

...

(e) Promoting public-private partnerships by developing cooperation mechanisms, supporting business owners and operators and infrastructure managers and by sharing plans, policies and procedures, as appropriate

In most countries, the vast majority of critical assets are privately owned. This circumstance, combined with the fact that the main responsibility for protecting CI assets and systems rests with their owners and operators, highlights the importance of establishing effective PPPs in order to achieve adequate levels of CI resilience.[35]

In dealing with PPPs, drafters of CIP strategies should aim at creating the conditions for their effectiveness by, first, defining their scope; second, determining their forms; and third, anticipating problems and challenges.

2.5.2.1 Defining the scope

PPPs should not focus on one particular stage of the protection cycle, but encompass all of them, from the design of security plans to crisis management and recovery. The benefits of resource pooling, mutual support and joint decision-making between the public sector and private CI operators extend to such areas as security assessments, review of security measures, critical asset and process identification, the elaboration of contingency plans, incidence response training, and others.

Information-sharing is a crucial – albeit not exclusive – dimension of PPPs and raises specific challenges such as in the field of data protection. Key issues related to information-sharing are examined in chapter 4.

2.5.2.2 Determining the forms

The most appropriate form of a given PPP depends on multiple considerations such as the objectives sought, the number of stakeholders to be involved and whether the partnership is expected to address strategic or operational issues. PPPs can take a variety of forms, ranging from very informal types of cooperation to more formal settings. The degree of formality is often linked to the level of control that government agencies aim to exercise. From a different angle, it has been argued that so-called "project-oriented" PPPs tend to be more effective than "process-oriented" ones, as the former would generally include more clearly defined missions, timelines and budgets.[36]

2.5.2.3 Anticipating problems and challenges

PPPs that are not accurately thought through are exposed to the risk of becoming what are sometimes termed "empty boxes", bringing limited or no added value to CIP. In order to ensure that public-private cooperative arrangements are born and continue to remain relevant and productive endeavours, it is necessary for Member States to bear in mind the most recurrent reasons for failure. Shortfalls may be rooted in expectation gaps between the private and the public sector, unsustainable funding models, unclear divisions of labour, and other such factors. Arguably, as noted in a 2017 issue of World Security Report, "preferences and the cost-benefit perceptions of the participating actors will ultimately determine the success or failure of the partnership. A sense of urgency helps to create a bond between the public and the private sectors, fostering a willingness to collaborate and achieve a common vision, ultimately allowing the partnership to mature and endure. The longevity of the partnership depends on the interplay between these factors and is a dynamic process with periods of both weak and strong performance".[37]

Other challenges may be associated with lack of motivation for operators to invest financial resources on the protection of their own CI. Section 2.7.2 discusses the need for CIP strategies to identify the appropriate types of incentives in this regard.

---

35 The process of privatization of several CI sectors and subsectors such as gas, postal systems and telecommunications services, which has historically occurred in many countries, has resulted in certain CI operations falling into private hands. This, in turn, has generated the need for strong PPPs. Information exchange for CIP purposes in a vital task to be performed under such partnerships.

36 Lina Kolesnikova, "Challenges for PPP in time of new types of security threats", *World Security Report*, January-February 2017. Available at https://issuu.com/torchmktg/docs/wsrjanfeb17/15.

37 Ibid.

Box 8
Values underpinning effective PPPs for CIP

The Meridian Process, an open forum for the exchange of ideas on CIP and collaboration among senior government policymakers, has identified a series of key factors underpinning effective PPPs for CIP:

- Trust: As PPPs often concern sensitive subjects, it is essential to create an atmosphere of trust in which all organizations show awareness of one another's need for discretion. Clear membership guidelines regarding operating rules may support trust building efforts.
- Value: PPPs need to produce benefits as a condition to sustain participants' enthusiasm and motivation over time.
- Respect: Each involved entity has to recognize the added value that the other entities bring to the collaborative endeavour.
- Code of conduct: It is necessary to have clear, specific and predictable rules that do not provide scope for discretion and prevent any conflict of interest.
- Awareness of one another's possibilities and restrictions: This prevents conflict through misjudgement of the reason for a negative response and allows for an optimum return on the efforts being undertaken. This implies that each organization should be familiar with other organizations' business.
- Realistic expectations: Involved entities have to take into consideration the affordability of resources, development budget and other factors, to be able to develop realistic expectations from the PPP in question.

Source: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

CASE STUDY 9
Public-private partnerships for CI resilience: Finland

In Finland, the National Emergency Supply Agency is entrusted with planning, developing and maintaining the security of supply in the country. While its historical role of maintaining reserve stockpiles to protect the livelihoods of the population and also the functioning of the economy remains part of its strategic tasks, the Agency is increasingly active in mainstreaming business continuity and resilience in various sectors of the economy through public-private partnerships.

The National Emergency Supply Agency has established a network of thematic clusters where key stakeholders of critical sectors develop partnerships in order to assess vulnerability and performance as well as plan for resilience. It also proposes dedicated tools, such as information systems, storage and transport facilities to support business continuity on these domains. In addition, the Agency finances specific activities related to business continuity and critical infrastructure protection. It prepares annual reports that evaluate the performance of companies in the critical sectors including ranking and specific recommendations. Among its results, the Agency boasts an increased number of PPPs with companies in critical sectors (there now more than one thousand such partnerships), which all yielded a business continuity plan specific to their activities and sector.

Source: https://www.oecd.org/governance/toolkit-on-risk-governance/home/.

CASE STUDY 10
UP KRITIS public-private partnerships platform for CIP: Germany

Institutionalized in 2007 and adjusted in 2013, UP KRITIS is the German PPP ensuring sectoral and cross-sectoral cooperation for CIP. Mutual trust underpins its work. Participants exchange know-how and experiences and learn from one another with regard to CIP. Within the framework of UP KRITIS, concepts are developed, contacts established, exercises held and a joint approach for IT crisis management developed and launched. At the same time, UP KRITIS deals with topics which go beyond the IT area, based on the recognition that a separate examination of physical security and IT security is not sufficient to achieve the joint goal of critical infrastructure protection.

Within UP KRITIS, two forms of cooperation take place: operative-technical cooperation (between all participants) and strategic-conceptual collaboration (in the established bodies). Crucially, business is involved in an incremental manner and can be more or less intense, depending on companies' availability for proactive engagement, the goal being to ensure that the system remains manageable while reaching out to as many companies as possible from all CI sectors. In particular, an organization is first integrated into UP KRITIS as a "participant". All Germany-based CI operators, national professional and sectoral associations from the CI sectors, as well as the competent government authorities, can apply to become participants in UP KRITIS. Participants appoint representatives for their organization, who are granted access to the products of UP KRITIS, including confidential information. If an organization wishes to collaborate more actively, it can become a "partner" and apply for the integration of its representatives into sectoral working groups and thematic working groups. Each working group constitutes an information network of its own, in which information can be exchanged on a confidential basis.

Other key components of the organizational structure are the Plenum and the Council. The Plenum is the cooperation committee of the system. It acts across sectors by setting the strategic key activities of UP KRITIS, deciding on the establishment or dissolution of working groups, planning future joint action and other measures. The Plenum consists of representatives of the CI operators, their professional and sectoral associations, and also representatives from the public sector. The Council strengthens partnership and cooperation within UP KRITIS and provides impetus for strategic goals and projects. It also ensures that the platform can perform its tasks using adequate resources and with the necessary support of management from the public and private sectors. The Council consists of high-ranking decision-makers drawn from the CI operators and the public sector.

Following the adoption of the IT Security Act in 2015 and several amendments of the Federal Office of Information Security (BSI) Act, the categories of CI entailing legal obligations for their operators are currently specified in the BSI Act in conjunction with the BSI Kritis Ordinance. In particular, Section 8a of the BSI Act requires CI operators to take appropriate organizational and technical precautionary measures in order to avoid disruptions to the availability, integrity, authenticity and confidentiality of their IT systems, components or processes that are decisive for the functionality of the CI operated by them.

The Federal Office of Information Security exercises a supervisory function pursuant to the BSI Act in relation to CI operators. This supervisory function is complemented by a cooperative role at a strategic and operative level within UP KRITIS, which aims to improve the protection of CI across sectors. The cross-sectoral cooperation between industry and the State within UP KRITIS has become a success, with over 750 organizations cooperating on the basis of mutual trust within sectoral and thematic working groups. At the same time, UP KRITIS deals with topics which go beyond the IT area, based on the recognition that a separate examination of physical security and IT security is not sufficient to achieve the joint goal of critical infrastructure protection and resilience. A constructive dialogue between the Government and CIP operators on future developments relating to the physical security and resilience of critical CI remains necessary. UP KRITIS thus offers a forum for exchange between the Government and CIP operators on new and upcoming legislation, such as forthcoming European Union directives on topics of relevance for CIP.

Source: Information provided by the Permanent Mission of Germany to the United Nations.

Tool 5
Handbook to Assist the Establishment of Public-Private Partnerships to Protect Vulnerable Targets – UNICRI

The Handbook was developed following a series of workshops, expert meetings, action-oriented analysis and testing events. Aimed at security practitioners from public entities and private companies, it follows a 10-step methodology and offers several tools to assist in the creation or enhancement of PPPs to prevent and respond to security threats involving vulnerable targets in general (soft targets and critical infrastructure) at national and local levels.

Tool 6
Eight-step guidance on PPPs for CIP – OSCE

www.osce.org/files/f/documents/4/b/103500.pdf

OSCE has elaborated basic eight-step guidance on how countries should maximize the benefits that PPPs can obtain by leveraging the common interests of all involved stakeholders. While the guidelines were developed in the framework of good practices for critical energy infrastructure, they appear to be generally applicable across sectors:

- Step 1: Analyse and identify the motivation of each partner to be included in CIP partnerships in order to clarify mutual expectations and contributions.
- Step 2: Define ambitions and goals of CIP partnerships based on overall national CIP goals; clarify the purpose of CIP partnerships and the tasks to be accomplished (see also step 5).
- Step 3: Screen the existing regulatory framework relevant for each critical infrastructure sector; identify mandatory and self-binding norms, rules and principles; assess the adequacy of the existing regulatory framework in view of expected risks and existing preparedness levels; discuss how to close possible gaps.
- Step 4: Provide mechanisms, protections and legal certainty for the exchange of CIP-related information among all stakeholders involved. In addition, provide mechanisms for voluntary efforts, including the development and exchange of best practices, consultation and dialogue to ensure ongoing and effective partnerships.
- Step 5: Set up an institutional structure that fosters cross-organizational cooperation and information exchange; clarify the roles and contributions of each partner (for example, government agencies, owners and operators of critical infrastructure, product suppliers, associations); identify single points of contact for each partner; establish guidelines for cooperation.
- Step 6: Start small by focusing on one or two critical infrastructure sectors; grow steadily while building on the readiness of all stakeholders to cooperate and consider threat levels.
- Step 7: Define critical milestones to review what has been achieved and identify potential next steps.
- Step 8: Provide for a constant review process to revisit and update partnerships to ensure continual progress commensurate with the overall risk landscape and the safety and security measures that are needed to provide an optimal level of protection.

2.5.3 Role of civil society and the public

The public at large has an important role to play in both preventing attacks against CI and reducing damage once an attack has occurred (crisis management). Some Member States explicitly envisage the role of individuals in the context of CIP strategies. For example, the French Plan Vigipirate[38] instructs citizens how to behave in the event of attacks in specific contexts which are relevant for the protection of CI, such as in the metro and on trains, aeroplanes and ships, or in the event of attacks with a toxic product. Sweden implements a whole-of-society approach, following recognition that individuals and families are often the ones affected most directly by a crisis, or are present on site before first responders or other social representatives. Individuals should be viewed as assets.[39] In the aviation sector, the so-called "security culture" initiative introduced by ICAO aims to assist entities operating in the aviation industry in enhancing the implementation of aviation security measures by a well-trained, motivated and professional workforce, and raising awareness among the public (see box 9).

The methods and channels for achieving collaborative attitudes on the part of the public differ substantively from those required to engage CI operators. As a starting point, the involvement of communities and individuals in overall CI resilience efforts entails the enactment of broad education programmes and awareness-raising campaigns. Communication strategies should differ in accordance with the target group. These strategies can be supported, at the local level and depending on the context, by measures such as the establishment of dedicated emergency numbers, the repetition of

[38] See https://www.gouvernement.fr/vigipirate.

[39] Helena Lindberg and Bengt Sundelius, "Whole-of-society disaster resilience: the Swedish way", in *The McGraw-Hill Homeland Security Handbook* (2nd edition), David Kamien (ed.), New York: McGraw-Hill, 2013, pp. 1295–1319. Available at https://www.semanticscholar.org/paper/Whole-of-Society-Disaster-Resilience-%3A-The-Swedish-Lindberg-Sundelius/9524aa4182828716ba5834c40ee6128f8674f54f.

messages in loud-speakers reminding users of public transport about their reporting duties, among others. Following waves of terrorist attacks in the transport systems of major capitals over the past twenty years, for example, the public administrations of several countries have implemented measures to encourage citizens to be alert and report suspicious situations to the authorities.

Widespread use of technological products by the public also means that social media can be instrumental in increasing situation awareness, inform individuals about actions being taken by the Government and deliver safety and security instructions in a timely manner. All of this appears to be especially relevant in rapidly evolving crisis scenarios.

Box 9
ICAO "security culture" initiative

In stipulating that ICAO should continue developing tools to enhance security awareness and security culture, ICAO resolution A40-11 identified security culture as a top priority.[40] In pursuit of this goal, the year 2021 was designated the "Year of Security Culture". Accordingly, ICAO has focused its work on the following priority activities:

- Conduct of a global security culture campaign, which will support the organization of national, regional and global events to raise security awareness in aviation.
- Intensifying collaboration with Member States and industry in supporting efforts to promote security culture in the greater aviation community, where security is everyone's responsibility.
- Issuing relevant guidance on practical security culture communication strategies, plans and campaigns.
- Continuing to offer training and assistance focused on promoting an effective and sustainable security culture within all organizations involved in civil aviation.

Member States, the United Nations family, international and regional organizations and industry stakeholders worked together on a campaign to support and promote the Year of Security Culture by delivering and supporting global security culture events (conferences, seminars, training courses, workshops and webinars) throughout 2021. While the campaign officially closed in 2022, work is set to continue, with the Year of Security Culture providing the impetus for a permanent focus on security culture by all in the civil aviation.

The ICAO Security Culture website[41] provides the global aviation community with security culture best practices and contains guidance documents, videos, articles and training links from States and industries, along with free-of-charge ICAO tools and resources in all United Nations official languages, including an ICAO toolkit on enhancing security culture and a starter pack for the ICAO security culture campaign.

40 Resolution A40-11 was adopted by the ICAO Assembly at its fortieth session, in 2019. Text available at https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_en.pdf.

41 See https://www.icao.int/Security/Security-Culture/Pages/default.aspx.

CASE STUDY 11
Methods for emergency population warning: Chile, France and the United Kingdom

Chile

Since its inception in 2012 and through its official implementation in 2017 onwards, Chile has been using an emergency alert system to send alerts and information about natural disasters such as floods, wildfires, tsunami and earthquake warnings. Since 2017, all cell phones on sale in the country are required by law to be compatible with the system. Although it is designed to respond to natural disasters, the system could potentially be deployed in the event of massive human-caused disasters.

France

The French Reseau National d'Alerte ("National Alert Network") is in place with the aim of warning of the imminence of a situation involving the security of the population. Made up of approximately 4,500 sirens,

the alert may be triggered, for example, in the event of a toxic or explosive cloud, a radioactive risk, a threat of aerial aggression and certain natural risks. The sirens emit a modulated signal, rising and falling, composed of three sequences of 1 minute 41 seconds, separated by a silence of 5 seconds. Upon hearing the signals, members of the population are expected to take such steps as going without delay to an enclosed room, switching off air conditioning, heating and ventilation and listening to the radio.

United Kingdom

The national mobile phone alert system is an emergency population warning system currently in development that uses cell broadcasts. Early testing began in 2014, with the first test alert sent in March 2020. The system is intended for use in major crises, such as flooding or terror attacks.

Cell broadcast technology involves sending messages to multiple mobile telephone users in a defined area at the same time. Cell broadcast messages are directed to radio cells as opposed to a specific telephone. As it is not affected by traffic load, cell broadcast is of particular interest in the event of acute crises when spikes in data loads (social media and mobile apps), regular SMS and voice call usage (mass call events) tend to significantly congest mobile networks.

Sources: http://www.sae.gob.cl; https://www.alpes-de-haute-provence.gouv.fr/Actions-de-l-Etat/Securite-et-protection-des-populations/Protection-civile/Le-reseau-national-d-alerte-sirene/Les-sirenes-d-alerte; and https://www.gov.uk/alerts.

2.6 Building CIP strategies around the concepts of risk management and crisis management

Addendum to the Madrid Guiding Principles

Guiding principle 50

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

...

(b) ... regularly conduct risk assessments to keep pace with the evolving nature of the threat and adversary, including by utilizing existing tools and guidance developed by international and regional organizations;

...

(d) Take preparedness measures, including to ensure effective protection of, and responses to, such attacks, that are informed by comprehensive risk assessments;

...

(f) Promote risk-based and mutually reinforcing efforts to protect critical infrastructure and soft targets

To be effective, any national strategy needs to place risk management and crisis management processes at the core of CIP efforts. Whether a voluntary or mandatory protection model is chosen, stakeholders involved in CIP (whether private-sector CI owners and operators or public authorities) need to be familiar with these concepts and consistently apply them within their respective sectors and fields of competence.

In the context of CIP efforts against terrorism, risk and crisis management can be seen as the key tools to achieve optimal levels of resilience. This latter concept is understood as the ability of specific CI, an entire critical sector or the members of affected communities to withstand the distress caused by one or more terrorist acts. Ideally, resilient infrastructure is one that not only recovers from a crisis, but also learns from past crises to become stronger in the face of future threats.

2.6.1 Risk management

The United Nations Office for Disaster Risk Reduction defines risk management as the "systematic approach and practice of managing uncertainty to minimize potential harm and loss. Risk management comprises risk assessment and analysis , and the implementation of strategies and specific actions to control, reduce and transfer risks. It is widely practiced by organizations to minimize risk in investment decisions and to address operational risks such as those of business disruption, production failure, environmental damage, social impacts and damage from fire and natural hazards."[42]

In the context of CIP, it is important to have a clear understanding of the key concepts underpinning the risk management concept and related processes. These may be defined as follows:

- *Threat*: whatever exploits a vulnerability of CI.
- *Consequence*: result of specific types of attacks on specific CI.
- *Vulnerability*: weakness of CI that may be exploited by a threat.
- *Risk*: potential for loss, damage, destruction or interference in the ability of CI to deliver its services as a result of a threat exploiting a vulnerability.

In order to identify and implement the most effective risk mitigation measures, risk management systems should first detail the mechanisms for obtaining valid threat-related information and conducting adequate threat assessments. These should take into account local, national and international circumstances. Within existing financial and technical constraints, the resulting mitigation measures should be proportionate to the nature and level of the assessed risk. The system should also be built with the necessary flexibility so as to ensure that it can quickly adapt to rapidly changing security landscapes.

[42] 2009 T terminology on disaster risk reduction. Available at https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction.

Box 10
ISO standards on risk management

The International Organization for Standardization (ISO) is an independent, non-governmental organization with a membership of 162 national standards bodies. Through its members, ISO brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to global challenges. ISO has published more than 22,000 international standards and related documents covering almost every industry, from technology to food safety, agriculture and health care.

ISO 31000 was developed by the ISO technical committee on risk management as a standard applicable to all organizations regardless of type, size, activities and location. It covers all types of risk and is intended for use by anyone who manages risks, not just professional risk managers. ISO 31000 specifically seeks to help organizations to develop a risk management strategy to effectively identify and mitigate risks, thereby enhancing the likelihood of achieving their objectives and increasing the protection of their assets. Its overarching goal is to develop a risk management culture where employees and stakeholders are aware of the importance of monitoring and managing risk.

Following the same risk management approach as ISO 31000, the ISO 27000 series provides the reference standard in the field of information security systems. ISO 27000 thus offers a guiding framework for the protection of CII.

A connected standard, developed by ISO in 2021, deals with travel risk management. This requires organizations to anticipate and assess the potential for events, develop treatments and communicate anticipated risk exposures to their travellers. Advising and providing travellers with adequate medical and emergency response guidance, security and information security precautions, including challenges to travel logistics, can have impacts on the outcome of disruptive events, including when they involve CI.

Sources: https://www.iso.org/iso-31000-risk-management.html/; https://www.iso.org/standard/73906.html; and https://www.iso.org/standard/54204.html.

2.6.2 Crisis management

In relation to CIP, crisis management refers to the processes in place for dealing with events that disrupt or threaten to disrupt the service delivery of CI. Crisis management systems typically require that the following steps be taken:

- Anticipating and planning appropriate responses to potential crises[43]
- Identifying an ongoing or imminent crisis
- Confronting the crisis to minimize its impact and ensure a return to normal service delivery as quickly as possible

Within crisis management frameworks, the notion of "response" is often employed to refer to action taken during and immediately after the commission of a terrorist act or threat to commit a terrorist act. Response actions typically aim at:

- Preventing or minimizing the consequences of the attack, such as loss of life, injury, damage to property and damage or disruption to infrastructure
- Undertaking criminal investigations
- Providing immediate relief and support to affected populations

In comparison with response, "recovery" commonly identifies action warranted in the longer term to support reconstruction efforts, including physical infrastructure and the restoration of the status quo in terms of communities' physical, social and economic well-being. The extended psychological impacts of terrorist acts beyond the specific site of the incident suggest that, in some cases, recovery may be understood as a process requiring integrated and sustained collaboration among government agencies, the private sector and civil society organizations.

[43] Countries often use the terms "contingency planning" and "emergency planning" interchangeably. Strictly speaking, however, emergency plans are reactive by nature while contingency plans are more proactive. While emergency plans are designed to limit the consequences or impact of an incident, contingency plans are designed to anticipate events and prepare all parties concerned for an emergency, as well as enabling a return.

2.6.3 Assessing the risk

In comparison with risk assessments conducted against other hazards, the identification and evaluation of the terrorist risks to CI raise specific issues. Some of these challenges stem from the higher uncertainty surrounding this type of scoping exercise. As has been observed, "a fundamental problem in this context is that terrorists adapt their behaviour to changes in the security landscape".[44] From this perspective, the terrorist threat should be regarded as a dynamic one, which adjusts for example to changes in the resources available to a terrorist group and to changes in the security features of a potential target.

CIP strategies should also recognize that terrorism-related risk assessments against CI are predicated on the ability to handle multiple sets of indicators and also to contextualize available information. Changes in geopolitical realities, economic situations, power dynamics between criminal organizations and other circumstances should all be accounted for and encourage the conduct of risk assessments at regular intervals of time.

Crucially, assessments can benefit from evidence of previous attacks or threats against CI, especially when these have taken place repeatedly over time or have consistently targeted certain sectors or CI in specific regions. Assessments can also draw on the data available from other countries, in particular when analogies can be inferred. By way of example, if a certain terrorist group has attacked critical facilities in country X and country Y and the group is also known to be active in country Z, this fact should be accounted for in security planning for similar facilities in country Z.

Efforts should also be made to detect "low intensity" signs of potential ongoing terrorist plans. Recorded acts of violations against CI, such as simple trespassing, might indicate terrorists' interest in how CI functions, or attempts to carry out close surveillance activities of certain places. At the same time, it is often impossible to make inferences on the basis of single and sporadic acts. Intelligence agencies have a key role to play in revealing patterns behind events that appear insignificant when considered in isolation.

While CIP strategies are not expected to contain full lists of threat indicators and sources, they should be constructed in such a way as to empower (or mandate, depending on the chosen CIP governance models) relevant authorities to shape risk assessment processes according to the fluid and volatile nature of the terrorist threat.

[44] Counter-Terrorism Committee Executive Directorate, "Physical protection of critical infrastructure against terrorist attacks", CTED Trends Report, 2017. Available at https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf.

Box 11
ICAO aviation security risk assessment methodology

The ICAO aviation security risk assessment methodology was designed to generate an understanding and a relative ranking of current residual risk in order to inform policymaking. While the methodology has been developed having in mind threats against civil aviation, most of its elements may be regarded as of general applicability. This risk assessment process comprises the following elements:

- Identification and analysis of plausible and specific threat scenarios and their likelihood
- Assessment of their consequences
- Assessment of existing mitigation measures and remaining vulnerabilities
- Obtainment of risk value based on the results of likelihood, consequences and vulnerabilities
- Assessments of a specific threat scenario
- Recommendations for further risk-based work and possible mitigation measures

The key components of the completion of the risk assessment are the following:

- *Threat scenario*: identification and description of a credible act of unlawful interference comprising a target (such as an airport terminal, associated infrastructure or an aircraft, or other CI), the modus operandi (including conveyance and concealment) and methods of an attack (such as an improvised explosive device), and the adversary (based on the role and adversary plays in the aviation system – passenger, non-travelling person, or insider). This should be sufficiently detailed to permit accurate assessment and analysis; "an attack against an aircraft" is not good enough as a scenario, whereas "a passenger attacking an airport terminal using an improvised explosive device (IED) in hold baggage" would suffice.
- *Likelihood of an attack (threat*): the probability or likelihood of that attack (threat scenario) being attempted, based on terrorist intentions and capabilities but not taking into account current security measures. The likelihood is used as an indicator of threat, considering both the intent and capability of a perpetrator to carry out a threat scenario.
- *Consequences*: the nature and scale of the consequences of the specific attack, in human, economic, political and reputational terms under a reasonable worst-case scenario.
- *Current mitigation measures*: the relevant standard and recommendation practices (which may not all be in ICAO Annex 17 and which, as generally assumed, are being effectively applied; where that is clearly not the case, the risk will be higher) or other relevant national or local programmes and regulations, in reducing the likelihood of the attack being successful or reducing the consequences if the attack were to occur. It is assumed that no threat can be entirely eliminated.
- *Vulnerability*: the extent of the remaining vulnerabilities once the current mitigating measures have been taken into account.
- Risk: the overall risk of a successful attack which remains, assuming current mitigating measures have been implemented, taking account of threat likelihood and consequences.
- *Possible additional mitigation measures*: identified measures that could be implemented to further mitigate residual risks where necessary.

It is important that the risk assessment identifies all plausible scenarios carefully and in sufficient detail, and is specific and thorough in considering each form of threat. Threats could be directed at specific airports, terminals or other infrastructure, such as fuel farms, air traffic control facilities or navigational equipment, and also at aircraft, including different forms of aviation, such as general aviation, passenger aircraft, and cargo-only aircraft. The means and methods by which a threat could be carried out should also be evaluated. This would include how a weapon or explosive device could be constructed, the means by which it might be conveyed (for example, whether carried on the person or vehicle-borne) and by whom (whether a staff member, passenger or member of the public), how it could be concealed, and how it could be activated or utilized in order to perpetrate an act of unlawful interference.

Source: ICAO representative.

In articulating their CIP strategies around a risk management approach, countries should operationalize the two overarching guiding principles outlined below.

2.6.3.1 Multi-level exercise

The determination of the nature and levels of threats to CI and related vulnerabilities is necessarily the joint and harmonized outcome of assessments carried out by multiple stakeholders at different levels of government (federal, when applicable, national and local). A CIP strategy should set the framework to integrate the threat landscape observed at the national level, the critical-sector level and the level of the CI operator.

Where national-level assessments are concerned, their objective is to reach an understanding of the threat faced by a country's CI, its consequences and related vulnerabilities. An important added value of nation-wide assessments is that they highlight how different critical sectors interact with one another. The intelligence-based processes and findings that support the elaboration of national security and counter-terrorism assessments are essential also for the determination of the threat landscape affecting CI.

In addition to national-level risk assessments, it is critical to develop risk profiles for specific CI sectors. These profiles need to include an evaluation of existing mitigation measures. Depending on the sector under consideration, risk assessments may be undertaken for specific subsectors and subsequently be fed back into broader sector risk profiles.[45]

At the infrastructure level, CI operators are often those that know best how the specific assets and processes under their control operate. Consequently, they have specific insight into their intrinsic vulnerabilities. In addition, companies often run risk management cycles independently of the institutional role that they are called to play in CIP. Corporations primarily engage in risk management to minimize damage that may affect company objectives, with a view to guaranteeing business continuity or to limiting the consequences of a threat. While not focusing on CIP, this type of risk management aims to identify risk to the continuity of production and establish mitigating measures. As a result, it may be of direct benefit to companies' infrastructure and increase resilience levels. Member States should thus carefully consider the role that company-run risk management processes should play in the context of CIP strategies, including how to integrate corporate-level assessments into CIP decision-making processes.

2.6.3.2 Multi-stakeholder process

An effective risk assessment exercise is the outcome of a consultation process which draws on the perspectives and findings of a variety of government agencies, emergency services and private-sector entities. While, under normal conditions, government agencies take the lead in elaborating national and sector-specific threat assessments and CI operators take the lead for CI-specific plans, the input of all stakeholders is always desirable. Although the involvement of a wide spectrum of stakeholders may slow-down the entire process, countries' experiences show that the values of inclusiveness and transparent decision-making is instrumental in achieving acceptance. This is a key prerequisite considering that multiple stakeholders have responsibilities for implementing CIP strategies.

The inclusiveness of the process also makes it possible to consider risks from multiple angles. Joint understanding is gained on the interplay between different types of infrastructure and critical sectors. Ensuring the broad participatory nature of the process and its overall coherence, however, comes with challenges. A general challenge is that different stakeholders perceive risks in different manners. As observed in the 2013 National Infrastructure Protection Plan of the United States Department of Homeland Security, "critical infrastructure partners manage risks based on diverse commitments to community, focus on customer welfare, and corporate governance structures. Risk tolerances will vary from organization to organization, as well as sector to sector, depending on business plans, resources, operating structure, and regulatory environments. They also differ between the private sector and the government based on underlying constraints. Different entities are likely to have different priorities with respect to security investment as well as potentially differing judgments as to what the appropriate point of risk tolerance may be".[46]

---

[45] For example, the Australian Critical Infrastructure Resilience Strategy breaks the transport sector down into the following subsectors: aviation, land-based mass passenger transport (including bridges and tunnels), land freight and maritime (shipping and ports). Under the same Strategy, the energy sector is composed of electricity systems, offshore oil and gas, onshore oil and gas and coal supply. Further details available at https://www.cisc.gov.au/help-and-support-subsite/Files/critical_infrastructure_resilience_strategy_plan.pdf.

[46] United States Department of Homeland Security, "NIPP 2013: partnering for critical Infrastructure security and resilience", 2013, p. 15. Available at https://www.cisa.gov/resources-tools/resources/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

Not only is it important to recognize the existence of different stakeholder mindsets and approaches, but also to understand how these may impact the overall process of setting joint priorities. From this perspective, achieving "critical infrastructure security and resilience depend on applying risk management practices of both industry and government, coupled with available resources and incentives, to guide and sustain efforts".[47]

CASE STUDY 12
Regional Resilience Assessment Program: Canada

The Canadian Regional Resilience Assessment Program is a comprehensive risk assessment programme for owners and operators of Canadian CI. It features site assessments to help organizations measure and improve their resilience to all hazards in Canada, including cyberthreats and intentional man-made events. The site assessments are voluntary, non-regulatory, free of charge and confidential. They also identify optional cost-effective measures to help owners and operators to mitigate risks and improve their ability to respond to and recover from disruptions.

To enhance critical infrastructure resilience, the Regional Resilience Assessment Program uses the following four tools:

- Critical infrastructure resilience tool (one day to complete)

  An on-site, survey-based tool that measures the resilience and protective measures of a facility. Outputs include a report and interactive dashboards that provide scores and peer comparisons and highlight dependencies and resilience enhancement options for physical security, resilience, and cybersecurity.
- Critical infrastructure multimedia tool (half a day to one day to complete)

  A virtual rendering of a facility based on floor plans. It features panoramic photographs of interior and exterior significant areas and can be shared with first responders and used in exercises.

  Although doing so is at their discretion, organizations are strongly encouraged to share the critical infrastructure multimedia tool with first responders so that it can be used as a tool to prepare for, and respond to, emergency situations.
- Canadian cyber resilience review (one day to one and a half days to complete)

  An on-site, survey-based tool that measures the cybersecurity posture of an organization.

  Outputs include two reports (brief and comprehensive) with scores across the 10 domains of the cybersecurity framework of the National Institute of Standards and Technology, peer comparisons, and resilience enhancement options.
- Network security resilience analysis tool (one day to complete)

  An on-site, technical analysis tool that provides device configuration remediation, and benchmarks cybersecurity networks against standards compliance.

  Outputs include reports (brief and comprehensive) with network visualization, identification of critical attack risk pathways along with network device non-compliance identification and resilience enhancement options.

Both the critical infrastructure resilience tool and the cyber resilience review require the presence of individuals who are subject matter experts on facility security, IT and facility management. Organizations can request each of the tools individually or all the tools as a package. Use of all three tools typically takes three days. Post-assessment check-ups may be conducted with the organization up to 24 months after the assessment. Organizations may also signal interest in participating in a broader regional assessment. These projects typically involve work across multiple organizations in a particular region. When examining a specific hazard, the objective is to help in identifying key interdependencies, and also opportunities to individually and collectively minimize the impact and likelihood of a disruption. During a regional assessment, the individual assessment tools are deployed alongside modelling tools, workshops, stakeholder meetings and subject matter expert interviews.

Source: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.

[47] Ibid., p. 15.

CASE STUDY 13
National and subnational risk assessments: Finland

National risk assessments

The drafting of national risk assessments by the Finnish Ministry of the Interior started in 2015 and is based on decision No. 1313/2013/EU of the European Parliament and of the Council on a "Union Civil Protection Mechanism".[48]

The national risk assessments are an amalgamation of risk assessments conducted by different branches of the national administration. These choose threat scenarios and disruptions that are seen as impairing the vital functions of society at the national level. The competent ministries are responsible for elaborating their own threat scenarios and disruptions by forming writing groups which also take advantage of the expert opinions in the ministries' respective branches of administration. The writing groups' efforts are combined and edited in their final form by the National Risk Assessment Working Group. European Union guidelines are used in drafting the national risk assessment. National risk assessments from other countries are also taken into account in the planning phase.

Threat scenarios taken into account by the latest national assessment, which was conducted in 2019, include:

- Terrorist acts targeting the structures of society or large crowds
- Disruptions of the public economy
- Disruptions of the financial system
- Major disruptions to the power supply
- Severe disruptions to the availability of fuels
- Severe disruptions to communications networks and services
- Water supply disruptions
- Disruptions to food supply
- Maritime multisector accidents
- Severe nuclear power accident in Finland or in the country's neighbouring areas

Subnational risk assessments

Subnational risk assessments are conducted as a separate project simultaneously with the national assessment. They are drafted in a cross-sectoral approach, so that the region's municipalities, authorities, businesses and organizations are represented in the working groups. The representatives make extensive use of the expertise and insights of their own communities and reference groups.

The aim of the subnational assessments is not to identify and list all possible threat scenarios affecting the region, but rather to choose those that are most significant. Outcomes are compiled into a written report distributed to the operators in the region for use and, if necessary, to other stakeholders. Both the national and subnational risk assessments are expected to be used, among others, by each CI operator's risk assessment as a shared basis for preparedness.

Source : https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161351/9_2019_National%20risk%20assessment.pdf

[48] In accordance with article 6 of the decision, member States are required to develop risk assessments at the national or appropriate subnational level and submit a summary of the relevant elements to the Commission every three years.

CASE STUDY 14
National risk assessment: Sweden

The Swedish Civil Contingencies Agency is responsible for issues related to civil protection, public safety, emergency management and civil defence, as long as no other authority has responsibility before, during and after an emergency or crisis. The Agency works via knowledge enhancement, support, training, exercises, regulation, supervision and its own operations in close cooperation with municipalities, county councils, other public authorities and the private sector.[49]

According to domestic law, all government entities are required to elaborate and submit a risk and vulnerability analysis to the Civil Contingencies Agency. Based on such reports, the Agency has been producing national risk assessments since 2011. These documents aim to provide strategic groundwork for the direction and further development of civil contingencies.

Based on the national risk assessment for 2021, the Agency has compiled a document on strengthening civil preparedness, which highlights several social challenges, along with the most significant threats and risks that Sweden faces. Among the identified areas where enhanced capabilities need to be developed, the document emphasizes the importance of improving critical infrastructure and supply security. It highlights, in particular, the need to identify critical infrastructure and for the competent stakeholders to analyse existing risks and have a back-up plan should those risks become reality. At the same time, the Agency notes that requirements are yet to be determined regarding which particular activities should be maintained within the identified critical infrastructure. It also notes that regulated obligations regarding risk and business continuity management are not comprehensive enough.

A connected area where the Agency sees a need for priority action by government agencies is in the field of cybersecurity and protective security.

Source: https://rib.msb.se/filer/pdf/29824.pdf.

CASE STUDY 15
Intelligence-led approach to the protection of CI against terrorist attacks: Australia

Australia relies on a strong intelligence-led, prevention and preparedness regime to support counter-terrorism arrangements. This approach encompasses targeted prevention and preparedness measures based on risk management principles and maintaining capabilities to manage various types of terrorist threats, attacks and their consequences. Counter-terrorism intelligence and criminal investigations are carried out by the Australian Security Intelligence Organisation (ASIO) and law enforcement agencies. Communicating CI terrorist threat information to owners and operators of CI quickly and appropriately enables those owners and operators to make better-informed risk management decisions and undertake effective risk mitigation measures, in response to the threat environment.

ASIO threat assessments indicate levels of threat against, and the probable nature of, terrorism, politically motivated violence, espionage, foreign interference, violent protest and sabotage. Threat assessments can be produced for specific events, facilities, people or sectors and are separate from the national terrorism threat level. ASIO distributes threat assessments to relevant Australian government agencies, state and territory governments, the Australian Federal Police, and state and territory police. CI owners and operators are also provided with a copy of the national terrorism threat assessment and are expected to use it in their preparation and planning processes. ASIO provides threat advice to the private sector and to government agencies via the Business Liaison Unit. Where there is particular urgency, ASIO contacts state and territory police and other relevant organizations, including owners and operators of CI, as soon as possible and in advance of the dispatch of the written advice. While ASIO threat assessments consider the intent and capability of terrorists, they do not assess the vulnerability or adequacy of existing security of CI. Subsequently, threat assessments should be used in security risk analysis to determine the requirement and type of mitigation measures for any given CI facility.

Source: https://www.police.vic.gov.au/sites/default/files/2019-03/NationalGuidelinesForProtectingCriticalInfrastructureFromTerrorismNovember2015.pdf.

[49] The Government of Sweden steers the Civil Contingencies Agency by means of a body of instructions and an annual appropriation. The instructions specify the Agency's responsibilities and tasks. The appropriation specifies its objectives and reporting requirements, and also the resources allocated for its administration and activities.

Tool 7
National Capabilities Assessment Framework – ENISA

https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

The National Capabilities Assessment Framework is the outcome of work conducted by the European Union Agency for Cybersecurity (ENISA). It is aimed at providing countries with a self-assessment of their level of maturity in terms of their cybersecurity capabilities both at the strategic and operational level. The Framework was designed with the support of ENISA subject matter experts and representatives from 19 European Union member States and EFTA countries. The target audience includes policymakers, experts and government officials responsible for or involved in designing, implementing and evaluating national cybersecurity strategies and, on a broader level, cybersecurity capabilities.

The Framework is based on five maturity levels defining the stages that countries go through when building cybersecurity capabilities. The levels represent increasing maturity stages, starting from level 1 (absence of a clearly defined approach to cybersecurity capacity-building) and ending with level 5 (the cybersecurity capacity-building strategy is dynamic and adaptive to environmental developments).

In addition, the Framework is characterized by four clusters: first, cybersecurity governance and standards; second, capacity-building and awareness; third, legal and regulatory; and fourth, cooperation. Each of those clusters covers a key thematic area for building cybersecurity capacity in a country and contains a pool of different objectives that countries might include in their strategies.

Tool 8
Global Overview of Assessment Tools

https://cybilportal.org/publications/global-overview-of-assessment-tools-goat/

Developed by Working Group A (Task Force Strategy and Assessments) of the Global Forum on Cyber Expertise, the Global Overview of Assessment Tools is premised on the need to create awareness on the different existing cybercapacity assessment tools and to provide details on their methodologies, outputs and impact. The Overview's objective is to support the policymaking process in identifying suitable tools and approaches geared to the prevailing needs and knowledge gaps, and also to provide guidance on what to do and whom to contact if a country wishes to be assessed.

Specifically selected tools for assessing a country's cybercapacity include the following:

- Combating Cybercrime: capacity-building tool of the World Bank
- Cyber Maturity in the Asia-Pacific Region: Australian Strategic Policy Institute
- Cyber Readiness Index 2.0: Potomac Institute for Policy Studies
- Cybersecurity Capacity Maturity Model for Nations: Global Cyber Security Capacity Centre
- Cyber Strategy Development and Implementation Framework: MITRE Corporation
- Global Cybersecurity Index: International Telecommunication Union (ITU)
- National Capabilities Assessment Framework: ENISA
- National Cyber Security Index: e-Governance Academy

2.6.4 Mitigating the risk

The previous section has highlighted the importance of carrying out comprehensive and integrated risk assessments at different levels of government and by multiple stakeholders. Risk management should eventually translate into specific mitigation measures aimed at minimizing the risk of a disruptive event impacting CI. Accordingly, this section examines the role of three specific types of mitigation measures in the context of CIP efforts. Notably, CIP strategies and related implementing actions should be predicated on the idea that effective protection measures at the CI level require the integration of physical, personnel-related and cybersecurity elements.

At the same time, mitigating the risk of terrorist attacks on CI should be part of a broad, multidisciplinary and nationwide task of anticipating and disrupting plans, conspiracies and other preparations to commit terrorist acts in general. CI protection ultimately depends on the coordinated activities of intelligence services and the law enforcement community

at large, among other factors. The extent to which criminal laws take a preventive approach, combined with the ability of investigative agencies to be proactive (as opposed to simply react to the commission of terrorist acts), plays a fundamental role in risk mitigation efforts.

The effect pf mitigation measures can typically be maximized through the implementation of the so called "defence-in-depth" concept, whereby a series of successive defensive measures are layered in order to protect a critical asset or process. If one set of measure fails, the offender immediately encounters another set of measures. The underlying principle is that infrastructure security is not significantly impaired by the loss of any single layer.

Lastly, in determining the most appropriate mitigation measures to apply to CI, Member States must evaluate the extent of their potential impact on the exercise of human rights (for example, impact on the freedom of movement created by site security restrictions, interferences in individuals' privacy caused by video surveillance technologies, and other effects). The goal of protecting CI against terrorist attacks should be balanced with the need to respect fundamental human rights as enshrined in international treaties such as the International Covenant on Civil and Political Rights. In particular, only measures that are deemed strictly necessary to achieve CIP should be implemented. Planned measures should also be evaluated and, if implemented, reassessed in terms of their proportionality to the sought objectives.

2.6.4.1 Physical protection measures

Within the framework of a multi-layered, defence-in-depth approach, a number of measures can be taken to enhance the physical protection of CI. Some of these measures include:

- Delineation of CI area perimeters and protection by physical barriers.
- Patrols and surveillance, by law enforcement and CI operators, with a view to quickly identifying suspicious activity occurring around a critical site (such as site reconnaissance) and reporting it to the competent authorities.
- Access control with security features used to increase its performance or effectiveness (such as barbed wire topping, a perimeter intrusion detection system, lighting or a closed-circuit television system).
- Use of technology such as screening and other security controls (such as conventional or high definition X-ray equipment, explosive detection dogs, manual searches, hand-held metal detectors, and explosives trace detection).

Physical security measures should be supported by properly vetted and trained personnel, sound and comprehensive contingency planning and security plans designed at the CI operator's level. Moreover, Member States are increasingly implementing so-called "security-by-design" approaches as a tool to achieve physical security goals at the stage of designing and constructing (or renovating) buildings that host CI.

CASE STUDY 16
Protective Security Act 2019: Sweden

The 2019 Protective Security Act applies to both public and private organizations engaged in security-sensitive activities that are important to the national security and infrastructure of Sweden. It covers a broad range of companies working in IT, law enforcement, transport, and other sectors. Before hiring new staff, any company handling "security-sensitive information," as defined in the Act, needs to conduct a protective security analysis, implement security protection measures and carry out a personnel security assessment .

The Swedish Protective Security Act covers any organization conducting security-sensitive activities. These are defined as activities that are:

- Critical to the national infrastructure of Sweden, or
- Important for the security of Sweden, or
- Covered by an international protective security commitment that is binding on Sweden

Organizations operating in the following sectors are deemed to be carrying out security-sensitive activities:

- Defence
- Law enforcement
- Energy supply
- Water supply
- Telecommunications
- Transport

Any company engaged in security-sensitive activities is covered by the Protective Security Act, regardless of whether it operates in one of the sectors listed above.

To comply with the Act, businesses must:

- Conduct a protective security analysis
- Implement security protection measures based on this analysis, covering both:
    - Information security, and
    - Physical security
- Before hiring any person, conduct a personnel security assessment of any staff member who will:
    - Have access to classified information, or
    - Be engaged in security-sensitive activities, or
    - Participate in operations requiring protection against terrorist acts
- Protect information about national security from exposure
- Restrict access to operations that:
    - Require protection against terrorist acts, or
    - Are critical to national security
- Enter into protective security agreements whenever a third party may gain access to confidential, secret, or classified activities (public authorities only)
- Appoint a protective security manager (effectively a chief information security officer, that oversees information security throughout the organization)

As the government agency responsible for national security and counter-terrorism in the country, the Swedish Security Service ("Säkerhetspolisen") is entrusted with enforcing the Protective Security Act and other security regulations within public agencies and companies. In particular, the Swedish Security Service can:

- Decide whether it is necessary to carry out a protective security inspection
- Carry out protective security inspections
- Issue recommendations for improving protective security
- Provide advice and support to organizations engaged in security-sensitive activities
- Conduct a security screening before a person is permitted to engage in security-sensitive activities or have access to classified information

Companies covered by the Protective Security Act can contact the Swedish Security Service for advice on compliance with the law.

Source: https://www.termsfeed.com/blog/swedish-protective-security-act/.

CASE STUDY 17
Security by design for critical information infrastructure: Singapore

The "security-by-design" concept can be applied not only to physical assets, but also to CII. The 2021 Cybersecurity Strategy of Singapore specifically sets the objective of pre-empting cyber vulnerabilities by promoting "security-by-design" practices. These are defined as "an approach to software and hardware development that seeks to minimize system vulnerabilities and reduce the attack surface, by designing and building in security at every development phase".

Under the Strategy, the Government undertakes to "strengthen engagement with … professional bodies such as those for engineers and software developers, to encourage them to build secure-by design products and services.

Source: https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021.

Tool 9
Guidance tools on physical security from Germany, Singapore, the United Kingdom and the United States

Country	Tool
Germany	**Protection of critical infrastructure – baseline protection concept, recommendation for companies** www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/Basisschutzkonzept_kritische_Infrastrukturen_en.html This tool has been elaborated by the Federal Ministry of the Interior and Community, the Federal Office for Civil Protection and Disaster Response and the Federal Criminal Police Office. The business community has provided its expertise from the outset. The baseline protection concept provides companies in Germany with recommendations from the point of view of internal security. It features a questionnaire and a checklist. **Competence Centre for the physical security (of government buildings)** https://bundesbau-bw.de/fileadmin/BBBW/Ueber_uns/2021-10_FLY_MaterielleSicherheit_8-Seiter_DE_ES_screen.pdf Based on a directive from the new coalition agreement of 2022, the Federal Ministry of the Interior and Community has set up a Competence Centre for the physical security of civilian government buildings. The Centre is responsible for elaborating basic concepts and guidelines on physical security (including against terroristic threats) and technical advice during the planning and implementation phase of projects for constructing government buildings.
United Kingdom	**Centre for the Protection of National Infrastructure (CPNI)** www.cpni.gov.uk/advice CPNI offers advice, toolkits and guides dealing with the following topics and sub-topics: • Personnel and people security (reducing insider risk; optimizing security of people; disrupting hostile reconnaissance) • Physical security (threat-specific mitigation search and screening; physical defences; access control and locks; intruder detection and monitoring; active access delay; building structures; windows and facades; doors; building services and spaces; control rooms; sensitive information and assets)
Singapore	**Guidelines for enhancing building security in Singapore** www.bca.gov.sg/Publications/BuildingSecurity/building_security_booklet.html The Guidelines provide a menu of good security practices and considerations to help building owners incorporate pragmatic security procedures, physical protection concepts and security technology into their building's security plans. As the Guidelines are intended to be used for all types of premises, and given that the risks associated with these premises vary considerably, the intention is not to provide recommendations, but rather information worth considering when planning for building security. The intent is also to ensure that security-related measures are not obtrusive and remain congruent with the overall design of the building, with integrated solutions that serve both functional and security purposes. The Guidelines are expected to serve as a common frame of reference and ensure a minimum level of acceptable security standards in the industry. **Video surveillance system standard for buildings** www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security Cameras at strategic locations throughout the building and its perimeter can help building owners to detect anomalies early, respond effectively to possible security threats and crime, and coordinate resources during business contingency. The video surveillance system also acts as a tool supporting post-incident investigations and providing evidence. The system does not, however, perform an active role in protective security and should not be designed to serve as the sole protective measure in a specified area, but should operate in conjunction with other security measures such as access control, intrusion detection alarm systems, fence intrusion detection systems, security responses and others. The video surveillance system standard for buildings is intended to support the adoption of video surveillance to enhance the overall management of a building's safety and security. It is based on a set of recommendations to guide building owners and to provide a consistent approach to the recommended specifications, installation and operation of video surveillance across buildings in Singapore. The standard may also be usefully employed by other countries as a source of guidance and inspiration. Given the dynamic nature of the video surveillance industry, this document focuses on good design and operational considerations, and may not spell out all specific technologies and capabilities within the video surveillance system. As there are many video surveillance options available on the market, building owners should consider engaging the services of a security consultant when designing a comprehensive video surveillance system.

Tool 9
Guidance tools on physical security from Germany, Singapore, the United Kingdom and the United States (con't)

United States	**Securing public gatherings (Cyber ISA)** cisa.gov/securing-public-gatherings CISA provides a number of capacity-building resources for CI owners and operators to enhance the security of public gatherings. The available resources cover numerous threat vectors, including unauthorized access to facilities, cybersecurity, election security, active shooters, bomb attacks, and small unmanned aircraft systems. **Employee vigilance through the "Power of Hello" (CISA)** cisa.gov/employee-vigilance-power-hello CISA has developed an infographic to help non-security professionals and CI employees identify and evaluate observable suspicious behaviour. The product suggests questions to consider when navigating a potential threat and includes information on when and how to obtain help. The tool is available in 17 languages. **De-escalation for CI owners and operators (CISA)** cisa.gov/de-escalation-series CISA elaborated four tools to assist CI owners and operators in recognizing the warning signs of someone on a pathway to violence; assess if the situation or person of concern is escalating, or if an emergency response is needed; and possibly de-escalate the situation through purposeful actions, verbal communication, and body language. The tools highlight the importance of reporting the situation through established protocols including local law enforcement for immediate threats. **Active shooter preparedness (CISA)** cisa.gov/active-shooter-preparedness The CISA Active Shooter Preparedness Program is specifically focused on supporting efforts by the public and private sectors to build security capacity against the active shooter threat, which is the most prominent attack vector in the United States. The Program consists of products, tools, videos, and translated resources that provide information on behavioural indicators, potential attack methods, emergency action plan creation, actions that may be taken to increase the probability of survival, and how to quickly recover from an incident. Resources include: • Video on options for consideration, translated into several languages • Emergency action plan guide, video, and template • Translated active shooter preparedness resources (cisa.gov/translated-active-shooter-resources)

2.6.4.2 Personnel security measures (insider threat)

It is unlikely for criminal and terrorist groups to succeed in their attempts to disrupt a CI facility without the collusion of the facility's employees providing access to sensitive data and information about weak points and processes, and other vulnerable areas. This highlights the need for protective strategies not only to secure the external perimeters of CI and to keep undesired visitors at bay, but also to leverage human resources management as a key tool to prevent the recruitment of elements associated with criminal and terrorist groups.

The notion of personnel security also refers to the policies and procedures needed to reduce the risk associated with insider threats (namely, those posed by current or former employee, third-party contractors, or business partners) exploiting their legitimate access to the premises, systems or processes of CI in order to carry out unauthorized acts. Effective personnel security involves a variety of measures ranging from background checks and selection procedures to security awareness training, the promotion of vigilance and a general culture of security.

Tool 10
Insider threat mitigation – CISA (United States)

cisa.gov/insider-threat-mitigation

CISA provides resources and training focused on assisting stakeholders in achieving a better understanding of the potential threats posed by insiders and methods to mitigating risk. The available tools are designed to help organizations to intervene before an individual with privileged access disrupts CI operations, whether unintentionally (owing to negligence) or through intentional acts.

Resources include:

- Insider Threat Mitigation Guide
- Self-assessment on the Insider Risk Mitigation Program
- Video entitled "Pathway to Violence" and associated fact sheet
- Fact sheet on preventing insider threats

2.6.4.3 Cybersecurity measures

Cybersecurity measures are designed to protect CI against cyberattacks. Not necessarily of a technological nature, they help to preserve the integrity, resilience and normal functioning of CI. They may, for example, include security procedures and policies, organizational measures, awareness and training, specific development guidelines and regular security assessments.

CASE STUDY 18
National cybersecurity frameworks on CII protection: Japan, Portugal, Singapore and United States

Japan: Cybersecurity Policy for Critical Infrastructure Protection, 2017

The purpose of the Cybersecurity Policy of Japan is to maintain safe and continuous provision of CI services based on the concept of mission assurance, preventing serious impacts on national life and socioeconomic activities caused by any CI outages resulting from cyberattacks and ensuring prompt recovery from outages. The policy is based on a number of overarching principles, including:

- CI operators are expected to implement cybersecurity measures on their own responsibility, although collaborative efforts among stakeholders are considered indispensable. While CI operators should seek the continuous improvement of those measures as entities providing services and bearing social responsibilities, government entities should provide them with the necessary support.
- All stakeholders should understand the importance of asking the questions "when", "where", "who", "why", "what" and "how" when responding to CI outages, depending on the scale of the outages, and should be able calmly to consider the signs or occurrence of any outages. They should also be capable of cooperating with other stakeholders and respond in a cooperative and concerted manner, in addition to ensuring robust communication among various stakeholders and taking proactive measures.
- Senior management should develop incident readiness even in normal times and, in the event of an incident, properly disclose information on responses, with the aim of gaining trust and nurturing a sense of security among stakeholders. They should also constantly secure management resources such as budgets and the personnel necessary for the abovementioned measures and appropriately allocate them from a risk-based perspective.

Portugal: National Cyberspace Security Strategy (2019–2023)

The Strategy is based on three strategic objectives, which translate into six axes of intervention. Axis 3 ("Protection of cyberspace and infrastructure") outlines the following lines of action:

- Identify and consolidate knowledge of CII, following changes in the national and international legal framework for cyberspace security.
- Promote the continuous development of capacities and maturity of national entities in the prevention, detection, response and recovery in presence of adverse scenarios for cyberspace security that may affect their networks and information systems and the overall system that supports them, consolidating mutual trust, sharing of information and knowledge, and speedy and effective cooperation.
- Promote national and sectoral cooperation structures for the protection of cyberspace, including the public sector at central, regional and local levels, and also the private sector, including small and medium-sized enterprises, for the sharing of information and the promotion of mutual collaboration in the protection of common interests.
- Ensure the application of mechanisms and incentives conducive to the development of national and international reference frameworks for cyberspace security management and their adoption by national entities with responsibilities over critical infrastructure and essential services.
- Maximize the security and defence of the networks and information systems of the armed forces and national defence with a view to maintaining the ability to operate in cyberspace through cyberdefence.

Singapore: 2018 Cybersecurity Act

Adopted in 2018, the Act formalizes the country's policy in the field and firmly articulates the protection of CII in terms of cybersecurity concepts and protective measures. The Act pursues four objectives:

- To establish a normative framework formalizing the obligations of CII owners to ensuring the cybersecurity of their respective CII.
- To vest the Cyber Security Agency of Singapore with powers to manage and respond to cybersecurity threats and incidents.

- To set up a framework for the sharing of cybersecurity information with and by the Cyber Security Agency, and the protection of such information.
- To establish a light-touch licensing framework for cybersecurity service providers.

United States approach and initiatives to protect CII

The Cybersecurity and Infrastructure Security Agency (CISA) leads the federal Government's efforts to secure the country's CI, including CII. With a view to preventing, mitigating and respond to cyberthreats in this domain, CISA initiatives aim to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyberthreat information-sharing
- Incorporate strong privacy and civil liberties protections in every initiative to secure critical infrastructure
- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop a comprehensive research and development plan

CISA encourages the adoption of the National Institute of Standards and Technology Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity. Revised in 2018, the Framework sets out guidance around four key functions enhance cybersecurity risk management:

- Identify – develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.
- Protect – develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect – develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – develop and implement appropriate activities to take action in response to a detected cybersecurity incident.
- Recover – develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired as a result of a cybersecurity incident.

Sources : https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf; https://www.csa.gov.sg/legislation/cybersecurity-act; https://www.cisa.gov/resources-tools/resources/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and; and https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Information provided by the Permanent Mission of Portugal to the United Nations.

Tool 11
Tools on CII protection: National Cybersecurity Strategy Guide and Repository – ITU

To support its Member States in the development of national cybersecurity strategies for the protection of CII, the International Telecommunication Union (ITU) has developed two major tools:

Guide to Developing a National Cybersecurity Strategy (NCS Guide), 2021

- https://ncsguide.org/the-guide/

The second edition of the Guide provides a flexible and user-friendly framework setting the context for a country's socioeconomic vision and current security posture. It assists policymakers in the development of a strategy that takes into consideration a country's specific situation, cultural and social values, and that encourages the pursuit of secure, resilient, ICT-enhanced and connected societies.

The Guide was developed through an iterative approach, which sought to reach agreement through consensus-building. It is based on existing resources and aims to facilitate its use by national stakeholders. Wherever possible, relevant sources and tools used to develop each set of recommendations are listed in the Reference section to encourage their broader use.

- National Cybersecurity Strategies Repository
  https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

The Repository is a collection of strategic national policies, action plans and other relevant elements related to cybersecurity. This list is populated and frequently updated with documents either acquired through research of primary and secondary sources, or provided directly by governments.

Tool 12

Tools and approaches to aviation cybersecurity–ICAO www.icao.int/cybersecurity/Pages/default.aspx

Over the years, the civil aviation sector has gone through a digital transformation aimed at leveraging the power of technology to enhance the sector's safety, security, efficiency and capacity. The civil aviation sector is characterized by its interconnectivity, complexity, high level of media exposure, and the critical role that it plays in countries' socioeconomic development. As such, civil aviation is an attractive target for perpetrators in both the physical world and the cyber domain.

The civil aviation sector is global by nature, and so is the interaction of systems and data flows that transcend national borders. Accordingly, ICAO addresses cyberthreats against civil aviation infrastructure by promoting and leveraging a collaborative attitude on the part of all concerned stakeholders.

ICAO Aviation Cybersecurity Strategy

Recognizing the multifaceted and multidisciplinary nature of cybersecurity, and noting that cyberattacks can simultaneously affect a wide range of areas and spread rapidly, the Aviation Cybersecurity Strategy underpins the ICAO vision for the civil aviation sector to remain resilient to cyberattacks, safe and trusted globally, while continuing to innovate and grow. The Strategy identifies areas where a harmonized and holistic approach must be ensured to cybersecurity and cyber resilience in civil aviation: international cooperation; governance; effective legislation and regulations; cybersecurity policy; information-sharing; incident management and emergency response; and capacity building, training, and cybersecurity culture.

www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

Cybersecurity Action Plan

The Action Plan is a guidance document that supports States and stakeholders in the implementation of the Aviation Cybersecurity Strategy. It develops the Strategy's seven pillars into 32 priority areas, which are further developed into 51 tasks for implementation.

Guidance material

In 2020, ICAO began developing aviation cybersecurity guidance material to support the development of a cross-cutting, harmonized approach to aviation cybersecurity across civil aviation disciplines. Guidance published to date includes a manual on the use of the Traffic Light Protocol to support cybersecurity information sharing, a guidance on cybersecurity policy, and guidance on developing and implementing a robust cybersecurity culture in civil aviation.

Capacity-building

ICAO also began developing an aviation cybersecurity training portfolio to further support its member States. Two courses have been finalized to date: the first, entitled "Foundations of Aviation Cybersecurity Leadership and Technical Management", is a deep awareness course that covers all aspects of aviation cybersecurity, and which was developed in partnership with Embry-Riddle Aeronautical University. The second, "Managing Security Risk in Air Traffic Management", combines cybersecurity and physical security elements in the air traffic management environment. It was developed in partnership with the European Organization for the Safety of Air Navigation (EUROCONTROL). Work continues on expanding the aviation cybersecurity training portfolio. ICAO is currently working on a third course which focuses on cybersecurity oversight in civil aviation, which is in development in partnership with the Civil Aviation Authority of the United Kingdom.

Cybersecurity Panel

In 2022, ICAO established a Cybersecurity Panel to advance work on aviation cybersecurity previously performed by an informal group. The Panel's tasks cover a wide spectrum of international civil aviation areas such as aviation safety, security, air navigation, and risk management as they pertain to cybersecurity. Its mandate covers the development of aviation cybersecurity standards, procedures and guidance for the international civil aviation sector, the review and assessment of the global aviation cyberthreat landscape, and the provision of expert consultation to ICAO panels and expert groups as they address aviation cybersecurity elements in their work.

Tool 13
City Preparedness for Cyber-Enabled Terrorism – Counter-Terrorism Preparedness Network

https://www.london.gov.uk/sites/default/files/ctpn_preparedness_for_cyber-enabled_terrorism_report_single_pages.pdf

Prepared by the Counter-Terrorism Preparedness Network (CTPN) in 2022, the report supports efforts to protect critical infrastructure from cyberattacks and, by extension, cyber-enabled terrorism. It focuses on preparedness for critical infrastructure, essential services and city operations, arguing that societies' dependence on, and the interdependence between, digital infrastructure offers potential avenues for cyber-enabled terrorism.

The report aims to engage authorities (specifically those acting at the city-level) by providing evidence of the need to continually enhance preparedness against a range of cyberthreats and work to ensure that the frequency and severity of cyber-enabled terrorism do not increase.

Tool 14
Cybersecurity and Physical Security Convergence Guide – Cybersecurity and Infrastructure Security Agency: United States

https://www.cisa.gov/cybersecurity-and-physical-security-convergence

The Guide has been developed as an information tool about convergence and the benefits of a holistic security strategy that aligns cybersecurity and physical security functions with organizational priorities and business objectives. It is premised on the notion that, when physical security and cybersecurity divisions operate in siloes, they lack a holistic view of security threats targeting their enterprise. As a result, successful attacks are more likely to occur and can lead to impacts such as compromise of sensitive or proprietary information, economic damage, disruption of critical functions or loss of life.

The document highlights the risks associated with siloed security functions and contains a description of convergence in the context of organizational security functions, benefits of convergence, a flexible framework for aligning security functions and several case studies.

Tool 15
Guidance and advice tools on cybersecurity from the National Cyber Security Centre: United Kingdom

https://www.ncsc.gov.uk/section/advice-guidance/all-topics

A vast range of guidance materials is available through the National Cyber Security Centre (NCSC) of the United Kingdom. The different tools are arranged by topic under 46 categories, which include:

- Access control
- Active cyber defence
- Asset management
- Authentication
- Certification
- Cloud
- Cryptography
- Cyber awareness
- Cyber strategy
- Exercising
- Incident management
- Passwords
- People-centred security
- Remote working
- Supply chain

Available resources can be filtered depending on the target audience, namely, cybersecurity professionals, large organizations, public sector, small and medium-sized organizations.

Tool 16
Guide to increased security in industrial information and control systems: Sweden

www.msb.se/RibData/Filer/pdf/27473.pdf

On the basis of internationally recognized guidance, practices and working methods, the Swedish Civil Contingency Agency has elaborated 17 recommendations to enhance security in industrial information and control systems. While some recommendations are technical in nature, others focus on methodological aspects, as outlined below:

1. Secure management's commitment and responsibility for security in industrial information and control systems.
2. Clarify roles and responsibilities for security in industrial information and control systems.
3. Maintain processes for system surveys and risk management in industrial information and control systems.
4. Ensure systematic change management in industrial information and control systems.
5. Ensure systematic contingency planning and incident management in industrial information and control systems.
6. Introduce security requirements in industrial information and control systems right from the start in all planning and procurement.
7. Create a good security culture and heighten awareness of the need for security in industrial information and control systems.
8. Work with a security architecture in the industrial information and control systems.
9. Continuously monitor connections and systems in order to detect intrusion attempts in industrial information and control systems.
10. Conduct regular risk analyses of industrial information and control systems.
11. Conduct periodic technical security audits of industrial information and control systems.
12. Continually evaluate the physical security of industrial information and control systems.
13. Regularly ensure that any and all connections to industrial information and control systems are secure and relevant.
14. Harden and upgrade industrial information and control systems in collaboration with system vendors.
15. Conduct training and practice regarding IT incidents in industrial information and control systems.
16. Follow up incidents in industrial information and control systems and monitor external security problems.
17. Participate in user associations, standardization bodies and other networks for security in industrial information and control systems.

The Guide provides explanations about each recommendation, subsidiary recommendations and examples of risks and problems that might be encountered.

Tool 17
Best practices for critical information infrastructure protection (CIIP) – Experiences from Latin America and the Caribbean and Selected Countries – Inter-American Development Bank

https://publications.iadb.org/publications/english/document/Best-Practices-for-Critical-Information-Infrastructure-Protection-(CIIP)-Experiences-from-Latin-America-and-the-Caribbean-and-Selected-Countries.pdf

The structure of this best-practices manual developed by the Inter-American Development Bank mirrors the typical structure for a CIIP framework, comprising the following pillars:

- Strategy and legislation
- Governance and regulation
- Definition and assignment
- Protection
- Information-sharing
- Crisis management

The featured case studies provide focused input into each of the above pillars and offer an overview of regionwide research on the CIP landscape in Latin American countries. The research carried out covers both the public and private sectors in 26 countries via desk research, electronic surveys and follow-up interviews. Electronic surveys were sent to over 900 private and public sector representatives.

Tool 18
Good practices in CIIP – Global Forum on Cyber Expertise-Meridian

https://thegfce.org/wp-content/uploads/2020/06/CriticalInformationInfrastructureProtectionCIIP.pdf

Run by the Meridian Community, a large group of officials from more than 60 countries, the Global Forum on Cyber Expertise-Meridian CIIP Initiative aims to support policymakers with responsibilities for CIIP to understand the implications and consequences of cybersecurity issues and to maintain awareness of current developments. By working together in a global initiative, the initiators leveraged their expertise for the benefit of a broader audience to help develop CIIP capabilities, in particular in developing countries. Under the initiative, two good practice manuals were developed in 2017:

- GFCE Global Good Practices – Critical Information Infrastructure Protection (CIIP)

Based on previous research, input from the Global Forum on Cyber Expertise-Meridian CIIP meeting in Mexico (2016), literature and experience elicited from interviews, this document provides policymakers with concise knowledge to help them define sustainable and efficient efforts to protect national CII.

- GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers

This good practices guide was developed to raise the protection barriers and to make progress on the CIIP path for the benefit of national CI and CII policymakers. The document is intended to assist countries which are either at the start of their CIP enhancement efforts or that have already developed some expertise in this domain.

As each country has a different legal and regulatory structure, style of governance over CI and CII, level of adaptation of its ICT and different institutional culture, the guide emphasizes the need for readers to apply any of the suggested practice in a way that meets individual country needs.

2.6.5 Planning for and handling crises affecting CI

CIP strategies need to consider which type of crisis management structures and processes need to be in place. Member States may determine, for example, that a single government entity be assigned primary responsibility and authority to determine the course of action to be taken when a crisis occurs. This entity will then coordinate interventions by the various emergency responders, ensuring the interoperability of communication systems and adequate response times, along with evacuation plans to limit the impact of an ongoing crisis. Emergency team response should be planned, tested and evaluated in advance to mitigate the effects of an attack.

The identification of the most appropriate crisis management framework also requires a determination as to whether or not emergency management will follow an all-hazard or hazard-specific approach. Both approaches have advantages and disadvantages. When crisis management structures are set up for specific types of threats, tailor-made processes can be put in place. Choosing a hazard-specific approach may, however, turn out to be problematic when the nature of the incident is not clear, as it may cause uncertainty as to the applicable framework for intervention.

Normative frameworks for crisis management in the CI domain can follow a sector-specific or cross-sectoral approach. If the first approach is chosen, the legal framework is often adopted by the ministry responsible for the sector in question or by the sector's regulator. By contrast, the cross-sectoral approach often sees the adoption of one or more legislative acts.[50] Whichever crisis management structure is chosen, clear human-rights-compatible legal and operational frameworks must be established, in the awareness that crisis management is important in the event not only of particularly disruptive terrorist attacks, but also of minor incidents, to avoid or reduce the impact or escalation of the crisis.

[50] In the event of an attack on a chemical, biological, radiological or nuclear facility, a specialized response is required to protect the public and first responders from contamination and mitigate the potential release of dangerous materials. A specialized response would entail specific emergency and contingency planning, in addition to specialized equipment for detection, personal protection and decontamination.

Once the basic crisis management structures and processes have been identified, CIP strategies need to ensure that these work smoothly in case of need. The basic prerequisites for achieving fluid and rapid decision-making are examined in chapter 5. The same chapter also discusses joint public-private exercises as key tools in crisis management.

Box 12
European Union Law Enforcement Emergency Response Protocol (2019)

Adopted by the European Union Council within the European Union "Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises", the 2019 Protocol assists European Union law enforcement authorities in providing immediate responses to major cross-border cyberattacks through rapid assessment, the secure and timely sharing of critical information and coordination of the international aspects of their investigations.

The impetus for the elaboration of the Protocol partly stems from the 2017 so-called "WannaCry" and "NotPetya" cyberattacks, which were unprecedented in scale and highlighted the extent to which incident-driven and reactive approaches were inadequate responses to the rapidly evolving cybercriminal modus operandi.

In complementing existing European Union crisis management mechanisms, the Protocol makes full use of the resources of Europol, including by assigning a central role to its European Cybercrime Centre (known as "EC3"). As its scope of application is limited to cybersecurity events of a malevolent and suspected criminal nature – with the exclusion of crises generated by natural disasters, human error or system failure – the Protocol envisages a fundamental task for first responders in terms of the preservation of electronic evidence found within affected IT systems with a view to sustaining any subsequent criminal investigation or judicial proceeding.

Source: www.europol.europa.eu/media-press/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks.

CASE STUDY 19
Sector-specific and cross-sectoral crisis management frameworks: country examples

CI sector-specific normative frameworks are often found in the telecommunications sector. In the Netherlands, for example, the National Continuity Forum Telecommunications (NCO-T) aims to ensure that an operator is able to run critical telecommunications services during exceptional circumstances. The membership of NCO-T comprises the designated operators and the Directorate-General for Energy, Telecommunications and Markets of the Ministry of Economic Affairs.

In France, the Piranet plan defines the crisis management structure and processes for the State to take the necessary measures in the specific event of a major ICT crisis. The Piranet plan is complementary to the Vigipirate plan. It is elaborated by the National Agency for the Security of Information Systems (ANSSI) and the General Secretariat for Defence and National Security (SGDSN) and may be triggered by the Prime Minister.

Other CI sectors may establish equivalent arrangements based on legal frameworks adopted by sector-specific regulators. As noted by the Mackenzie Institute, for example, following the attacks of 11 September 2001, "the New York Stock Exchange – a perennial potential target of terrorist attacks – was able to continue with its trading operations as it had already established an alternative trading floor outside New York City, as have other financial institutions since then to replicate their business operations outside their municipal areas in case of terrorism-caused catastrophes".[51]

By contrast, an example of cross-sectoral normative frameworks is the Crisis Act of Estonia, chapter IV of which deals with the organization of continuous operation of vital services. The Act sets forth roles and responsibilities of ministries, local and national crisis management agencies and also CI operators necessary to guarantee the continued delivery of 41 critical services.

The European Commission maintains a website with detailed overviews of the national disaster management systems in force in 24 European countries.

Sources: https://itlaw.fandom.com/wiki/National_Continuity_Forum_Telecommunications; www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/; www.riigiteataja.ee/en/eli/525062014011/consolide; and https://ec.europa.eu/echo/what/civil-protection/national-disaster-management-system_en

[51] Joshua Sinai, "New trends in terrorism's targeting of the business sector", Mackenzie Institute, 2016. Available at https://mackenzieinstitute.com/2016/05/new-trends-in-terrorisms-targeting-of-the-business-sector/.

CASE STUDY 20
Crisis management governance structure: New Zealand

In New Zealand, the basic document setting forth an all-hazards, all-inclusive governance structure for managing potential, developing or actual crises (including, but not limited to, those affecting CI) is the National Security System Handbook. The criteria for the national security system to be triggered fall into two broad categories. These relate either to the characteristics of the risks, or to the way in which the risks need to be managed.

Risk characteristics

- Unusual features of scale, nature, intensity, or possible consequences
- Challenges for sovereignty, or nationwide law and order
- Multiple or interrelated problems which, when taken together, constitute a national or system-wide risk
- High degree of uncertainty or complexity such that only the central Government has the capability to tackle them
- Interdependent issues with the potential for cascade effects or escalation

Management requirements

- Response requirements are unusually demanding of resources.
- There is ambiguity regarding who has the lead in managing a risk, or there are conflicting views about solutions.
- The initial response is inappropriate or insufficient from a national perspective.
- There are cross-agency implications.
- There is an opportunity for the Government to contribute to conditions that will enhance overall national security.

For any national security risk (or major element of such a risk), a lead agency is identified. These agencies are mandated (either explicitly through legislation or because of their specific expertise) to manage an emergency arising from a list of specific hazards.

Crisis management in New Zealand leverages the functions of several different bodies, including:

- *Watch groups*: These are called upon to obtain situational clarity in what is often a chaotic environment and are responsible for ensuring that systems are in place to ensure effective management of complex issues. Watch groups are ordinarily made up of senior officials able to commit resources and agree on actions on behalf of their organization. The exact composition of the watch groups depends on the nature of the event and includes agencies with a role to play in responding to the issue at hand. This might include agencies which do not usually think of themselves as "national security" agencies and do not have a great deal of experience in operating within the national security system structures.
- *Officials Committee for Domestic and External Security Coordination*: This body, known as ODESC, provides strategic direction, supports the lead agency and has links with the political level, including advising the Cabinet National Security Committee.
- *Working or specialist groups*: These are created when it is desirable for a profession or discipline to determine and present a consolidated view, or specific advice, to a watch group or ODESC. Examples include the Government Legal Network, the Economic Advisory Group, the Science Network and the Intelligence Community.
- *National Crisis Management Centre*: This provides a secure, centralized facility for various coordinating tasks, such as directing response operations, planning and support; information gathering, management and sharing; and liaison between the operational response and the national strategic response.
- *Red teaming*: Red teaming involves subjecting a plan, ideas or assumptions to rigorous analysis and challenges in order to improve the validity and quality of the final plan. Multi-agency red teams can be established throughout all stages of a crisis – and indeed, a project – and can operate in parallel to the response. Within a national crisis, red teaming helps to provide a fresh perspective on the approach being used to manage the threat.

As part of a wider programme to update the national emergency management system, New Zealand is in the process of discussing possible changes to further ensure infrastructure resilience. The discussion revolves around a number of topics, including:

- *Identification of minimum levels of service*: The requirements for identifying minimum levels of service for critical infrastructure in the event of an emergency should be clarified and strengthened. This includes requirements for infrastructure providers to disclose information about preparedness and level of service expectations. Proactive disclosure of this information will support transparency and help the Government, individuals and organizations to understand the risks that they face, to prepare and to make choices about how best to manage those risks.

CASE STUDY 20
(continued)

- *Coordinated approach to managing risk*: A sustained increase in resourcing is needed to ensure a coordinated approach to managing risk across the country's critical infrastructure. Lead sector agencies need clearer roles for the coordination of resilience activities within and across critical infrastructure sectors. This reflects the interdependencies across infrastructure networks. These changes are required to clarify expectations of how resilient the critical infrastructure needs to be and the roles and resourcing of different parties involved in delivering that infrastructure.

Sources: https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security/new-zealands-national-security; https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf; and www.tewaihanga.govt.nz/assets/Uploads/211012-Draft-New-Zealand-Infrastructure-Strategy.pdf

CASE STUDY 21
New responses to cyber incidents in the United States: the 2022 Cyber Incident Reporting for Critical Infrastructure Act

When cyber incidents occur, the Department of Homeland Security provides assistance to potentially affected entities, analyses the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response. The Department works in close coordination with other agencies with complementary cyber missions, and also private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

in this context, on 15 March 2022 the Cyber Incident Reporting for Critical Infrastructure Act was signed into law. The Act imposes two new reporting obligations on owners and operators of critical infrastructure:

- Obligation to report certain cyber incidents to CISA within 72 hours of the point when the entity "reasonably believes" that such an incident has occurred
- Obligation to report ransomware payments within 24 hours

The Act essentially establishes CISA as the central federal agency responsible for cyber-reporting for companies operating within a critical infrastructure sector, advancing the forthcoming rule-making process and coordinating with other agencies in respect of information-sharing and new initiatives. After reporting an incident, in particular, covered entities are required to submit updates as "substantial new or different information becomes available" until the covered entity notifies CISA that the incident has been fully mitigated and resolved.

The Act also requires CISA to aggregate, analyse and share information learned from submitted reports to provide government agencies, Congress, companies and the public with an assessment of the constantly evolving cyberthreat landscape. When sharing information with non-federal entities and the public, CISA is required to anonymize the victim entities that filed the reports.

In the light of the Act's requirements, potentially affected entities are expected to determine whether changes to their cyberprogrammes may be required; to examine their internal policies and procedures to reflect the Act's requirements; and to address and prepare for overlapping disclosure obligations under state, federal and international laws.

Sources: www.cisa.gov/cyber-incident-response and www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/

Tool 19
Cybersecurity incident and vulnerability response playbooks – CISA: United States

www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

The playbooks are designed to provide United States federal civilian agencies with operational procedures for planning and conducting cybersecurity incident and vulnerability response activities. They apply to incidents that involve confirmed malicious cyberactivity and for which a major incident has been declared or has not yet been reasonably ruled out. Some examples include incidents involving the lateral movement, credential access or exfiltration of data; network intrusions involving more than one user or system; or compromised administrator accounts. The playbooks include one checklist for incident response and another for incident response preparation, both of which may be adapted for use by organizations outside the federal Government.

2.7 Ensuring the financial sustainability and continued relevance of strategies

CIP strategies should lay the groundwork for, first, ensuring the financial viability of the overall CIP effort; and, second, setting up, reviewing and monitoring mechanisms as part of risk management processes to update existing lists of CI and, if necessary, identification criteria, adding new critical sectors, and other measures. The institutional frameworks and processes underpinning CIP strategies should also be subject to regular scrutiny to ensure their continued relevance in the face of changing threat landscapes, lessons learned from past crises, and other factors.

2.7.1 Financial sustainability

While CI operators have primary responsibility for ensuring the protection and resilience of the critical assets and processes under their control, the enhancement of physical and cyber protection measures often requires the commitment of significant amounts of resources. Achieving CI resilience can be a costly endeavour. In such a context, CIP strategies must ensure that investments in ensuring an optimal level of CI protection are financially sustainable. In practice, States need to find balanced and viable cost-sharing arrangements between CI owners and operators, government agencies and insurance providers.

An important tool to encourage the engagement of CI owners and operators is the creation of financial incentives. These range from subsidies to tax relief efforts and loans. Incentives appear all the more important at times of economic crisis, when operators may naturally lean towards spending resources on short-term growth objectives rather than long-term security goals.

The need for government intervention in the form of financial support may also be felt in the event of disruptive events affecting CI. According to a study conducted by the International Bank for Reconstruction and Development, "the economic and social impacts from disruption to critical infrastructure come primarily from the loss of the service they provide, not from the cost of physical damages to the assets themselves. For example, direct damages from disasters to the power generation and transport infrastructure are estimated at $18 billion a year in low- and middle-income countries globally."[52]

CIP strategies may also consider the role of insurance mechanisms, in particular with a view to supporting the recovery action necessary for the reconstruction of seriously damaged assets and the restoration of interrupted services. The discussion about insurance schemes for CI only started after the events of 11 September 2001. Before then, the terrorism risk was commonly included in standard insurance policies without payment of any higher premiums. Following those events and other hugely destructive terrorist attacks, such as those that took place in Madrid on 11 March 2004, perceptions changed radically, owing to the unprecedented amounts of compensation that had to be disbursed by the insurance industry. As has been observed, "an analysis of terrorism as part of the problem of 'protection of critical infrastructures' shows that terrorism is now a recognized source of acute risks, those which are closest to the outer limit of insurability".[53] As pure reliance on market mechanisms was not satisfactory, Governments had to determine the nature and extent of their financial involvement in CI recovery actions. Nowadays, "the creation and implementation of adequate financial coverage for such events are increasingly a subject for national consideration well beyond the scope of the insurance industry alone".[54]

---

52 World Bank, *Financial Protection of Critical Infrastructure Services*, Washington, DC, 2021. Available at https://www.financialprotectionforum.org/publication/financial-protection-of-critical-infrastructure-services.

53 Erwann Michel-Kerjan, *Financial Protection of Critical Infrastructure: Uncertainty, Insurability and Terrorism Risk*, Institut Veolia Environnement, Paris, 2018, Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.1268&rep=rep1&type=pdf.

54 Ibid.

CASE STUDY 22
Incentives and funding mechanisms for CI resilience: Japan, Sweden and the United States

Japan

Japan has stepped up efforts to persuade businesses that private action aimed at strengthening cybersecurity should be seen not as a cost, but rather as an investment to promote companies' products and services and increase competitiveness. In this context, the Government has established a mechanism for rewarding companies (via financial benefits) which prioritize cyber issues. In addition, it has sponsored programmes to encourage the professional development of employees with skills in industrial cybersecurity.

Sweden

The Swedish CIP strategy recognizes that its implementation requires an increased need for resources, both human and financial. According to the 2006 Emergency Preparedness and Heightened Alert Ordinance, authorities can apply for funds from the Emergency Preparedness Allocation. Other entities may indirectly benefit from this funding mechanism by cooperating in projects with authorities identified in the ordinance.

United States

Through the Security and Resilience Challenge of the National Infrastructure Protection Plan (referred to as "NIPP"), CISA – in partnership with the National Institute of Hometown Security – funds innovative ideas that can provide technologies and tools to the critical infrastructure community. Projects funded under the NIPP Challenge are meant not only to have tangible, near-term results so that they can be quickly developed and implemented, but also to be financially, practically and logistically sustainable in the long term, so that they can enhance the security and resilience of critical infrastructure across multiple sectors for years to come. Projects are evaluated by a National Institute of Hometown Security independent panel against a range of criteria which also take into account their viability and expected impact.

Sources: www.japanindustrynews.com/2017/01/japans-approach-tackling-cybersecurity-challenges/; www.msb.se/RibData/Filer/pdf/27412.pdf; and www.cisa.gov/nipp-security-and-resilience-challenge

CASE STUDY 23
Insurance schemes for CI resilience against terrorist acts: France, Spain, the United Kingdom and the United States

France

Active since 2002, the body known as Gestion de l'Assurance et de la Réassurance des Risques d'Attentats et Actes de Terrorisme (Insurance and Reinsurance Management of the Risks of Attacks and Terrorist Acts, abbreviated as "GAREAT") is a non-profit-making structure composed of insurance companies. GAREAT manages the reinsurance of risks for acts of terrorism that cause damage in France (regardless of the country in which the act of terrorism is perpetrated). GAREAT is composed of two sections: the "Large Risks" section, which includes risks whose sums insured amount to 20 million euros or more, and the "Small and Medium-sized Risks" section, which manages risks with sums insured below 20 million euros. GAREAT relies on the principle of mutuality, whereby all members are jointly liable with the others within the same section. The State provides unlimited coverage to the GAREAT programme through the Caisse Centrale de Réassurance.

Spain

The Consorcio de Compensación de Seguros (Insurance Compensation Consortium) provides compensation for damage to people and property caused by what are defined as "extraordinary risks". In order to be entitled to compensation by the Consorcio, an insurance policy in certain specific branches must have been subscribed. Special cover by the Consorcio is provided automatically when damage is the result of an act of terrorism. The Consorcio is a public organization attached to the Ministry of Economy, Industry and Competitiveness.

United Kingdom

The system in place in the United Kingdom is a public-private partnership called "Pool Re". Most insurers providing commercial property and consequential loss insurance in the United Kingdom are members of Pool Re and have agreed to offer terrorism cover to their clients. Any policy-holders who have taken out such cover and sustain losses as a result of damage from an act of terrorism are expected to contact their insurer who will arrange for the claim to be considered under the normal procedures. Pool Re has arrangements with all its members to reimburse them the cost of claims paid out by them under the terrorism cover that they provide. Insurers pay premiums to Pool Re for this purpose. The Government has committed itself to supporting Pool Re if ever the latter has insufficient funds to pay a legitimate claim.

United States

The system operating in the United States revolves around a risk-sharing arrangement between the federal Government, the insured and the insurer. Based on the Terrorism Risk Insurance Act of 2002, insurers are obliged to offer terrorism insurance to their clients (although insurers are free to set the price of coverage). In turn, clients are not under any obligation to take out coverage. Crucially, under the Act, the attack must be certified as an "act of terrorism" by the Secretary of the Treasury. The definition requires that the attack be committed by foreign interests.

On 20 December 2019, the President signed into law the Terrorism Risk Insurance Program Reauthorization Act, which extended the Programme until 31 December 2027.

Sources: www.gareat.com; www.consorseguros.es/web/inicio; www.poolre.co.uk/ and https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program.

Tool 20

Financial Protection of Critical Infrastructure Services – International Bank for Reconstruction and Development

www.financialprotectionforum.org/publication/financial-protection-of-critical-infrastructure-services

Prepared by the International Bank for Reconstruction and Development in 2021 under the disaster risk-financing and insurance agenda of the 2020 meeting of Finance Ministers of the Asia-Pacific Economic Cooperation, this technical report focuses on protecting critical infrastructure services rather than the underpinning assets. While it mainly addresses disruptions related to natural hazards, it may also be used as a blueprint to tackle crises resulting from human-caused shocks, such as terrorism and cyberattacks. The report outlines the contours of an operational framework for the financial protection of critical infrastructure that combines three interconnected pillars:

- Financial protection of physical assets. This pillar entails having finance and plans in place to rehabilitate or reconstruct critical assets after a disaster. Protection could include, for example, public assets insurance or budgetary mechanisms such as disaster funds.
- Shock-responsive systems linking financial and operational preparedness to ensure rapid recovery of critical services. Under this pillar, preparedness implies having plans, finance and systems in place to rapidly mobilize action in the event of a shock, thereby either ensuring continuity or reducing the severity and duration of any disruptions to critical services.
- National financial protection strategy that integrates critical infrastructure to efficiently manage the contingent liabilities related to such shock-responsive systems. Under this pillar, the focus is on, first, reducing any financial shock to government balance sheets that might arise from the costs of recovering and reinstating critical services post-disasters; and, second, ensuring that timely, predictable and cost-effective finance is available in emergencies so that the Government can quickly restore services when needed.

Tool 21
Economic and financial incentives: Policy Toolkit on Governance of Critical infrastructure Resilience – OECD

www.oecd-ilibrary.org/governance/good-governance-for-critical-infrastructure-resilience_fc4124df-en

The OECD Policy Toolkit (see tool 2) contains specific recommendations, key policy questions and benchmark indicators on how economic and financial incentives can be leveraged to strengthen CI resilience for CI operators. In particular, "Governments should define a mix of policy tools to incentivize operators' investments in resilience and achieve shared resilience objectives. Such measures should address the entire infrastructure life-cycle from planning to operations, maintenance and renewal or retrofitting. Government measures to stabilize resilience should be informed by cost-benefit analysis taking into account repercussions on the cost of service.

Why is this important?

Governments can choose from a variety of policy tools and mechanisms to advance implementation of resilience objectives, from voluntary frameworks and incentive mechanisms, to regulatory or legal tools. Operators have a keen interest in maintaining the continuity of their services and their reputation by investing in resilience. Investments in resilience, however, often entail upfront costs, even if these should be compensated in terms of greater reliability of service and resilience to shocks. The question is how to find the right balance. Additional requirements imposed by governments to strengthen resilience may result in additional costs ultimately borne by customers, citizens and businesses. It is important to tailor public policy instruments to provide effective incentives for operators to invest in resilience, while managing the financial repercussions.

The regulatory approach has strengths in that it provides clear and measurable obligations, for instance setting reliability requirements, or requiring business continuity plans, insurance mechanisms and minimum security standards. If over-prescriptive, however, it can also prove costly, fail to keep pace with rapid technological developments and create compliance challenges. Imposing a compensation scheme for customers whose service is disrupted, or other types of measures may offer a more efficient way of stabilizing resilience investments, notably in public-private-partnerships. This approach also provides operators with a choice of ways to increase their resilience. Voluntary frameworks such as the development of resilience guidelines, awareness-raising activities or the sharing of good practices are often preferred option, as they favour stakeholder engagement, but they also have significant uncertainties. Finding a balance between public financial support and private investments for such resilience measures can be achieved with cost-benefit analysis methods that prioritize the most effective ways of sharing the costs of an overall collective effort towards achieving shared resilience objectives.

Key policy questions:

- Are there resilience measures defined to increase the level of protection, robustness, redundancy or adaptability across critical infrastructure life cycle?
- Are there minimum security standards in place to ensure operators invest in resilience?
- Are sectoral regulators playing a role in stabilizing critical infrastructure resilience?
- Are cost-benefit analyses being used to prioritize resilience measures, evaluate their impact on costs of services, and find cost-sharing arrangements?

Benchmark indicators:

- Implementation plans to ensure critical infrastructure resilience
- Infrastructure regulations with provisions on resilience
- Assessments of the cost-benefits of resilience measures

2.7.2 Reviewing and monitoring mechanisms

Infrastructure that is identified as delivering critical services at a certain point in time may no longer perform those functions at a later stage. Conversely, changes in the economy and in the expectations of societies may render indispensable certain assets and processes that were not prioritized before. For example, the current phase of global energy transition may render the supply of certain types of fuels less critical while enhancing the strategic value of others.

Moreover, the nature and intensity of threats affecting CI change over time. For instance, some terrorist groups may pose less of a threat in certain countries while continuing to exert pressure elsewhere. At the end of 2017, Da'esh had lost control of approximately 95 per cent of the territory that it used to control in 2014. CI located in those areas became less exposed to the type of threats posed by Da'esh, while potentially being subject to other sources and types of threat. By

contrast, the geopolitical upheaval taking place in the Middle East – accompanied by the return of several Da'esh operatives and foreign terrorist fighters to their countries of origin – has made intelligence agencies increasingly worried about the heightened risk of terrorist attacks targeting CI in those countries.

CIP strategies – and related institutional frameworks and processes – may also become inadequate in the light of the experience gathered by countries in actual crisis management. Certain processes enshrined in strategic documents and action plans may reveal their inadequacy when these processes are tested on the ground.

With this in mind, CIP strategies need to provide for mechanisms which, at regular time intervals, aim to:

- Update what are often vast lists of national CI
- Determine whether certain sectors and subsectors need to be added or removed from those regarded as "critical"
- Ensure that all stakeholders engage in the regular reassessment of threats affecting CI and related vulnerabilities
- Adopt a lessons-learned approach to the fine-tuning of strategic goals, frameworks, coordination mechanisms and other processes

CASE STUDY 24
Reviewing lists of critical assets and strategies: Canada and Spain

Canada

The Canadian National Strategy for Critical Infrastructure requires "federal, provincial and territorial governments [to) work together to monitor the implementation of the Strategy and support the assessment of programs and activities targeted at enhancing the resiliency of critical infrastructure in Canada".

Spain

According to Royal Decree 704/2011, setting forth regulations for the protection of critical infrastructure, "in the event of a significant modification affecting the infrastructures listed [in the National Catalogue], when these modifications are relevant for the purposes foreseen in these regulations, the competent operators will provide, through the means put at their disposal by the Ministry of the Interior, the new information to the National Centre for the Protection of Infrastructures and Cybersecurity (CNPIC), which shall validate them prior to their inclusion into the Catalogue. In any event, the update of available information should take place on an annual basis" (art. 5.5)

Sources: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf and www.boe.es/buscar/act.php?id=BOE-A-2011-8849.

3. Establishing liability

> Security Council resolution 2341 (2017)
>
> The Security Council […]
>
> ...
>
> Recalls its decision in resolution 1373 (2001) that all States shall establish terrorist acts as serious criminal offences in domestic laws and regulations, and calls upon all Member States to ensure that they have established criminal responsibility for terrorist attacks intended to destroy or disable critical infrastructure, as well as the planning of, training for, and financing of and logistical support for such attacks

CIP strategies need to consider a two-pronged liability regime to tackle conduct that jeopardizes CI security:

- A regime of criminal responsibility for those who carry out attacks (or who threaten or plan such attacks) on CI (sections 3.1–3.3)
- A sanctions regime for individuals and entities with statutory and regulatory responsibilities in terms of protecting and securing CI falling within their remit (section 3.4)

3.1 Criminalization requirements in the universal legal framework against terrorism

A distinctive feature of resolution 2341 (2017) consists in its call upon Member States to specifically criminalize acts against CI. In doing so, the Security Council builds upon a number of previously adopted instruments that set forth general requirements for Member States in terms of bringing to justice perpetrators of terrorist acts and facilitators thereof. The landmark instrument in this field is resolution 1373 (2001). Adopted shortly after the events of 11 September 2001, this instrument provides for, among other measures, a comprehensive set of criminal justice requirements, such as the obligations to:

- Criminalize the provision or collection of funds in relation to the commission of terrorist acts
- Deny safe heaven to all those who plan, support or commit terrorist acts and bring them to justice
- Establish terrorist acts as serious criminal offences in domestic laws

In addition to Security Council resolutions, a series of treaties dealing with the prevention and suppression of international terrorism set forth criminalization requirements in the CI domain. In the absence of agreement on the scope of application of a comprehensive treaty covering all aspects and manifestations of international terrorism, these separate instruments were adopted over the course of some fifty years. The incremental, sector-specific and pragmatic approach followed by the international community has resulted in the adoption of conventions and protocols dealing with such specific areas as maritime and aviation security, nuclear and terrorist financing, and others.

The text of the above-mentioned treaties, which together constitute what is termed below “the universal legal framework against terrorism”, does not employ the expression “critical infrastructure”. As illustrated in table 4, however, most of them include offence-creating provisions directly targeting conduct aimed at destroying or interfering with the functioning of CI. To the extent that Member States are parties to these treaties, they are required to incorporate their provisions in their

domestic law. This entails, notably, establishing the conduct set forth in those instruments as criminal offences in their national legislation.[55]

Table 4
CI-related offences under the universal legal framework against terrorism

Sector	Conventions and protocols	Main offences[a]
Aviation	Tokyo Convention (1963): Convention on Offences and Certain Other Acts Committed on Board Aircraft, as amended by the Montreal Protocol	Requires the following contracting States to establish jurisdiction to punish offences committed on board aircraft: • State of registration of the aircraft • State of landing, when the aircraft on board which the offence is committed lands in its territory with the alleged offender still on board • State of the operator, when the offence is committed on board an aircraft leased without crew to a lessee whose principal place of business or, if the lessee has no such place of business, whose permanent residence, is in that State
	Hague Convention (1970): Convention for the Suppression of Unlawful Seizure of Aircraft and its supplementary Beijing Protocol (2010)	Seizing or exercising control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means
	Montreal Convention (1971): Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, supplemented by the Montreal Protocol (1988): Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation; and the Beijing Convention (2010): Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation	• Performing an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft • Destroying an aircraft in service or causing damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight • Placing, or causing to be placed on an aircraft in service, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight • Destroying or damaging air navigation facilities or interfering with their operation, if any such act is likely to endanger the safety of aircraft in flight • Communicating information which is known to be false, thereby endangering the safety of an aircraft in flight • Using against or on board an aircraft in service any biological, chemical or nuclear weapon or explosive, radioactive, or similar substances in a manner that causes or is likely to cause death, serious bodily injury or serious damage to property or the environment; • Destroying or seriously damaging the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupting the services of the airport, if such an act endangers or is likely to endanger safety at that airport

[55] As provided by resolution 1373 (2001), Member States that have not yet become parties to one or more of the above-mentioned counter-terrorism conventions and protocols are called upon to do so as soon as possible.

Sector	Conventions and protocols	Main offences[a]
Maritime	1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation	• Seizing or exercising control over a ship by force or threat thereof or any other form of intimidation • Performing an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship • Destroying a ship or causing damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship • Placing or causing to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship • Destroying or seriously damaging maritime navigational facilities or seriously interfering with their operation, if any such act is likely to endanger the safe navigation of a ship • Communicating information known to be false, thereby endangering the safe navigation of a ship
	2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation	When the purpose of the act is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act: using against or on a ship or discharges from a ship any explosive, radioactive material or biological, chemical or nuclear weapon in a manner that causes or is likely to cause death or serious injury or damage
	1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf	• Seizing or exercising control over a fixed platform by force or threat thereof or any other form of intimidation • Performing an act of violence against a person on board a fixed platform if that act is likely to endanger its safety • Destroying a fixed platform or causing damage to it which is likely to endanger its safety • Placing or causing to be placed on a fixed platform a device or substance which is likely to destroy that fixed platform or likely to endanger its safety.
	2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf	When the purpose of the act is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act: using against or on a fixed platform or discharges from a fixed platform any explosive, radioactive material or biological, chemical or nuclear weapon in a manner that causes or is likely to cause death or serious injury or damage
Nuclear	2005 International Convention for the Suppression of Acts of Nuclear Terrorism and 2005 Amendment to the Convention on the Physical Protection of Nuclear Material	Using or damaging a nuclear facility, interfering with its operation, or committing any other act directed against a nuclear facility in a manner which releases or risks the release of radioactive material, • With the intent to cause death or serious bodily injury; or substantial damage to property or to the environment; or • With knowledge that the act is likely to cause death or serious injury to any person or substantial damage to property or to the environment by exposure to radiation or release of radioactive substances unless the act is undertaken in conformity with the national law of the State Party in the territory of which the nuclear facility is situated; or • To compel a natural or legal person, an international organization or a State to do or refrain from doing an act.
Diplomatic personnel	1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons	Carrying out a violent attack upon the official premises, the private accommodation or the means of transport of an internationally protected person likely to endanger his or her person or liberty.
Government facilities, public transport systems	1997 International Convention for the Suppression of Terrorist Bombings	Delivering, placing, discharging or detonating an explosive or other lethal device into or against a place of public use, a State or government facility, a public transport system or an infrastructure facility with the intent to cause extensive destruction of such a place, facility or system, where such destruction results in, or is likely to result in, major economic loss.
	1999 International Convention for the Suppression of the Financing of Terrorism	Placing or providing funds for the purpose or in the knowledge that the funds will be used to commit an act of terrorism (as defined in the Convention itself) or any other act set forth in one of the universal instruments against terrorism
Financing of terrorist acts against CI	1999 International Convention for the Suppression of the Financing of Terrorism	Placing or providing funds for the purpose or in the knowledge that the funds will be used to commit an act of terrorism (as defined in the Convention itself) or any other act set forth in one of the universal instruments against terrorism

[a] For the full range of criminalization requirements and exact wording used by the conventions, see their official texts.

Beside the universal legal framework against terrorism, a number of counter-terrorism regional instruments establish CI-related criminalization requirements, in particular in the field of CII. A ground-breaking instrument in his field is the 2001 Council of Europe Convention on Cybercrime, which introduced for the first time criminal conduct dealing with violation of network security (in addition to establishing powers and procedures such as the search of computer networks and interception). More recently, the European Union has adopted a directive aimed at harmonizing the criminal law of the member States in the area of attacks against information systems. Another example is the 2014 African Union Convention on Cyber Security and Data Protection (see box 13).

Box 13
Criminalization of attacks against information systems: European Union and African Union legal frameworks

- 2013 European Union Directive on attacks against information systems

A key objective of the 2013 European Union Directive is the establishment of minimum rules for the definition of criminal offences and corresponding sanctions. The Directive provides for criminal penalties at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. The Directive addresses, for example, the creation of so-called "botnets", in other words, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyberattacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyberattack.

The Directive identifies three aggravating circumstances whereby the offences in question need to be punished by a maximum term of imprisonment of at least five years, namely:

- When they are committed within the framework of a criminal organization
- When they cause serious damage
- When they are committed against a critical infrastructure information system

2014 African Union Convention on Cyber Security and Data Protection

Adopted in 2014, the African Union Convention requires that "each State Party … adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure" (art. 25).

In addition to establishing offences dealing with direct attacks on computer systems, the Convention adopts a markedly preventative approach to the commission of cyber-related offences. Under article 29, paragraph 1 (h), in particular, Parties undertake to "make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing access to part or all of a computer system".

3.1.1 Criminalization and international cooperation

An important reason why Member States should criminalize conduct identified in the universal legal framework against terrorism is to facilitate international cooperation in criminal matters. Significant obstacles to such cooperation will be removed if the relevant (namely, CI-related) offences are introduced in the criminal legislation of States parties. Crucially, the requirement that extradition and mutual legal assistance can only be granted when the offence in question is criminalized in both the requested and the requesting country (known as the "dual criminality" principle) would be automatically fulfilled if both parties faithfully transpose treaty language into their respective criminal statutes.

At the same time, the ability of individual countries to successfully prosecute offenders will often depend on the effectiveness of existing international channels for law enforcement cooperation, the surrender of fugitives and the exchange of evidence. Countries seeking to maximize the protection of CI from the criminal justice angle should consider the role of the universal framework against terrorism in providing legal bases for extradition and mutual legal assistance, either in support of or in the absence of bilateral or regional arrangements to this effect.

Whatever cooperation channel is used, Member States need to ensure full respect for fair trial and due process standards. This applies not only in the context of domestic proceedings aimed at ascertaining individuals' criminal responsibility, but also those instituted on behalf of other countries for the surrender of fugitives or the transmission of evidentiary items.

3.2 National approaches to the establishment of criminal liability for attacks on CI

The criminalization of acts directed at CI is instrumental in achieving three interconnected objectives:

- Providing adequate levels of deterrence through the application of serious penalties on perpetrators of terrorist acts against CI
- Disrupting criminal and terrorist plans directed at CI through the use of criminal law as a preventive tool, noting the requirement set forth in resolution 2341 (2017) for Member States to establish as criminal offences "the planning of, training for, and financing of and logistical support" for terrorist attacks
- Setting the legal bases and conditions for smooth international cooperation in the criminal justice field on CI-related matters

As mentioned in section 3.1, national authorities shall establish as criminal offences conduct identified in the universal legal instruments against terrorism to which they are parties. As these instruments only cover CI in a piecemeal fashion, however, Member States also need to determine the extent to which CI-related offences should be criminalized beyond what is strictly required by those instruments. In planning the introduction of comprehensive CI-related criminal and terrorism-related legislation, Member States should bear in mind that there is no international definition of "critical infrastructure".

In general terms, three broad drafting options may be envisaged:

- Criminalize conduct related to specific types of infrastructure ("sector-specific approach")
- Criminalize conduct against CI regardless of the sector or sectors to which the affected CI belongs ("cross-sectoral approach")
- Rely on general criminal legislation which applies to CI although it was not designed for CI protection purposes ("non-CI-specific approach")

It is worth noting that the above-mentioned approaches are not mutually exclusive and, in practice, countries often adopt an amalgam of the three. Whichever approach (or combination of approaches) is chosen, criminal offences should be formulated in accordance with the principle of legality. This requires that criminal liability and punishment be based upon a prior enactment of a prohibition that is expressed with adequate precision and clarity.

3.2.1 Sector-specific approach

CI-related offences can target specific critical sectors such as those in the nuclear, transport and other fields. Relevant conduct can be criminalized with or without envisaging a specific terrorist purpose as an element of the offence. While resolution 2341 (2017) calls upon States to be able to establish criminal responsibility for terrorist attacks, it certainly does not preclude countries from broadening the scope of the offences in question by criminalizing conduct that is not linked to a terrorist purpose. Indeed, the wording used in most of the universal legal instruments against terrorism supports this outcome. For example, the 1970 Convention for the Suppression of Unlawful Seizure of Aircraft requires that Parties establish as an offence the act of taking control on an aircraft (by force or threat thereof or any other form of intimidation) regardless of the specific intention or the underlying motivations of the offender.

Several examples of sector-specific legislation are found in so-called "common law" countries, such as the Fijian Civil Aviation (Security Act), 1994, the Sri Lankan Suppression of Terrorist Bombings Act, 1999, and the United Kingdom Internationally Protected Persons Act, 1978. Often, when a sector-specific approach is chosen, related offences are part of broader normative frameworks also designed to regulate in detail sector operations, licensing requirements and procedures, and other such matters. An example is the Japanese Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors.

The advantage of this approach is that it allows countries to fine-tune their criminalization requirements to the threats that are specific to certain types of infrastructure and sectors. It also facilitates the identification of penalties that more accurately reflect perceptions of the level of criticality of certain assets and expected impacts in case of disruptions. The main downside of this approach is that it restricts the reach of criminal law to a closed list of sectors and assets, thus leaving the others unattended and in need of separate legislative action.

3.2.2 Cross-sectoral approach

Some Member States adopt legislation to criminalize attacks against CI as such, regardless of the sectors to which it belongs. The advantage of this approach is that it provides a framework to ensure coverage of all CI sectors, including those that may potentially be added as critical ones in the future. One possible disadvantage is the lack of precision, in that the applicable legislation may establish one set of sanctions which is indistinctively applicable across sectors. In such cases, policymakers may consider – while still respecting the principle of legality – establishing a wider penalty window, enabling judges to adjust sanction levels to the specific circumstances of each case.

Cross-sectoral criminal offences may or may not envisage a terrorist intention. When they do, acts perpetrated against CI are squarely placed within the scope of counter-terrorism legal frameworks with all the consequences in terms of specialized procedures, investigative techniques, competent authorities, and so forth. Most commonly, domestic counter-terrorism statutes refer to "public infrastructure" or "essential services, facilities or systems" whenever their destruction or interference in their functioning leads to major economic loss, danger for human life, and other such effects.[56]

It is worth noting that a number of laws criminalizing attacks against CI as terrorist acts provide exemptions for action taken in the context of the legitimate exercise of certain civil, political or social rights. For example, the Canadian criminal code excludes from the notion of "terrorist activity" those acts that, while causing "serious interference with or serious disruption of an essential service, facility or system, whether public or private" are committed as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in what is defined as terrorist activity.[57]

[56] For example, Kenyan legislation defines "terrorist act" as an act or threat of action which, among others, "interferes with an electronic system resulting in the disruption of the provision of communication, financial, transport or other essential services [or] interferes or disrupts the provision of essential or emergency services".

[57] Criminal code, 83.01(1).

Box 14
CI and the European Union Framework Decision on Combating Terrorism

Under the European Union Framework Decision on Combating Terrorism,[58] several types of attacks against CI are regarded as "terrorist offences", notably:

- Extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss
- Seizure of aircraft, ships or other means of public or goods transport
- Interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/ ?uri=CELEX :32002F0475&from=EN.

CASE STUDY 25
Cross-sectoral approach to criminalization: Canada

Canadian criminal legislation identifies a set of offences comprising conduct aimed at damaging, disrupting and in other ways interfering with "essential infrastructure", as defined in the 2020 Critical Infrastructure Defence Act:

Prohibitions

2. (1) No person shall, without lawful right, justification or excuse, wilfully enter on any essential infrastructure.

(2) No person shall, without lawful right, justification or excuse, wilfully damage or destroy any essential infrastructure.

(3) No person shall, without lawful right, justification or excuse, wilfully obstruct, interrupt or interfere with the construction, maintenance, use or operation of any essential infrastructure in a manner that renders the essential infrastructure dangerous, useless, inoperative or ineffective.

(4) No person shall aid, counsel or direct another person to commit an offence under subsection (1), (2) or (3), whether or not the other person actually commits the offence.

(5) A person who enters on any essential infrastructure, having obtained by false pretences permission to enter on the essential infrastructure from the owner or an authorized representative of the owner, is deemed to have contravened subsection (1) unless the person had a lawful right, justification or excuse to enter on the essential infrastructure.

Offences and penalties

3(1) A person who contravenes section 2 is guilty of an offence and liable

(a) in the case of an individual,

(i) for a first offence, to a fine not less than $1000 and not exceeding $10 000, or to imprisonment for a term not exceeding 6 months, or to both a fine and imprisonment, and

(ii) for a 2nd or subsequent offence in relation to the same premises, to a fine not less than $1000 and not exceeding $25 000, or to imprisonment for a term not exceeding 6 months, or to both a fine and imprisonment, and

(b) in the case of a corporation, to a fine not less than $10 000 and not exceeding $200 000.

(2) Where a corporation commits an offence under subsection (1), any officer, director or agent of the corporation who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is guilty of that offence and liable to the penalty provided for the offence, whether or not the corporation has been prosecuted for or convicted of that offence.

(3) Each day that a contravention continues constitutes a separate offence.

Source: www.canlii.org/en/ab/laws/stat/sa-2020-c-c-32.7/latest/sa-2020-c-c-32.7.html.

[58] European Union Framework Decision of 13 June 2002 on Combating Terrorism (2002/475/JHA), art. 1.

CASE STUDY 26
Two criminal law frameworks on CIP: South Africa

South Africa contemplates criminal sanctions for acts targeting CI both in its 2004 counter-terrorism legislation and its 2019 Critical Infrastructure Protection Act.[59]

2004 Protection of Constitutional Democracy against Terrorist and Related Activities Act

"Terrorist activity" is understood as:

(a) any act committed in or outside the Republic, which:

…

(vi) is designed or calculated to cause serious interference with or serious disruption of an essential service, facility or system, or the delivery of any such service, facility or system, whether public or private, including, but not limited to

(aa) a system used for, or by, an electronic system, including an information system;

(bb) a telecommunication service or system;

(cc) a banking or financial service or financial system;

(dd) a system used for the delivery of essential government services;

(ee) a system used for, or by, an essential public utility or transport provider;

(ff) an essential infrastructure facility; or

(gg) any essential emergency services, such as police, medical or civil defence services;

(vii) causes any major economic loss or extensive destabilization of an economic system or substantial devastation of the national economy of a country; or

(viii) creates a serious public emergency situation or a general insurrection in the Republic, whether the harm contemplated in paragraphs (a) (i) to (vii) is or may be suffered in or outside the Republic, and whether the activity referred to in subparagraphs (ii) to (viii) was committed by way of any means or method; and

(b) which is intended, or by its nature and context, can reasonably be regarded as being intended, in whole or in part, directly or indirectly, to

(i) threaten the unity and territorial integrity of the Republic;

(ii) intimidate, or to induce or cause feelings of insecurity within, the public, or a segment of the public, with regard to its security, including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population; or

(iii) unduly compel, intimidate, force, coerce, induce or cause a person, a government, the general public or a segment of the public, or a domestic or an international organization or body or intergovernmental organization or body, to do or to abstain or refrain from doing any act, or to adopt or abandon a particular standpoint, or to act in accordance with certain principles,whether the public or the person, government, body, or organization or institution referred to in subparagraphs (ii) or (iii), as the case may be, is inside or outside the Republic; and

(c) which is committed, directly or indirectly, in whole or in part, for the purpose of the advancement of an individual or collective political, religious, ideological or philosophical motive, objective, cause or undertaking

2019 Protection of Critical Infrastructure Act

Absent a "terrorist intention", or in cases not covered by the 2004 counter-terrorism legislation, the 2019 Protection of Critical Infrastructure Act may provide an alternative legal basis for prosecuting acts directed at CI.

[59] 7 Arguably, if the conduct in question falls within the scope of both legal frameworks, counter-terrorism legislation would apply as lex specialis if the specific "terrorist intention" set forth in the counter-terrorism law is proven.

Where the applicable penalties are concerned, these are modulated by the 2019 Act depending on whether the conduct in question involves CI that has been categorized as low-risk, medium-risk or high-risk. The categorization takes place at the time when the competent national authorities decide to classify a specific asset as being critical. The assessment must take into account both the probability of failure, disruption or destruction of the infrastructure in question or threat thereof; and the impact and consequence of failure, disruption or destruction of infrastructure or threat thereof (section 19).

(7) Under the 2019 Act,[60] criminal penalties are established for any person who unlawfully:

(a) furnishes, disseminates or publishes in any manner whatsoever information relating to the security measures applicable at or in respect of a critical infrastructure other than in accordance with the Protected Disclosures Act, 2000 (Act No. 26 of 2000), the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other Act of Parliament that provides for the lawful disclosure of information;

(b) takes or records, or causes to take or record, an analog or digital photographic image, video or film of the security measures at a critical infrastructure;

(c) hinders, obstructs or disobeys a person in control of a critical infrastructure in taking any steps required or ordered in terms of this Act in relation to the security of any critical infrastructure;

(d) hinders, obstructs or disobeys any person while performing a function or in doing anything required to be done in terms of this Act;

(e) enters or gains access to critical infrastructure without the consent of the security manager or person in control of that critical infrastructure;

(f) enters or gains access to critical infrastructure in contravention of the notice contemplated in section 24(8) or 25(8);

(g) damages, endangers or disrupts a critical infrastructure or threatens the safety or security at a critical infrastructure or part thereof;

(h) threatens to damage critical infrastructure; or

(i) colludes with or assists another person in the commission, performance or carrying out of an activity referred to in paragraphs (a) to (h), commits an offence and is, subject to subsection (3) and (4), liable on conviction to a fine or to imprisonment for a period not exceeding three years, or to both a fine and imprisonment.

3.2.3 Non-CI-specific approach

In some cases, criminal acts perpetrated against CI are sanctioned by being categorized as so-called "standard", or "classical", offences such as damage to property, arson, trespassing and others.

One advantage of the non CI-specific approach is that Member States may rely on a set of basic and well-established offences whenever more targeted criminal legal frameworks are unavailable. In addition, the criminal justice officials of some countries may be more familiar with the application of classical offences than they would be with new CI-related regimes. Moreover, it is far more likely that certain basic offences – including those rooted in the common law tradition – may be accompanied by much more solid and consolidated jurisprudence and case-law precedents.

Drawbacks to this approach include the lack of differentiation between essential and non-essential assets, which may lead to the application of penalties that do not reflect the more severe impacts – or potential impacts – caused by the disruption of critical infrastructure. Added to which, the prohibition to apply criminal laws by analogy may raise questions about the possibility of assigning offences to the cyber domain that were conceived for the physical world only (for example, using traditional trespassing offences to deal with unauthorized access to computer systems).[61]

[60] Chap. 5, Offences and penalties, sect. 26.

[61] From a practical point of view, the investigation of cyber offences poses particular challenges in terms of attribution of the conduct in question.

3.3 Reach of CI-related criminal legislation

When drafting CI-related criminal legislation, careful consideration should be given to its scope of application. In particular, national authorities should ensure that the competent national courts can exercise their jurisdiction in the following scenarios:

- An attack perpetrated against CI located in the territory of the State when the attack produces substantial effects in another State. For example, an industrial control system located in Country A governs gas delivery in Country B. Following the manipulation of the industrial control system, disruptions are felt in Country B, but not in Country A. This latter should nonetheless be in a position to bring the alleged perpetrators to justice.

  Following an attack against CI located in Country A, the alleged perpetrator escapes to Country B. The universal legal framework against terrorism requires that parties establish their extraterritorial jurisdiction over acts committed abroad in at least two cases:

  - The offence was committed by one of their nationals (active nationality principle).
  - The alleged perpetrator is found on the territory of the State and is not extradited to any State requesting extradition for the same conduct (so-called "aut dedere aut judicare" principle).

Box 15
Compulsory and optional jurisdiction under the universal legal framework against terrorism

Most universal counter-terrorism treaties set forth specific jurisdictional criteria. For example, in the case of an offence involving aircraft under the 1970 Convention for the Suppression of Unlawful Seizure of Aircraft and the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, national courts shall establish jurisdiction over offences on board the aircraft, if the aircraft lands in the territory of the State with the alleged offender still on board and no other State party requests his or her extradition for prosecution purposes.

Other treaties provide for optional grounds for jurisdiction, for example, in the case of offences committed abroad against a national (known as the "passive nationality principle"). National authorities should consider introducing such additional grounds and determine, for cases or CI sectors not covered by the applicable international legal framework, the appropriate reach of their CI-related criminal laws.

CASE STUDY 27
Ensuring the proper shaping and application of criminal legislation in the cybersecurity field

In December 2014, the Criminal Division of the United States Department of Justice created a Cybersecurity Unit within the Computer Crime and Intellectual Property Section. One of the Unit's objectives is to ensure that law enforcement authorities are used effectively to bring perpetrators to justice while also protecting the privacy of ordinary citizens. In pursuing this objective, the Unit also helps to shape cybersecurity legislation to protect the country's computer networks and individual victims from cyberattacks. The Unit also engages in outreach activities to the private sector with a view to promoting lawful cybersecurity practices. The Cybersecurity Unit is led by the Special Counsel for National Security at the Computer Crime and Intellectual Property Section.

Source: www.justice.gov/criminal-ccips/cybersecurity-unit.

3.4 Sanctions for breaching CIP regulatory frameworks

CI needs to be protected not only from those who intentionally seek to disrupt its operations, but also from the risk that those in charge of their security fail to comply with the established regulatory frameworks. For example, the legislation of a number of Member States, in particular those that predominantly apply a mandatory approach to CIP (see section

2.5.1), requires CI operators to prepare detailed security plans involving the critical assets or processes under their control. Those plans typically need to be submitted within specific time frames. Domestic regulations may also require that the competent authorities carry out inspections at specific CI facilities to verify that submitted security plans have been duly implemented. Other potential infringements of security-related obligations concern the dissemination or publication of confidential information about assets' vulnerabilities, adopted or planned mitigation measures, and so forth.

In all these instances, Member States need to ensure that a proper sanctioning regime is in place; this is achieved, typically, through a mix of administrative and criminal sanctions, depending on the gravity (or the reiteration) of the conduct in question.

CASE STUDY 28
Inspection and sanctions regime for CI operators: France

France adopts what may be termed an "incremental" approach to the imposition of sanctions against non-compliant operators. This approach aims to first engage operators in a sustained dialogue in the event that site inspections reveal potential security issues.

The task of controlling security levels at a given CI facility is entrusted to an interministerial defence and security committee and a local commission on defence and security, supported by the departmental prefects. Inspection reports aim to highlight vulnerabilities vis-à-vis identified threats and recommend measures to be taken to strengthen resilience. An immediate assessment is carried out at the end of the inspection in the presence of the person responsible for CI security. This meeting aims to present not only the initial evaluation by the inspection team, but also to ascertain the operator's viewpoint.

The second step is the drawing up of an inspection report which contains recommendations for improving

the protection of the CI in question in relation to its context and its security reference system. The report highlights CI vulnerabilities in the face of the identified threats and the measures to be taken to mitigate risks and reduce the likelihood of attacks. The supervisory authority, and also the prefect of the department, are informed of the follow-up given to the inspection report.

In the case of reported problems, the above-mentioned process can lead to the revision of the operator's plan, or a formal notice to execute, within a period of between one and three months, the security measures that have not been carried out. Only in extreme cases of non-compliance can the process lead to referral to the judicial authority for the application of criminal sanctions.

Source: www.legifrance.gouv.fr/download/pdf/circ?id=37828.

4. Sharing information and experience

Security Council resolution 2341 (2017)

The Security Council

…

4. Calls upon Member States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to or recovery from terrorist attacks planned or committed against critical infrastructure;

5. Further calls upon States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks;

…

7. Encourages the United Nations as well as those Member States and relevant regional and international organizations that have developed respective strategies to deal with protection of critical infrastructure to work with all States and relevant international, regional and subregional organizations and entities to identify and share good practices and measures to manage the risk of terrorist attacks on critical infrastructure.

Addendum to the Madrid Guiding Principles

Guiding principle 50

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

…

(g) Establish or strengthen mechanisms to share information, expertise (such as tools, guidance) and experience among public and private stakeholders to investigate and respond to terrorist attacks on such targets.

Guiding principle 51

In their further efforts to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider:

…

(b) Putting in place national frameworks and mechanisms to support risk-based decision-making, information-sharing and public-private partnering for both Government and industry, including with a view to working together to determine priorities, ...

…

(d) Establishing processes for sharing relevant information with industry and private sector partners by, for example, issuing security clearances and increasing awareness

4.1 Information-sharing in the context of CIP strategies

The development of well-functioning channels for information-sharing among all stakeholders involved in CIP efforts is an essential ingredient of success and a key factor on which PPPs should be built (see sect. 2.4.2). Inter-agency coordination is also predicated on solid information-sharing protocols and practices (see chap. 7). Furthermore, the extent and quality of international cooperation on CI are shaped by States' ability and willingness to exchange information across borders (see chapter 8).

4.2 Dimensions of information-sharing for CIP

In setting the broad operational framework for information-sharing, CIP strategies and related implementation plans should address three basic issues:

- What information should be exchanged.
- How information should be shared for any given task.
- Among which entities information should be shared and on which levels of confidentiality it should be based.

Information for CIP needs to be exchanged at the strategic, technical and tactical levels. From another perspective, information can be incident or non-incident related. It can also take the form of real-time exchange of information in the context of imminent or ongoing crises, when the recipient is expected to take immediate action. Whenever this latter type of information is concerned, the platforms for information-sharing (with related security features) will be structured very differently from those that seek to convey best practices, strategic advice, or other benefits.

Information-sharing can (and should) occur between different types of stakeholders:

- Between competent public authorities and CI operators (both within a given sector and across sectors)
- Between one or more CI operators and other CI operators (both within a given sector and across sectors)
- Between one or more public authorities and other public authorities, (inter-agency information exchange)

All the above-mentioned types of information-sharing channels can – and, indeed, should – be established both among domestic stakeholders and among entities belonging to two or more countries.

Tool 22
Knowledge portal (Cybil portal) – Global Forum on Cyber Expertise

https://cybilportal.org/

Facilitated by the Global Forum on Cyber Expertise, the Cybil portal is a knowledge-sharing portal for the international cyber capacity-building community. The portal enables Governments, funders and implementing agencies to find and share best practices and practical information to support the design and delivery of capacity-building projects and activities. It also acts as a source of information on cybersecurity and capacity-building in cybercrime prevention for civil society, the academic sector and the technical community.

The overall aim of the portal is to establish a neutral, open and globally owned multi-stakeholder knowledge-sharing platform that makes possible the following:

- Sharing of data, information and results of global cyber capacity-building efforts
- Ensuring transparent access to data and information on cyber capacity-building tools with a simple user interface
- Integration of existing resources and information that are already available
- More effective use of cyber capacity-building resources for capacity-building programming by the Global Forum on Cyber Expertise community;
- Harmonization of cyber capacity-building initiatives and approaches.

4.2.1 Information-sharing between government authorities and CI operators

The exchange of information between public agencies with CIP responsibilities and CI operators – regardless whether these latter are public or private entities[62] – should flow from both directions and cover, notably:

- Threat assessments: Law enforcement bodies and intelligence services should provide CI operators with national threat assessments affecting specific critical assets and processes and critical sectors. This information needs to be fed into the risk assessments that CI operators are expected to conduct, often in compliance with regulatory requirements mandating them to prepare and share CI-level security plans. Conversely, it is essential for individual CI operators to share their own threat assessments with the competent government authorities for these latter to be able to paint an accurate picture of the threat, both within a given CI sector and at the cross-sectoral level.
- Suspicious activities: CI operators have a critical role to play in observing and reporting unusual activities taking place within or around the assets and processes of which they are in charge. This task should be the responsibility not only of those specifically in charge of security, but also those who get into contact with CI assets, processes and systems as employees, contractors, suppliers, and other stakeholders. Appropriate awareness-raising programmes and training activities should be in place to ensure that those people are in a position to recognize suspicious behaviour and know to whom to report it.
- Incident-related data and perspectives: Lessons learned from past incidents (including successful practices and interventions and failures) offer important insights into ways of preventing the same situation from reoccurring. This, in turn, provides a basis for more effective risk management and recovery action.

Box 16
Public-private information-sharing on cyberterrorism threats

OSCE has compiled a table summarizing the main types of CI-related information that the public sector needs to exchange with the private sector (and vice versa) to address cyber-related terrorist threats. While the table focuses on the energy sector, information that it contains therein is relevant to other critical sectors as well.[63]

Public sector[64] information	Private sector information
• Insights about cybercapabilities of key terrorist organizations	• Information about major asset categories in the energy sector (such as gas, oil, electricity and renewables data; reliability indicators; information from energy trade exchanges)
• Information about linkages between different terrorist and non-terrorist groups	• Technical vulnerability information for specific hardware and software products used by energy infrastructure operators
• Insights about past attack vectors	• Anonymized information about the impact of past attacks
• Insights on possible future attack vectors deduced from analyses of cybercriminal underground websites	• Insights on recovery needs to deal with different forms of attacks
	• Insights from attack patterns in other critical infrastructure sectors that could serve as early warning indicators for the energy sector

Information-sharing with the competent government authorities may present particular challenges due to frequent manifestations of mutual suspicion, in particular when critical assets are operated by private-sector entities. According to OSCE,

62 The process of privatization of several CI sectors and subsectors such as gas, postal systems and telecommunication services, which has historically occurred in many countries, has resulted in several CI operations falling into private hands. This, in turn, has generated the need for strong public-private partnerships. Information exchange for CIP purposes is a vital task to be performed under such partnerships.

63 See www.osce.org/files/f/documents/4/b/103500.pdf.

64 Reference to "public sector" in the table is understood to cover government agencies.

"in terms of security awareness, there is still a great discrepancy between the actual potential threat of targeted attacks and how they are perceived. This is mainly due to the fact that most attacks that take place in the areas of energy supply and industry are not made public, since the operators of affected installations have no desire to make these incidents known. This approach creates a situation (incidents are perceived as isolated events) that strengthens this tendency to keeping incidents secret. Industry in some countries is asked, encouraged, and sometimes obligated to report these incidents."[65]

In the end, establishing smooth flows of information between privately-operated CI and the competent government authorities may be seen as a goal in and of itself, helping to create a genuine sense of community around CIP issues.

CASE STUDY 29
Incentives for the private sector to share information as part of the cybersecurity strategy: Japan

The Japanese 2015 cybersecurity strategy sought to overcome the reluctance of businesses to share information with public authorities for fear of losing credibility or market share. According to this strategy, to make information-sharing more active, it is essential to relieve CII operators' psychological burden of potentially losing the credit or ruining the reputation of their businesses if providing information to a relevant party and enable them to recognize the advantages of such action instead. The Government will encourage CII operators to create a common understanding on making appropriate modifications of information to be provided, such as concealing informers' identities and specifying the scope and limit of information to be shared and will create an environment where informers will not suffer any unreasonable loss or disadvantage from providing information.

Source: www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

CASE STUDY 30
Automated indicator sharing, CISA: United States

Automated indicator sharing (referred to as "AIS") is a functionality developed by CISA. It enables the real-time exchange of machine-readable cyberthreat indicators and defensive measures to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks. Threat indicators and defensive measures may include, for example, information about attempted adversary compromises as they are being observed, to help protect other participants of the AIS community and limit the adversary's use of an attack method.

The AIS community includes private sector entities, federal departments and agencies, state, local, tribal, and territorial governments, information-sharing and analysis centres and organizations and foreign partners and companies. AIS is offered at no cost to participants as part of the CISA mission to work with public and private sector partners to identify and help mitigate cyberthreats through information-sharing.

AIS uses two open standards: the Structured Threat Information Expression (known as "STIX™") for cyberthreat indicators and defensive measures information and the Trusted Automated Exchange of Indicator Information ("TAXII™") for machine-to-machine communications. Valuing organizational privacy, AIS anonymizes submissions by default when transmitting them, meaning that the identity of submitters is not revealed without their prior express consent.

In the future, CISA intends to provide additional AIS features to enable participants to identify the most operationally relevant indicators. As it solicits participant feedback, CISA plans to introduce updates to make AIS as useful and relevant to the community as possible.

Source: www.cisa.gov/ais.

[65] See www.osce.org/files/f/documents/4/b/103500.pdf.

Tool 23
ICAO guiding principles on the sharing of threat information

ICAO has developed general guiding principles on the sharing of threat information between State and critical infrastructure operators. These stipulate that lines of communication, both formal and informal, between the aviation security officials of States should assist in the rapid exchange of information, including any raising of the threat level. The exchange of information on techniques used to try to breach security, experience with security equipment, and operational practices is also extremely advantageous. Formal procedures for exchanging information between identified responsible officials, including publication of a list of telephone numbers, street addresses, telex and facsimile numbers, as well as e-mail and aeronautical fixed service (known as "AFS") addresses, should be available for communications during a serious incident.

States should develop procedures for the analysis and dissemination of threat information and ensure that appropriate actions are taken by aircraft and airport operators to counter the identified threat. Information should be disseminated when individuals need it in order to carry out their duties effectively, in application of the "need-to-know" principle.

In conducting a risk assessment, Member States should obtain information about the threat, in particular on possible targets and modus operandi. Such information may come from a variety of sources, including the following:

- Actual incidents, including successful or unsuccessful attacks on aviation, which provide information on terrorist objectives and methodologies (ICAO member States may find relevant information on acts of unlawful interference and other security incidents in the ICAO Acts of Unlawful Interference Database)
- Closed sources, primarily counter-terrorist intelligence and assessments, which may be gathered or prepared by intelligence, law enforcement and other agencies of States
- Open sources, which may include publicly available information on unusual or suspicious occurrences, and the availability of items that could be used for terrorist purposes, and any other information that may contribute to the threat picture

More information with regard to sharing the information and security culture in aviation may be found in the ICAO Aviation Security Manual (Doc 8973-Restricted).

4.2.2 Information-sharing between CI operators

The delivery of most critical services to society is the outcome of complex supply chains requiring the input of different entities operating in multiple infrastructure sectors and industry segments. Supply-chain dependencies show the importance of having proper operator-to-operator channels for information flows across sectors.

The need to have in place adequate information-sharing arrangements also concerns different CI operators producing or delivering the same type of goods or services within the same sector. This is especially relevant for the purpose of exchanging good practices, information about risk assessment methodologies, advice about the usefulness of certain adopted mitigation measures, lessons learned following incidents, and other valuable materials. Well-experienced operators with long-standing practices in CI protection may usefully transmit their knowledge to others that are less familiar with applicable regulatory frameworks and CI compliance strategies. At the same time, it is important to remain cognizant of the intrinsic difficulty of ensuring smooth information flows between two or more privately operated CI entities that are market competitors. Although these entities may be wary of cooperating with each other, especially in the exchange of sensitive information, it is important for CIP strategies to address this issue with a view to limiting potential drawbacks.

CASE STUDY 31
Private-sector initiative for information-sharing across CI in the financial sector

The Financial Services Information Sharing and Analysis Center (referred to as "FS-ISAC") is a global cyber intelligence-sharing community exclusively focused on financial services. Serving financial institutions and, in turn, their customers, the organization leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network to anticipate, mitigate and respond to cyberthreats.

Headquartered in the United States, the organization has offices in the United Kingdom and Singapore and member financial institutions in approximately 70 countries. Its members represent $100 trillion in assets and 16,000 active users.

The Financial Services Information Sharing and Analysis Center maintains member confidentiality and privacy through the Traffic Light Protocol model (see section 4.3.2)

Source: www.fsisac.com/who-we-are.

4.2.3 Information-sharing between government agencies

The establishment of inter-agency information-sharing mechanisms (involving both national and local levels of government) is vital to the extent that public institutions are mandated to coordinate and implement CIP-related action both horizontally and vertically. An example of, so to speak, "horizontal" information-sharing is the situation when multiple ministries and agencies are responsible for specific sectors and need to cooperate to address issues of mutual concern, such as to assess the impact of dependencies across sectors, or to manage a crisis that affects multiple sectors simultaneously. Examples of vertical-type arrangements are those necessary to support the division of labour between municipal, regional and national authorities.

This dimension of information-sharing is part of a broader inter-agency coordination effort which is further examined in chapter 5.

CASE STUDY 32
Information-sharing at the city level: Counter Terrorism Preparedness Network

Currently funded by the city of Stockholm, the Counter Terrorism Preparedness Network is a prominent example of an international information-sharing platform connecting public entities at the city level. The mission of the Network is to bring together strategic leaders, practitioners and academics to inform local policies and practices that build resilience to keep our cities and communities safe from terrorism. This overall objective is being pursued with the setting of a number of specific goals:

- Develop and maintain relationships across partner cities in the Network.
- Provide a secure and constructive platform for cities to share their experiences.
- Exchange lessons, practices and materials that can strengthen city resilience to terrorism.
- Undertake research to influence and inform city-level activities, arrangements and policy.
- Support the implementation of recommendations and monitor their subsequent impact.
- Review Network reports as new strategic lessons, research or practices are identified.
- Collaborate through an ongoing exchange of expertise and engage with other relevant stakeholders to provide connectivity with parallel projects, initiatives and agendas.

The Counter Terrorism Preparedness Network is governed by an international board, facilitated by the London Resilience Group and hosted by the London Fire Commissioner.

Source: www.london.gov.uk/what-we-do/fire-and-resilience/counter-terrorism-preparedness-network-ctpn/who-we-are-and-what-we-do.

CASE STUDY 33
Securing the flow of information: United Kingdom High-Integrity Telecommunications System

Technology can significantly support agencies in keeping critical information flowing at times of emergency. In the United Kingdom, this objective is pursued by the High-Integrity Telecommunications System (HITS). Developed by the Government of the United Kingdom, HITS is an independent system that will continue to function when conventional landline and mobile telecoms are unavailable or degraded. Based on the military Skynet 5 satellite network, it is available to police and other emergency services personnel at fixed sites located across the United Kingdom, with further transportable units enabling HITS to be deployed wherever and whenever the need arises. Allowing both voice and data transmission, as well as access to the internet, HITS plays a critical role in enabling uninterrupted communication between regional and national levels of crisis coordination during any kind of disruptive event.

Source: www.gov.uk/guidance/resilient-communications.

4.3 Prerequisites for effective information-sharing

Experience shows that the effectiveness of information-sharing on CIP depends on two basic factors:

- The ability to create a common understanding of what type of information needs to be shared and why, thus fostering the conditions for trust among involved stakeholders.
- The provision of adequate levels of protection for sensitive information whose sharing is encouraged or mandated under CIP arrangements.

It is important for drafters of CIP strategies (and those called upon to implement them) to understand how these two factors interact with each other. While levels of trust will decline if information is not properly protected, stringent levels of information protection will not per se generate higher trust among participants.

4.3.1 Trust

Creating genuine trust among participants in a certain information-sharing arrangement can be a time-consuming effort and requires the active commitment of all involved stakeholders. To a significant extent, the establishment of adequate levels of trust is predicated on the shared awareness of each participating agency's added value. Once trust has been established, flows of information stand to gain significantly in both qualitative and quantitative terms.

Box 17
Success factors in CIP information-sharing

Based on a survey of CIP methodologies predominantly focusing on European countries, the European Union-funded project on recommended elements of critical infrastructure protection for policymakers in Europe (RECIPE) has compiled a list of the main success factors in information-sharing. Accordingly, as stated in the RECIPE guidelines, *Recommended Elements of Critical Infrastructure Protection for Policy Makers in Europe*:

"Experience has shown that trust is best built up in small sized face-to-face meetings.

"In general, there are some basic dos and don'ts. As a general rule, information-sharing is best initiated at a level that is not too detailed. It is not always necessary to share information that is too specific, for instance knowledge on critical objects and their location, or specific information on vulnerabilities or incidents. Several successful information exchanges stress that starting small will help to establish the required level of trust.

"For establishing trust, there should be continuity in the people attending the information exchange meetings. The participants should be appointed at a personal level with enough mandate and responsibility in their own environment. Generally, no substitutes are allowed.

"Information sharing meetings focus on the exchange of information: all organizations involved should (in principle) contribute information.

"The information provider shall ensure that the information provided is of the right level of content and background. Based upon the information, the recipients of the information should be able to take appropriate actions in their respective organizations or be alerted about the new threat. Above all, the information provider remains the owner of the shared information and its sensitivity classification.

"Most examples of successful information sharing are on a voluntary basis, built on trust.

"However, there are also some mandatory examples, in which information on risk assessments and incidents has to be shared, e.g. the reporting on large disturbances to public communications networks according to article 13a of the EU telecommunications package. In the mandated approach, it is often hard to guarantee quality of the exchanged information. Even mandated approaches therefore emphasize that a key to the success of their scheme is still to build trust and a spirit of voluntary cooperation" (p. 52);

and

"Experience shows that tools for electronic information exchange are best used as an additional tool for existing trusted information sharing communities. If no level of trust exists, then it is very hard to create a high level of trust in the electronic environment" (p. 58)

Source: www.researchgate.net/publication/261987293_RECIPE_Good_Practices_Manual_for_CIP_Policies.

4.3.2 Protecting sensitive information

Stakeholders called upon to cooperate on CIP matters often need to handle confidential information. As a result, CIP strategies need to foresee mechanisms to deal with information whose circulation is restricted on various grounds including, for instance, human rights law, national security and intellectual property rights. For example, most operators of privately-owned CI are likely to share data on incidents or vulnerability factors only if they receive appropriate assurances that the release of sensitive information will not have a negative effect on their businesses (for example, information will not provide competitors with a market edge, nor will it be used against them by public agencies for purposes other than CI protection). A major challenge thus lies in ensuring that as much information as possible is shared among the various stakeholders while protecting its confidential nature. This can be both sensitive business information held by companies, or classified information held by State agencies.

The creation of an environment of trust for information-sharing depends on the setting of clear legal and operational frameworks to protect the sensitive nature of shared data. In designing such frameworks, the overarching objective to facilitate the circulation of information for CIP purposes should always take into account the applicable human rights and data protection regimes. Under the European Union Charter of Fundamental Rights, for example, personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate

basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".[66]

Box 18
Sensitive CIP-related information in the European Union legal framework

European Union Council Directive 2008/114/EC on the "identification and designation of European critical infrastructure" provides the following definition of "sensitive critical infrastructure protection related information": "Facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations".[67]

The same Directive sets forth a "specialty principle" whereby "Member States, the Commission and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information submitted to Member States or to the Commission is not used for any purpose other than the protection of CI. ... This Article shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed".[68]

Not all CI-related information needs to be treated confidentially. In the same way, not all information regarded as "sensitive" deserves the same degree of protection. Limitations to the circulation of CI-related information can take various forms and be more or less stringent, depending on the specific circumstances and objectives of a certain type of information exchange. New Zealand, for example, has established the basic principle that incidents should be dealt with at the lowest possible classification level as a means of ensuring the early and effective dissemination of critical information to all responders in charge of reducing impact.[69]

Operationally, a number of approaches can be used to protect the circulation of sensitive information and these often complement one another. Typically, these approaches are centred around the following matters: security clearances and vetting procedures; colour-coding systems; and electronic tools, as further explored below.

4.3.2.1 Security clearances and vetting

Governments may provide security clearances for key stakeholders who need to access sensitive CI-related information. According to European Union Council Directive 2008/114/EC, "any person handling classified information pursuant to this Directive on behalf of a Member State or the Commission shall have an appropriate level of security vetting".[70]

Information-sharing platforms may also adopt specific selection criteria for the admission of new members based, for example, on the need for existing participants to approve the inclusion of new entities, background screening, interviews with the public bodies in charge of the platform, and other requirements.

In some cases, the private sector may find it challenging to involve members of the law enforcement community for fear that revealing certain types of information might trigger action on their part that would prejudice the willingness of participants to share information at all. It is important for CIP strategies to take account of these potential difficulties and find ways to overcome them.

66 Art. 8 (2).
67 Art. 2 (d).
68 Art. 9.
69 See https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf.
70 Art. 9.

4.3.2.2 Colour-coding systems

These systems are based on the principle that whoever supplies information determines the extent to which the information itself can circulate. The Traffic Light Protocol applies this concept in that the source of the information labels it with one of four colours:

Red: Restricted to named recipients only.

Amber: Limited circulation, with the originator expected to determine the limits and conditions of information-sharing.

Green: Information can be circulated within a certain community, but cannot be made publicly available (for example on the Internet) or released outside the community.

White: Unrestricted circulation.

One advantage of the Traffic Light Protocol is its user-friendliness and the clear boundaries that it sets between the responsibilities of the issuer and the recipient.

4.3.2.3 Electronic tools

In order to secure information-sharing, some platforms use electronic tools, such as extranets, to exchange documents. An extranet is a telecommunications network which uses Internet technology and whose objective is to facilitate exchanges between a main entity and two or more partners who are geographically distant. Partners must authenticate themselves to be allowed to view the network information.

CASE STUDY 34
National approaches on the protection of sensitive CI-related information: Australia, France, United States

Australia

Established by the Government of Australia in 2003, the Trusted Information Sharing Network is the country's primary engagement mechanism for business-government information-sharing and resilience building initiatives. The Network provides a secure environment in which CI owners and operators across seven sector groups meet regularly to share information and cooperate within and across sectors to address security and business continuity challenges. The sector groups within the Network include banking and finance, communications, energy, food and grocery, health, transport and water services. In addition, there are specialist forums (known as "cross-sectoral interest groups") which assist in the temporary exploration of cross-cutting issues, and a "resilience expert advisory group" which has a strong focus on organizational resilience. Coordination and strategic guidance for the Network is provided by the Critical Infrastructure Advisory Council, which is made up of the chairs of each of the Network's groups, senior Government representatives from relevant agencies, and senior state and territory government representatives.

France

The directives and plans adopted under the national system for the security of vital activities (known by its French abbreviation "SAIV") are classified at the "confidential defence" level. Whether they are the issuers or the recipients, CI operators ensure the destruction of classified documents that they no longer need, especially when:

- A classified document is revised or repealed.
- A "vital point" is cancelled.
- A "vital zone" is cancelled.
- An operator loses its status as "vital operator".

"Vital operators" may not wish to reveal some very sensitive information related to risk and crisis management. In that case, they must invoke specific procedures. The competent administrative authorities overseeing the operators' security plans may discuss the issue with the operators if necessary for the performance of their role. Such authorities may take cognizance of the information that the operators wish to withhold, without necessarily using it as they wish.

United States

The Homeland Security Information Network is the official system employed by the Department of Homeland Security for the trusted sharing of sensitive but unclassified information between federal, state, local, territorial, tribal, international and private sector partners. Operators use the Network to obtain homeland security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information that they need to perform their missions.

Within the Network, a platform known as "HSIN-CI" is the primary system through which private sector owners and operators, the Department of Homeland Security, and other federal, state and local government agencies collaborate to protect the country's critical infrastructure. HSIN-CI provides real-time collaboration tools, including a virtual meeting space, document sharing, alerts and instant messaging at no charge.

Through HSIN-CI, users are able to:

- Receive, submit, and discuss timely, actionable, and accurate information.
- Maintain a direct, trusted channel with Department of Homeland Security and other vetted sector stakeholders.
- Communicate information pertaining to threats, vulnerabilities, security, and response and recovery activities affecting sector and cross-sector operations.

Sources: www.cisc.gov.au/engagement/trusted-information-sharing-network; www.legifrance.gouv.fr/download/pdf/circ?id=37828; and www.dhs.gov/hsin-critical-infrastructure.

CASE STUDY 35
Critical Infrastructure Information Gateway (CI Gateway): Canada

One of the objectives pursued under the National Strategy and Action Plan for Critical Infrastructure is the timely advancement of information-sharing and protection among CI partners. To achieve this, the Strategy calls for the development of a CI gateway, a web-based critical infrastructure information-sharing portal to be hosted on the Public Safety Canada domain.

The 2014–2017 Action Plan for Critical Infrastructure recognized that several information-sharing arrangements had been developed under the original Action Plan and built on these achievements by further expanding information-sharing opportunities through various means, including formal agreements, virtual and physical mechanisms, and the creation and dissemination of information products.

According to the 2014–2017 Action Plan, key objectives in this area included:

- Expanding stakeholder membership and participation in the Canadian Critical Infrastructure Gateway and leveraging the CI Gateway's capabilities to improve information-sharing and collaboration on specific projects: Public Safety Canada is committed to building on the successful launch of the CI Gateway by ensuring that its membership spans the ten sectors and other key stakeholders, encouraging active membership participation, and promoting its use by sector networks and communities of practice to share information and best practices, and to work together on specific projects.
- Sponsoring security clearances among private sector stakeholders in order to enable increased sharing of sensitive information: Some of the information gathered by the Canadian security and intelligence community is sensitive and can only be shared with individuals with an appropriate security clearance. Public Safety Canada is committed to working with lead federal departments and agencies to increase the number of security cleared stakeholders in the private sector.

In line with previous action plans, the 2021–2023 Action Plan engaged stakeholders to "continue efforts to modernize the CI Gateway to meet the changing needs of the critical infrastructure community, and promote the use of the CI Gateway to increase the number of users and site visits ».

Sources: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx and www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx.

Tool 24
Protection of sensitive aviation security information – ICAO

ICAO has developed general guiding principles on the protection of aviation-related security information. This should be restricted to those persons who require such information in the performance of their duties and are therefore authorized to have access to and use such information (this is known as the "need-to-know" principle). Protective measures should be applied to sensitive aviation security information and the degree of protection should be specified by either the State or relevant entities, taking into consideration the national requirements for the protection of sensitive information established by the relevant authorities. Protective measures should be applied to identity, handle, share or dispose of sensitive aviation security information.

States should establish written policies, procedures and guidance in respect of identifying, handling, sharing (by oral, physical and electronic means) and disposing of sensitive aviation security information to avoid any unauthorized disclosure. Such policies, procedures and guidance should also address unauthorized disclosure by using a protective marking.

When handling sensitive aviation security information, States or relevant entities should protect such information from unauthorized access or disclosure. States or relevant entities should consider that access to sensitive aviation security information be limited to those who have a need to know; authorized personnel should only have access to and use sensitive aviation security information as required for the performance of their duties; sensitive aviation security information should not be replicated unnecessarily; sensitive aviation security information should be properly stored in a secure manner, such as a locked filing cabinet or drawer, when not in use; and electronic files containing sensitive aviation security information should be stored in a secure manner, such as encryption, password protection and secure servers. Such electronic files, if stored on a secure portable electronic device, should be locked in a filing cabinet or locked drawer when not in use.

When sharing sensitive aviation security information, States or relevant entities should protect such information from unauthorized access or disclosure by application of protective measures when transmitting sensitive aviation security information, such as providing the recipient with the appropriate handling instructions, using authorized delivery methods, such as authorized couriers and secure packaging methods. The electronic files containing sensitive aviation security information should be transmitted using encryption or password protection. If using a password, it should be sufficiently strong and transmitted separately from the original electronic file. Prior arrangements should be made with the recipient for the transport method, as well as confirmation of receipt, together with establishment of a non-disclosure agreement before providing sensitive aviation security information. Oral discussions (by telephone, videoconferencing or in person) about sensitive aviation security information should only be held with persons with the need to know and in settings where such discussions cannot be overheard by those who are unauthorized to do so.

States or relevant entities should also establish national record retention laws or policies to ensure that sensitive aviation security information is not retained longer than necessary. When disposing of sensitive aviation security information, States or relevant entities should destroy the material in a manner that ensures that such information is not retrievable and cannot be reconstructed to prevent unauthorized access or disclosure. States or relevant entities should ensure that any third party with whom sensitive aviation security information is shared follows the same disposal methods.

Whenever information needs to be exchanged between States, the information requirement should be established by written sharing agreements or arrangements. Such arrangements should include provisions in respect of identifying, handling, sharing and disclosing of sensitive security information with other States. These latter should clearly identify information as sensitive aviation security information and communicate any specific requirements for protective measures to be applied prior to sharing such information with other States. When receiving sensitive aviation security information, States should apply the required protective measures to prevented unauthorized use or disclosure.

Source: ICAO Aviation Security Manual, Doc 8973-Restricted.

5. Ensuring inter-agency coordination

Security Council resolution 2341 (2017)

The Security Council,

...

6. *Urges* all States to ensure that all their relevant domestic departments, agencies and other entities work closely and effectively together on matters of protection of critical infrastructure against terrorist attacks

5.1 Need for and challenges of a multi-agency approach to CIP

There is a plethora of norms, rules and standards on safety and security issues in different CI sectors set by various government agencies. Terrorism-related intelligence, which is needed to evaluate current types and levels of threat to CI, is often collected by multiple agencies answerable to different ministries. Crisis management and recovery efforts are complex processes in which several public entities (at the local, municipal, regional and national levels) intervene (first-responders, law enforcement, and others). In addition, in many cases a number of entities may be involved in a given security function within the same critical sector. Such is the case of the aviation sector, where the competent authority, airport management and law enforcement bodies may share responsibility for the protection of airports, air navigation aids and services.

Broad interagency coordination is a key prerequisite for the implementation of adequate levels of CIP. Cross-sectoral national strategies need to connect the dots, so to speak, among a variety of domestic agencies with responsibilities for CIP-relevant action. Coordination should be achieved among stakeholders such as ministries (such as those of communications, economic affairs, security, justice, the interior, defence and the Cabinet Office), regional bodies and regulators collaborating at the strategic, tactical and operational levels. Achieving this overarching objective, however, is not always straightforward. The use of different terminology and jargon by the various entities involved in prevention, response and recovery action, along with the lack of unified procedures and communication channels, has the potential to affect the quality of the overall CIP effort. Added to which, "in some cases public authorities tend to follow diverging agendas when it comes to CIP. Some of them adhere to the power of market forces, whereas others are strong believers in the government's legislative role. These differences, however, can become serious stumbling blocks for cooperation when engaging with the private sector."[71]

[71] OSCE, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, Vienna, 2013. Available at www.osce.org/atu/103500?download=true.

CASE STUDY 36
Federal-Provincial-Territorial Critical Infrastructure Working Group: Canada

Alongside the country's sectoral networks and cross-sectoral forum, a Federal-Provincial-Territorial Critical Infrastructure Working Group has been created under the Canadian National Strategy and Action Plan. This body offers an example of vertical coordination among authorities in a federal system of Government. Its stated objectives are to:

- Support the implementation of the Strategy within federal, provincial and territorial jurisdictions
- Provide guidance and participate in the evolution and implementation of the Action Plan
- Act as a clearing-house for governments on critical infrastructure-related issues to the federal, provincial and territorial senior officials responsible for emergency management
- Facilitate federal, provincial and territorial networking to support critical infrastructure information-sharing, risk management, critical infrastructure planning and exercises
- Identify critical infrastructure issues of regional or jurisdictional concern
- Advance a common understanding of critical infrastructure risks and interdependencies
- Encourage participation in exercises to test sector-specific work plans and identify new risks
- Provide guidance on current and future challenges related to critical infrastructure
- Identify linkages among federal, provincial and territorial programs and initiatives and facilitate sharing of information and best practices

Membership in the Working Group is open to all governments in accordance with their needs and as their resources permit. Decisions are only taken following the sharing of information and an opportunity given to all members to comment. The Working Group is co-chaired by a representative from the Emergency Management and National Security Branch of Public Safety Canada and a provincial or territorial representative determined by group consensus.

The 2021–2023 Action Plan has reiterated the commitment by the Government of Canada to continue collaborating with the Federal-Provincial-Territorial Critical Infrastructure Working Group and engaging on current and emerging issues facing critical infrastructure sectors.

Sources: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr/index-en.aspx and www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx.

5.2 Agency coordination in crisis scenarios

An important aspect of inter-agency coordination is the ability of all stakeholders to promptly and effectively act in crisis situations. Once the basic crisis management structures and processes have been identified, CIP strategies need to ensure that these will work smoothly in case of need. Some basic prerequisites for achieving fluid and rapid decision-making are the following:

- Clear attribution of roles and responsibilities, with the proviso that decisions should be taken at the lowest appropriate level and that coordination is available at the highest necessary level. Arguably, "tight integration of CI operators into crisis management requires fulfilment of a large set of requirements. Mutual understanding of roles, responsibilities, capabilities and abilities is a lengthy process that requires investment in terms of time, human cooperation, learning each other's slang".[72]
- Full understanding of the consequences of CI disruption, including its cascading effects. It has been noted that "the current crisis management emphasis in most nations is much more focused on a single disruption of CI and its potential consequences, e.g. planning for disruption of drinking water supply, than it is on cascading failure and to

[72] Good Practices Manual for CIP policies for policy-makers in Europe, RECIPE, 2011. Available at www.researchgate.net/publication/261987293_RECIPE_Good_Practices_Manual_for_CIP_Policies.

common mode failure, such as a major storm disrupting multiple CI at the same time. The recommendation is to prepare for common mode failures and cascading failure effects affecting multiple CI at the same time".[73]

- Appointment of focal points in all involved agencies with 24/7 availability.
- Setting up of adequate information management systems to support effective data collection, analysis and circulation in support of single and multi-agency decision-making, and also the provision of information to the public. Communication arrangements should be designed to minimize situations where conflicting instructions are received. Ideally, also, information management systems are backed up by secure communication lines.

CASE STUDY 37
Crisis management following the 2005 London terrorist bombing

On 7 July 2005, as a result of four bombs being detonated on London's transport system, 52 members of the public were killed. The circumstances of the accident made the coordination of the emergency response particularly challenging. As highlighted by the Coroner's report following the inquest into the events, "the location of the three explosions in the tunnels meant that there were limited eye witnesses as to what had occurred. Second, communications in the tunnels were limited. Third, the widespread disruption caused by the explosions resulted in an avalanche of incoming calls overwhelming radio operators and causing congestion on all radio and telephone communications. It took time to identify and extract the most significant and important information from the plethora of reports which were received (in addition to the usual daily demands upon the emergency services and London Underground), so that the agencies could respond appropriately".

The Coroner found a number of weaknesses in the emergency response and made several recommendations. In particular, "the evidence revealed not merely failings in the communications systems then in place, but some basic misunderstandings between the emergency services as to their respective roles and operations, for example, failure by some emergency personnel to appreciate and understand the obligation on the part of the first LAS [London Ambulance Service] staff in attendance to act as ambulance incident officers as opposed to becoming involved in the treatment of casualties … Individual emergency responders encountered delay and difficulties in trying to ascertain what the nature of the incidents were, or what resources were required, and there were significant differences in the way in which each emergency responder endeavoured to address common issues, such as the use of radios where there was a possible risk of detonating secondary devices … The evidence demonstrates, therefore, a need for a review of the extent and scope of inter-agency training. Such training is vital in helping to reduce confusion and in fostering a better understanding of the emergency services' respective roles".

The Coroner's report observed that, while training (either in the form of so-called "table-top" or "real-life" exercises) was already been extensively provided to senior management levels, "the evidence also indicated that there was considerably less inter-agency training available for those 'frontline' members of the emergency services tasked with responding to the initial chaos, carnage and confusion of a major incident".

- Other recommendations covered:
- Inter-agency major incident training for frontline staff;
- Protocols for sharing emergency alert information between Transport for London and the emergency services
- Establishment and manning of rendezvous points
- Procedures for confirming and communicating information that traction current is switched off on the London Underground
- Provision of first aid equipment and stretchers on underground trains and stations
- Procedures for multi-casualty triage
- Emergency care of the type provided by the London Air Ambulance and Medical Emergency Response Incident Teams

In the report, the Coroner also referred to issues such as the regulation of the supply of hydrogen peroxide; effective inter-agency liaison; good communications and information-sharing; Airwave base radio stations and their capacity in the event of a major incident; and transparency between different emergency responders.

Source: http://image.guardian.co.uk/sys-files/Guardian/documents/2011/05/06/rule43-report.pdf.

[73] Ibid.

CASE STUDY 38
National Guide for the Notification and Management of Cyber Incidents, 2019: Spain

The Government of Spain assigns to different public institutions competence for cybersecurity issues related to knowledge of, management of and reaction to cybersecurity incidents affecting the various information and communication networks of the country. Public sector agencies, citizens, companies, critical infrastructure operators, and academic and research networks have at their disposal a series of reference bodies on which the Government's response capacity to cybersecurity incidents is based:

- CCN-CERT: Information Security Incident Response Capability of the National Cryptologic Centre, which has general competence over the public sector and systems that handle classified information.
- INCIBE-CERT: belonging to the National Institute of Cybersecurity, which has competence over the general public and the private sector. INCIBE-CERT also provides incident response services to institutions affiliated to the Spanish academic and research network, in coordination with CCN-CERT regarding public bodies.
- CNPIC: National Centre for Infrastructure Protection and Cybersecurity, which has competence over critical infrastructure and critical operators.
- ESP-DEF-CERT: belonging to the Joint Command of Cyber Defence, which has competence over the networks and information and telecommunications systems of the Armed Forces, and also other networks and systems specifically entrusted to it that affect national defence.

The National Guide is the official reference for cybercrime notification (whether mandatory or optional communication), and for requests for response to cybersecurity incidents. The document is a vade mecum allowing any entity – public or private – and also individual citizens to find precise guidance on to whom and how to report a cybersecurity incident. The Guide complies with the Spanish and European Union regulatory frameworks and with guidance issued by relevant international organizations that seek to harmonize the capacity to respond to cybersecurity incidents.

Source: https://cybilportal.org/wp-content/uploads/2020/04/SPAIN-CYBERINCIDENTS-NATIONAL-GUIDE.pdf.

5.3 Joint exercises and training activities

Addendum to the Madrid Guiding Principles

Guiding principle 51

In their further efforts to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider:

...

(a) Updating contingency planning, such as guidance, exercises and training for law enforcement and other relevant ministries, and industry to keep pace with actual threats, to refine strategies and ensure that stakeholders adapt to evolving threats

In the context of CIP, inter-agency exercises and training activities are universally recognized as essential tools to promote and consolidate inter-agency coordination. In practice, different forms of exercises need to be implemented, depending on the objectives sought, the number of entities and participants involved, resource availability, and other factors. In most cases, the objectives pursued are to:

- Achieve a common understanding of applicable processes and methodologies.
- Clarify reciprocal roles and responsibility in CI protection cycles.
- Create personnel confidence in executing CI-related protection instructions and policies (essential during the stressful phases of a real crisis).
- Identify weaknesses and introduce any modifications necessary for the safe conclusion of an actual emergency situation.
- Ensure the operational reliability and compatibility of all communication equipment designated for use during a crisis.

Box 19
Training, exercises and drills under the International Ship and Port Facility Security Code

In force since 2004, the International Ship and Port Facility Security Code (ISPS Code) is an amendment to the Safety of Life at Sea (SOLAS) Convention. Its objective is to enhance the detection and mitigation of security threats faced by ships engaged in international voyages and the port facilities serving such ships. The Code binds contracting governments and the shipping industry in a structured partnership based on the development of a strong security-based culture and risk-assessment methodology.

On this basis, the Code provides for mandatory training and exercises as part of the measures envisaged to step up stakeholders' understanding of their respective security-related duties and responsibilities (sections 13 and 18 of the Code). Drills, in particular, need to be envisaged at appropriate intervals. With regard to ship security, drills shall take into account "the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances" (section 13.3.) Concerning port facility security, drills shall take into account "the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances" (section 18.3).

CASE STUDY 39
Cyber Europe

Managed by the European Union Agency for Cybersecurity (ENISA), Cyber Europe is a series of cyber incident and crisis management exercises for both the public and private sectors from the European Union and EFTA Member States. The exercises are simulations of large-scale cybersecurity incidents escalating to become fully-fledged cybercrises. They offer IT security, business continuity and crisis management teams the opportunity to analyse advanced technical cybersecurity incidents and to deal with complex business continuity and crisis management situations.

Cyber Europe exercises started in 2010 and have taken place every two years. The last exercise in the series, Cyber Europe 2018, involved more than 1,000 participants from across Europe. The next exercise took place in the summer of 2022 and developed a scenario revolving around health care, with the participation of national and government computer security incident response teams, cybersecurity authorities, ministries of health, health-care organizations (such as hospitals and clinics), e-health service providers and health insurance providers.

The 2022 scenario is expected to feature real-life inspired technical incidents building up into a major crisis at all levels: local, organizational, national, and European. Business continuity plans and crisis management procedures will be put to the test. The exercise will be organized for IT-security, business continuity and crisis management teams from the European Union and EFTA member States.

Source: www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022.

CASE STUDY 40
Compilation of exercises by the Institute for Strategic Studies: Ukraine

The Ukrainian Institute for Strategic Studies has compiled an inventory of the most common types of exercises and their main uses:

- Seminars: to provide general guidance on existing strategies, plans, policies, procedures, protocols, resources and concepts.
- Table-top exercises: to generate discussion of a hypothetical, simulated emergency. Table-top exercises are useful in facilitating conceptual understanding, identifying strengths and areas for improvement and achieving changes in perceptions.
- Simulations (games): to explore the consequences of player decisions and actions. This type of exercise is often based on the creation of a competitive environment where two or more teams face each other in real-life situations.
- Drill exercises: to provide training on new equipment, validate procedures or practice and maintain current abilities. Drill exercises are based on the notion of teaching and perfecting skills through task repetition.
- Full-scale (live): to confront participants with scenarios intended to mirror real situations, requiring them to act and react in real time.

As some of the above-mentioned exercises involve a large number of participants and are based on complex live simulations, they require careful planning and often months, if not years, of preparation.

Source: https://niss.gov.ua/en/publikacii/analitichni-dopovidi/state-critical-infrastructure-protection-system-national-security.

Tool 25
Cybersecurity training and exercises: CISA initiatives (United States)

CISA relies on two major resources to upgrade stakeholders' skills in protecting CI cybersecurity:

- Cybersecurity Workforce Training Guide

www.cisa.gov/publication/cybersecurity-workforce-training-guide

Released in 2021, the Guide is addressed to current and future federal, state, local, tribal and territorial staff. It helps them develop a training plan based on their current skill level and desired career opportunities.

- CISA tabletop exercise packages (referred to as "CTEPs")

www.cisa.gov/cisa-tabletop-exercises-packages

This is a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios. Each package is customizable and includes template exercise objectives, scenarios, and discussion questions, along with a collection of references and resources. Available scenarios cover a broad array of physical security and cybersecurity topics, including industrial control systems, vehicle ramming, insider threats, active assailants, and unmanned aerial systems. CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response and post-incident recovery.

5.4 Promoting interoperable processes and solutions

Addendum to the Madrid Guiding Principles

Guiding principle 50

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

...

(e) Promote better interoperability in security and crisis management

A key concept for inter-agency coordination is "interoperability". In the context of inter-agency coordination, the possibility to rely on interoperable processes acquires special importance for emergency response communication. In this regard, it has been observed that

the issue ... has been a concern for almost as long as radios have been used by first responders and other public safety officials. However, it was not until the 9/11 World Trade Center terrorist attack that interoperability was elevated from a long-standing concern to a critical national priority.

One of the greatest tragedies of the September 11th disaster occurred due to the inability to effectively relay warnings to fire rescue personnel that the towers were about to collapse, and that they needed to evacuate immediately. Many experts concur that this failure of the fire department's radio system to communicate effectively with other agencies, or even between newer and older radio models, was primarily responsible for the deaths of 343 firefighters.[74]

The use of interoperable systems is key not only to allowing police and other responders (police, fire and rescue, ambulance services) to communicate with one another to coordinate action, but also to enable them to streamline resources in budgeting and planning for disaster relief and recovery efforts.

[74] The basis of interoperability for emergency communications, Federal Signal, 2013. Available at www.fedsig.com/sites/default/files/news/pdf/The%20bais%20of%20Interoperability%20for%20Emergency%20Communications.pdf.

Box 20
Interoperability under the Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy: Canada

The Canadian Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy defines interoperability as being of an operational/functional or technical nature.

"(1) Operational / functional interoperability is the ability to work together effectively. Specifically, it is the ability of different jurisdictions or disciplines to provide services to and accept services from other jurisdictions or disciplines in a coordinated manner, and to use those services to operate more effectively together at an emergency. From a practical perspective, operational interoperability means that personnel from different jurisdictions or services perform as a team under a common command-and-control structure.

"(2) Technical interoperability is the ability to communicate and exchange information and to integrate equipment and technical capabilities. It is the ability of systems to provide dynamic interactive information and data exchange among command, control, and communications elements for planning, coordinating, integrating, and executing response operations."

Source: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg/rslnc-strtg-eng.pdf.

5.5 Overcoming cultural barriers

While the adoption of interoperable solutions and streamlined, integrated processes can go a long way towards breaking silos and promoting inter-agency coordination, the fact remains that CI protection relies on the day-to-day operation of people with the most diverse technical and professional backgrounds. Different mindsets may be rooted in different terminologies, methodological approaches and ways of organizing work.

The private-public sector divide offers a typical scenario where different perceptions are at play in term of where the balance should lie between security expenditures (for example, to improve the resilience of CI) and the implementation of business-friendly cost-saving measures. in addition, the effect of cultural barriers and uneven perceptions can also be observed in those working for different branches of the same government.

Member States' experiences and perceptions may vary significantly depending on the specific institutional, social and economic structures in which the various professions involved operate. Without necessarily aiming to render uniform deeply rooted styles of behaviour, each Member State may wish to develop awareness of these issues and find ways (for example, by openly and regularly discussing these in joint training activities) to ensure that these do not eventually stand in the way of ongoing efforts to achieve CI resilience.

CASE STUDY 41
Study on cultural gaps among CIP stakeholders: Sweden

The extent to which cultural gaps among CI stakeholders may stand in the way of achieving optimal levels of collaboration has been examined with particular attention in Sweden in the framework of the country's whole-of-society approach to CI resilience and, at a more general level, social security. Accordingly, a study devoted to disaster resilience has isolated a number of professional relationships involved in CI protection and analysed the specific cultural challenges attached to each of them. The study stresses, for example, gaps between safety and security professionals in the way that these two groups manage information. While security officials are accustomed to handling classified information within restricted circles of people, safety personnel tend to rely on open sources and not to see the role of confidential information. That said, however, "with threats becoming more complex, where an event at first can be difficult to define as an apparent "normal" accident or as a terrorist attack, robust cooperation between, for example, police forces and emergency responders needs to be developed well in advance" (Lindberg and Sundelius 2013, p. 1301).

While certain behavioural gaps may be found along the civilian-military divide, the study identifies more pronounced obstacles to civil-civil coordination, the main reason being that "roles and responsibilities in the complex civilian sphere are often less clear cut and sometimes even overlapping. As threats evolve, rules and routines may be missing or outdated. Jurisdictional lines can be viewed as complimentary or as competing. Some resistance to being coordinated can be detected, and one reason is probably that interactions for the purpose of modifying behaviours can be highly sensitive among proud professionals".

Source: www.semanticscholar.org/paper/Whole-of-Society-Disaster-Resilience-%3A-The-Swedish-Lindberg-Sundelius/9524aa4182828716ba5834c40ee6128f8674f54f.

6. Enhancing international cooperation for CIP

Security Council resolution 2341 (2017)

The Security Council,

...

8. Affirms that regional and bilateral economic cooperation and development initiatives play a vital role in achieving stability and prosperity, and in this regard calls upon all States to enhance their cooperation to protect critical infrastructure, including regional connectivity projects and related cross-border infrastructure, from terrorist attacks, as appropriate, through bilateral and multilateral means in information-sharing, risk assessment and joint law enforcement;

9. Urges States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, technical assistance, technology transfers and programmes, where it is needed to enable all States to achieve the goal of protection of critical infrastructure against terrorist attacks

6.1 Dimensions of international cooperation on CIP

One of the most distinctive trends in today's global landscape is the internationalization of supply chains, whether for the delivery of critical or non-critical products and services. CI interdependencies and interconnectedness run across borders. Risks to Member States' CI may equally originate in neighbouring countries (especially in the case of shared physical infrastructure) or very distant countries (notably in the case of cyber-related infrastructure). In the event of an attack on critical information infrastructure (CII), a crisis unfolding in one country may have been planned and piloted in the territory of another country.

Potential scenarios illustrating the need to place international cooperation firmly within Member States' CIP strategies include the following:

- Two or more Member States share the same infrastructure (cross-border CI).
- One Member State depends, wholly or partly, on products, services, technologies and other items delivered by CI located in another Member State.

Current forms and levels of international cooperation on CIP vary substantially across countries. They may be more or less extensive in scope and articulated depending on the specific type of arrangements in place, the countries' degree of economic integration with others, and other factors. In considering plans for new or reinforced international partnerships on CIP, Member States should be focusing on multiple thematic areas. In most cases when international cooperation efforts on CIP are in place, they revolve around issues of information-sharing, crisis management and joint exercises.

An important dimension of CIP-related exchanges is international cooperation for criminal justice purposes. As Security Council resolution 2341 (2017) requires the establishment of criminal responsibility for attacks against CI, bringing the alleged perpetrators to justice often depends on Member States' activation and use of effective channels for international cooperation in the criminal justice field.

Box 21
INTERPOL global platform for law enforcement communication

The INTERPOL global, round-the-clock platform I-24/7 connects law enforcement officers in all 195 INTERPOL member countries and enables authorized users to share, in a secure environment, sensitive and urgent police information with their counterparts around the globe, 24 hours a day, 365 days a year. I-24/7 is the network that provides access to the various criminal databases maintained by INTERPOL. Authorized users can search and cross-check data in a matter of seconds, with direct access to databases on such subjects as suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art.

At the national level, I-24/7 is made directly accessible to national central bureaux and, subject to authorization from these bureaux, to a large number of national institutions. In this regard, a growing number of the Organization's members have chosen to extend access to the exclusive communications network I-24/7 to national law enforcement bodies at strategic locations, such as border crossings, airports, and customs and immigration posts. Coupled with other INTERPOL tools that facilitate access to databases, such expansion gives frontline officers direct access to the Organization's police databases, within which they may freely consult and sometimes also record data.

CASE STUDY 42
International sharing of threat information in the civil aviation field

In the aviation sector, an important dimension of information-sharing consists of the exchange of threat information.

The ICAO Aviation Security Manual (Doc 8973-Restricted) recommends the establishment of lines of communication, both formal and informal, between the aviation security officials of States to assist in the rapid exchange of information, including any increase in the threat level. The exchange of information on techniques used to try to breach security, experience with security equipment, and operational practices are also extremely advantageous.

Formal procedures for exchanging information between identified responsible officials, including publication of a list of telephone numbers, street addresses, telex and facsimile numbers, and also email and aeronautical fixed service addresses, should be available for communications during a serious incident. States should develop procedures for the analysis and dissemination of threat information and ensure that appropriate actions are taken by aircraft and airport operators to counter the identified threat. Information should be disseminated when individuals need it in order to carry out their duties effectively, in other words, in application of the need-to-know principle.

States with limited resources for dealing with imminent threats or acts of unlawful interference should consider negotiating legal and procedural assistance with adjacent States that are better equipped to collect and disseminate threat and incident information.

Requests by a State for special security measures for a specific flight should be accommodated whenever necessary. To ensure that such requests receive appropriate attention, States should identify the procedures and the government, aircraft and airport operator representatives who should be aware of the threat information. In addition, the parameters of special security measures, responsibility for additional costs and the time frame for the initiation of action should be negotiated with the concerned aircraft operator and airports.

Urgent communications may be facilitated through use of the ICAO Aviation Security Point of Contact Network, established for the communication of imminent threats to civil air transport operations, pursuant to the views expressed by the Group of Eight Lyon-Roma Anti-Crime and Terrorism Group. Pursuant to Assembly resolution A39-18: "Consolidated statement of continuing ICAO policies related to aviation security", States which have not done so are urged to participate in the ICAO Aviation Security Point of Contact Network. The objective of the Network is to provide details of international aviation security contacts within each State, which are designated as the appropriate authority to send and receive communications, at any time of the day or night, concerning imminent threat information, security requests of an urgent nature, and guidelines to support security requirements, in order to counter an imminent threat. Points of contact should be available at all times, engaged in the threat assessment process and close to the decision-making process for aviation security procedures.

Source: ICAO, Aviation Security Manual, Doc 8973-Restricted.

6.2 Major cross-border initiatives

Over the past few years, increased awareness of CI interdependencies and their cross-border implications has triggered the adoption of a number of international agreements and partnerships. In view of the economic weight of the countries involved and the presence of the highly complex infrastructure networks that they share, this section examines the framework linking European Union Member States and the United States-Canada cooperation arrangements in the field. It also considers recent experiences and initiatives implemented by the Nordic countries.

6.2.1 European Union

The current European Union-wide approach to CIP is enshrined in a 2008 Directive, which introduces the notion of "European critical infrastructure" (referred to in the Union as "ECI") as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States."[75] The scope of application of the 2008 Directive is limited to the energy and transport sectors. Moreover, it is designed complement, as opposed to replace, existing sectoral measures adopted at the European Union level or by individual member States.

The designation process for European critical infrastructure comprises various steps requiring European Union member States to:

- Inform other member States about potential European critical infrastructure located on their territory and affecting them, and engage them in bilateral or multilateral discussions.
- Designate such infrastructure as European critical infrastructure following agreement with the member States involved.
- On an annual basis, inform the European Commission about the number of designated European critical infrastructure facilities per sector and the number of member States dependent on each designated European critical infrastructure facility.
- Inform concerned owners and operators that their infrastructure has been designated as European critical infrastructure.
- Ensure that designated European critical infrastructure facilities possess an operator security plan and that this plan is regularly reviewed.
- Ensure that each European critical infrastructure facility designates a security liaison officer to act as a focal point between the European critical infrastructure and the relevant national authority.
- Conduct a threat assessment in relation to European critical infrastructure subsectors within one year of the designation of critical infrastructure on its territory as European critical infrastructure within those subsectors.
- Report summary data every two years to the European Commission on the types of risks, threats and vulnerabilities encountered for each European critical infrastructure facilities sector within which such infrastructure has been designated.
- Appoint a "European critical infrastructure protection contact point" to coordinate European critical infrastructure protection issues domestically, in relation to other member States and the European Commission.

In 2013, an evaluation of the status of implementation of the 2008 Directive revealed a mixed scenario. While member States clearly continued to see the importance of having a CIP-related, European Union-wide framework in place, a number of challenges were highlighted. In particular, it was pointed out that "less than 20 European CI [had been designated] and

[75] Council Directive 2008/114 of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG.

consequently very few new operator security plans [had] been produced. Some clear CI of European dimension, such as main energy transmission networks, [were] not included. Despite having helped foster European cooperation in the CIP process, the Directive [had] mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation. The sector-focused approach of the Directive likewise represents a challenge to a number of Member States, as in practice the analysis of criticalities is not confined to sectoral boundaries and follows rather a 'system' or 'service' approach (e.g. hospitals, financial services)".76

Based on the outcome of its assessment, in 2013 the European Commission began a process of reorientation of the European Union-wide CIP action by exploring a new, more practical approach that would substantially move from a sector-specific to a systemic model. The need for change was further evidenced by an evaluation of the 2008 Directive – conducted in 2019–which highlighted how existing European and national measures face limitations in helping operators to confront the operational challenges that they currently face and the vulnerabilities that their interdependent nature entail.[77]

In 2020, the new approach was crystallized in a European Union Commission proposal for a directive on the resilience of critical entities.[78] The proposal reiterates the need for a fundamental switch from protecting specific assets towards reinforcing the resilience of the critical entities that operate them. In so doing, it reflects the "resilient operator" concept enshrined in the 2020 European Union Agenda on Counter Terrorism.[79]

Box 22
From critical assets protection to system resilience: new paradigm of the European Union Commission

The 2020 European Union Commission proposal for a new directive on the resilience of critical entities reflects the priorities of the Commission's European Union Security Union Strategy. This latter calls for a revised approach to critical infrastructure resilience that better suits the current and anticipated future risk landscape, the ever-close interdependencies both between critical sectors and between physical and digital infrastructure.

The proposed instrument is designed to replace Directive 2008/114, on European critical infrastructure, which only applies to the energy and transport sectors, focuses solely on protective measures and provides a procedure for identifying and designating European critical infrastructure through cross-border dialogue. Departing from the current approach, the proposed directive:

- Has a wider scope of application, as it covers ten critical sectors, namely energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration and space.
- Establishes a procedure for member States to identify critical entities by using common criteria on the basis of a national risk assessment.
- Sets out specific obligations for member States and the identified critical entities, including those with particular European significance, namely, critical entities that provide essential services to or in more than one third of member States that would be subject to specific oversight.

The Commission also envisages supporting both competent authorities and critical entities in their efforts to comply with their obligations under the directive. Moreover, the Critical Entities Resilience Group – a Commission expert group – is expected to provide advice to the Commission and promote strategic cooperation and the exchange of information. Lastly, the proposed directive provides for the possibility of cooperating with partner countries, for example in the area of risk assessments.

Source: https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

76 Working Document on a New Approach to the European Programme for Critical Infrastructure Protection, European Commission, 2013. Available at https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf.

77 See https://ec.europa.eu/home-affairs/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf.

78 See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0829&from=EN. In December 2021, the Council approved a general approach on the new draft directive.

79 See https://ec.europa.eu/home-affairs/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf.

CASE STUDY 43
AIRPOL and RAILPOL

Cross-border collaboration on the protection of CI within European countries is not limited to the framework set by the 2008 Directive. It also takes place in forums that, albeit not specifically devoted to CI protection, are instrumental towards this goal. The transport sector, through the activities implemented by AIRPOL and RAILPOL, offers two relevant examples.

Created in 2011, the aviation network known as "AIRPOL" is a coordinating body of law enforcement units at European airports. Its mission is to enhance the overall security in the civil aviation domain by:

- Optimizing the effectiveness and efficiency of airport and aviation related law-enforcement and border guard issues.
- Contributing to a more harmonized approach of enforcement in this domain.

AIRPOL works around three deliverables:

- Elaboration of a permanent and functional network, focused on the sharing of best practices, intelligence, general information and the exchange of staff in the future in several areas.
- Coordination of high impact cross-border actions.

Establishment of an advisory role as a representative body of experts.

The equivalent body in the rail sector, known as "RAILPOL", is an international network of the organizations responsible for policing the railways in European Union member States. Its aim is to enhance and intensify international railway police cooperation in Europe, to prevent threats and guarantee the effectiveness of measures against cross-border crime. RAILPOL is made up of representatives of the organizations responsible for railway policing duties in European Union Member States.

Source: www.airpoleuropa.eu/; and www.railpol.eu/.

6.2.2 Canada-United States cooperation

Not only is the Canadian-United States border the longest in the world, but in Canada over 90 per cent of the population lives within 160 km of that border. Added to which, several refineries, nuclear power plants, large manufacturing facilities and other critical facilities are located close to the border. A major consequence is the presence of a high number of dependencies and cross-border CI the protection of which crucially depends on bilateral cooperation initiatives.

The main tool for cross-border cooperation on CIP is the 2010 Canada-United States Action Plan.80 While the Plan builds upon existing sectoral cooperative arrangements between the two countries, the stimulus for an integrated approach mainly stemmed from:

- The need to support strong private sector collaboration across the border
- The need to avoid duplication of efforts that are inevitable when purely sectoral approaches are taken
- The need to enhance the timeliness and accuracy of communication with CI stakeholders both domestically and across borders

The Canada-United States Action Plan is structured around three objectives: partnering for CI critical infrastructure resiliency; information-sharing; and risk management, as outlined below.

6.2.2.1 Partnering for critical infrastructure resiliency

The methodology employed to achieve this objective is to leverage existing organizational and partnership structures. On such structure is the Emergency Management Consultative Group, established under the 2008 Canada-United States Agreement on Emergency Management Cooperation to provide central oversight in support of joint emergency

80 See www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf.

management. One of the working groups established under the Consultative Group deals specifically with CI and its function has been identified as to provide direction and continuity to support the Canada-United States Action Plan.

Under this objective, the Action Plan also envisages the provision of mechanisms and opportunities for the United States sector and government coordinating councils and the Canadian sector networks to work together to improve sector-specific cross-border collaboration. In addition, the Action Plan has created a virtual Canada-United States Critical Infrastructure Risk Analysis Cell, to develop and produce collaborative analytical products with cross-border applicability.

6.2.2.2 Information-sharing

Under this objective, the two countries have pledged to work together in order to:

- Develop compatible mechanisms and protocols to protect and share sensitive critical infrastructure information
- Identify public and private sector information requirements to support the development of valuable analytical products
- Ensure effective information-sharing during and following an incident affecting critical infrastructure

6.2.2.3 Risk management

Under the Action Plan, CI risk management commits the two countries to working together to assess risks and developing plans to address priority areas. Sub-actions will be identified following a thorough review of each country's risk-informed priorities and identification of areas of mutual interest.

Box 23
Border management during and following an emergency: Canada-United States Framework

Concluded by the Department of Public Safety and Emergency Preparedness of Canada (known as "Public Safety Canada") and the United States Department of Homeland Security, the Framework applies to incidents – including but not limited to terrorist attacks – which significantly affect the border between the two countries. The Framework is designed to complement existing initiatives by facilitating coordinated, cooperative and timely border management decision-making to mitigate impacts on people and economies.

Envisaged measures include:

- Communication: The two countries commit themselves to communicating with each other as soon as practicable and to having their officials communicate until operations at the border are restored. They also commit themselves to sharing information on the nature of the incident, communicating about those goods and people considered to be a national priority of one or both countries, and facilitating joint messaging to critical infrastructure sectors, health officials, the trade and the general public.
- Border Management: The two countries commit themselves to maintaining the communication channels needed to respond to, and recover from the emergency, and to activating their respective decision-making processes to manage the movement of goods and people across the border.

Source: www.dhs.gov/xlibrary/assets/border_management_framework_2009-05-27.pdf.

6.2.3 Cooperative initiatives of the Nordic countries

The past few years have seen a growing number of initiatives addressing the cross-border dimension of CIP in the Northern European countries. Among them, the Nordic Emergency Management Cooperation is a prominent example of this kind of subregional initiative. A so-termed "reinforced version" of this operational platform was agreed upon in 2009 and linked Denmark, Finland, Iceland, Norway and Sweden. The initiative is structured around a series of working groups with annual reporting obligations to the competent ministers. In 2011, a new working group was established to address vulnerabilities and prospects for shared operational readiness in the cyber domain.[81]

[81] See www.msb.se/en/about-msb/international-co-operation/nordic-co-operations/.

For the period 2019–2021, in particular, the Nordic ministers responsible for civil protection and preparedness have identified a number of priority areas for cooperation among participating countries, including:

- Nordic cooperation on chemical, biological, radiological, nuclear substances and high-yield explosive substances (referred to as "CBRNE substances"): The purpose is to prevent, discover and handle incidents related to CBRNE substances by allocating resources for handling serious accidents, ensure access to expertise and cooperate with other sectors. Joint exercises are an integral component of the work programme, preferably as part of the exercises envisaged by the European Union Civil Protection Mechanism.
- Nordic cooperation on emergency communication: While Norway (through its emergency network), Sweden (through the national digital communications system Rakel), and Finland (through the public safety network Virve) are currently interconnected, enabling effective communication and cooperation across national borders, it is being investigated how users of other Nordic terrestrial trunked radio (TETRA) systems[82] – in Denmark (Sine) and Iceland – may also contribute to a robust and unlimited emergency response situation and emergency calls.

CASE STUDY 44
Norwegian-Swedish inter-system interface project

The Norwegian-Swedish inter-system interface project, known as the "ISI project", was a scheme between Norway and Sweden aimed at facilitating cross-border command and collaboration by creating possibilities for stakeholders in both countries to utilize their own equipment within the framework of Nødnett (the Norwegian public safety network) and Rakel (the Swedish emergency communication network). The project was carried out between 2013 and 2016 and involved Norwegian and Swedish representatives from rescue services, the police and health and ambulance services working in three working groups. In parallel with the project's working groups, a technology development group was also established.

The project was run by the Norwegian and Swedish government agencies responsible for the development and operation of systems for emergency communication in the respective countries. Motorola Systems and Airbus were collaborative partners in charge of the necessary technological developments. One success factor of the project was its early focus on communication challenges that the different user categories perceive in their everyday work in the two countries' border districts. The project resulted in:

- Proposal (draft) for a legally based agreement
- Methodology for command and collaboration
- Structure for communication in talk groups
- Common terminology
- Guidelines for use of technical equipment
- Training for users and decision-makers
- Concluding major exercise where the inter-system interface in its entirety was tested in a real situation

Source: www.msb.se/siteassets/dokument/publikationer/english-publications/a-quick-guide-to-the-norwegian-swedish-isi-project-a-cross-border-development-scheme.pdf.

[82] TETRA is a land mobile radio open standard for digital trunked radio technology. Developed by public safety and two-way radio industry experts together with the European Telecommunications Standards Institute, the standard ensures that TETRA devices – along with the network infrastructure – provide secure, reliable and instant voice and data communications in critical missions and operations.

6.3 Cross-border technical, capacity-building and financial assistance

Security Council resolution 2341 (2017)

The Security Council,

...

9. *Urges* States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, technical assistance, technology transfers and programmes, where it is needed to enable all States to achieve the goal of protection of critical infrastructure against terrorist attacks

Addendum to the Madrid Guiding Principles

In their further efforts to protect critical infrastructure and "soft" targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider:

Assisting in the delivery of effective and targeted capacity development, training and other necessary resources, and technical assistance, where it is needed to enable all States to develop appropriate capacity to implement contingency and response plans with regard to attacks against "soft" targets. (Guiding principle 51 (f))

Not only is CIP a resource-consuming effort in its various phases and dimensions; it also requires the mobilization of high levels of expertise in several domains. While CIP should be a priority issue shared by all Member States, the necessary resources and multidisciplinary skills are not readily available in all of them. Both at the sector level and cross-sectorally, awareness of the need for targeted technical assistance and capacity-building in this field is growing. In the civil a viation field, for example, ICAO encourages States with limited resources for dealing with imminent threats to "consider negotiating legal and procedural assistance with adjacent States that are better equipped to collect and disseminate threat information".[83]

[83] ICAO Aviation Security Manual (Doc 8973-Restricted).

Box 24
Regional efforts in critical infrastructure protection: OSCE and OAS initiatives

OSCE

With 57 participating States, the Organization for Security and Cooperation in Europe (OSCE) is the world's largest regional organization. OSCE pursues a comprehensive approach to security that encompasses political and military, economic and environmental, and human aspects. It therefore addresses a wide range of security-related concerns, including arms control, confidence-building and security-building measures, human rights, national minorities, democratization, policing strategies, counter-terrorism and economic and environmental activities. All 57 participating States enjoy equal status, and decisions are taken by consensus on a politically-binding basis.

As instructed by its participating States, OSCE has a history of addressing critical infrastructure protection, beginning in 2007 with Ministerial Council decision No. 6/07[84] on protecting critical energy infrastructure from terrorist attacks. In the same year, Ministerial Council decision No. 5/07[85] emphasized the role of public-private partnerships when countering terrorism, including specific reference to critical infrastructure protection. The OSCE participating States widened the scope of the organization's critical infrastructure work to international transport and other critical sectors through the OSCE 2012 Consolidated Framework for the Fight Against Terrorism.[86] Since 2007, OSCE has supported its participating States through capacity-building and technical assistance, including the production of guidance material such as the 2013 Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace[87] and – outside the domain of terrorism – the 2016 Handbook on Protecting Electricity Networks from Natural Disasters.[88] In 2021, OSCE opened its Virtual Centre for the Protection of Critical Energy Infrastructure, which includes training courses and other materials for participating States.[89] In areas other than terrorism, since 2013 OSCE participating States have adopted 16 cyber and ICT security confidence-building measures (referred to as "CBMs"):[90] CBM No. 15 focuses specifically on collaboration between States' authorities responsible for securing critical infrastructure, including exchanging of best practices, sharing information on ICT threats and improving the security of national and transnational ICT-enabled critical infrastructure.

As an entity established under Chapter VIII of the Charter of the United Nations, OSCE also supports the implementation of key United Nations documents that relate to critical infrastructure and soft targets protection, including Security Council resolutions 1540 (2004), 2396 (2017), 2341 (2017) and the United Nations Global Counter-Terrorism Strategy.

OAS

Within the Organization of American States (OAS), the Secretariat for Multidimensional Security is currently providing technical support to member States in the drafting process for a model regional strategy on the protection of CI for all hazards, including natural disasters.

The initiative is being implemented through the Inter-American Committee against Terrorism and the Secretariat for Integral Development, and with the support of the United States Government, notably the United States Mission to the OAS, CISA and the Army Corps of Engineers.

With the development of the regional strategy, OAS aims to:

- Assist its member States in managing, operating, maintaining, and modernizing critical infrastructure systems against all-hazards
- Build a regional community of subject matter experts

The regional strategy is expected to be finalized in 2023.

Sources: OSCE and OAS representatives.

84 See www.osce.org/mc/29482.

85 See www.osce.org/mc/29569.

86 See www.osce.org/pc/98008.

87 See www.osce.org/files/f/documents/7/5/103954.pdf.

88 See www.osce.org/files/f/documents/a/d/242651.pdf.

89 See www.osce.org/secretariat/443674.

90 OSCE Permanent Council decision 1202: www.osce.org/pc/227281 endorsed by the Ministerial Council: www.osce.org/cio/288086.

Member States may also envisage assisting others in need during the planning stage for enhancing CI resilience. This could take the form of knowledge – or know-how – transfers in relation to the various cycles of CIP, from risk assessment to the setting up of an appropriate governance framework.

Along these lines, the Meridian Process has put forward a proposal whereby countries "with less developed policies and activities may be offered resources and knowledge, and may learn from [guide, or buddy countries] about valuable organizational or process-wise approaches and about pitfalls to avoid. In this way, their CIIP journey may be faster than going on the path alone … Offering to be a guide nation, when a nation is ahead of other nations on the CIIP path, brings benefits as well. The buddy nation may ask CIIP questions which the guide nation has not yet considered. Moreover, a strengthened CIIP in the buddy nation creates a safer CII node in cyberspace. At the same time, guide nations should ensure that all necessary coordination and authorization has been undertaken with the relevant ministries and agencies in their nations before making approaches to a potential buddy. It is however possible to begin with informal buddying discussions to establish compatibility and mutual interests, before each nation decides to develop a more formal buddying relationship".[91]

CASE STUDY 45
European Union Civil Protection Mechanism

Established in October 2001, the European Union Civil Protection Mechanism aims to strengthen cooperation between European Union member States and six participating countries on civil protection to improve prevention, preparedness and response to disasters.

When an emergency overwhelms the response capabilities of an individual country, it can request assistance through the Mechanism. Following a request, the Emergency Response Coordination Centre mobilizes assistance or expertise. The Centre monitors events around the globe on a 24/7 basis and ensures rapid deployment of emergency support through a direct link with national civil protection authorities. Specialized teams and equipment such as search and rescue and medical teams can be mobilized at short notice for deployments inside and outside Europe. The European Commission plays a key role in coordinating the disaster response, contributing to at least 75 per cent of the transport and operational costs of deployments.

Any country in the world, including the United Nations and its agencies or a relevant international organization, can call on the European Union Civil Protection Mechanism for help. In 2021, the Mechanism was activated 114 times.

The Mechanism also helps to coordinate disaster preparedness and prevention activities of national authorities and contributes to the exchange of best practices. This facilitates the continuous development of higher common standards, enabling teams to understand different approaches better and work interchangeably when a disaster strikes.

Source: https://ec.europa.eu/echo/what/civil-protection/eu-civil-protection-mechanism_en.

Tool 26
Power Sector Cybersecurity Building Blocks – USAID

https://resilient-energy.org/cybersecurity-resilience

Developed through the partnership between the United States Agency for International Development (USAID)and the National Renewable Energy Laboratory, this tool is designed to assist a variety of stakeholders in USAID assistance countries to improve security of the electrical grid by looking at issues of governance, procurement, risk management, compliance, organization security policies, technical controls, incident response, and awareness capacity-building. The Tool is available in French, Russian and Spanish.

[91] GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers, GFCE-Meridian, 2016. Available at www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

7. Sector-specific international initiatives

This chapter provides an overview of key initiatives carried out by United Nations-system agencies in a selected number of CI sectors. Neither the list of sectors nor the described initiatives aim to be comprehensive. Rather, the purpose is to direct readers towards resources and tools that might guide them in designing sound sectoral CIP plans in the context of broader national strategies.

7.1 Maritime sector

As the leading international agency in the field, the International Maritime Organization (IMO) addresses issues of CI protection, including against terrorist attacks, as part of its initiatives to secure the civil maritime industry. This includes both the shipping and the port sectors. As far as these latter are concerned, in particular, "while many countries view … ports as critical infrastructure, without clear national and local legislation, policies and direction coordinating all those activities, security responses [are], at best, fragmented. Essential to the success of port and port facility security regimes — whether for countering theft or preventing access to ships by terrorists — [are] a well-coordinated, risk-based preventive strategy".[92] As stated by the IMO representative at a Security Council meeting, to address these issues, "IMO [has] developed a range of guidance, self-assessment tools and training materials for the protection of ports, ships and offshore installations. As threats had evolved, IMO's focus on reactive efforts to counter terrorism had been replaced by an emphasis on proactive measures … That maritime security and maritime law enforcement were viewed as departmental issues — for the navy, coast guard, or police — rather than a multi-agency issue was a main obstacle, as those agencies often competed for scarce resources". In particular, the IMO Integrated Technical Cooperation Programme in global maritime security relies on the twin pillars of technical assistance and capacity-building to support countries in their efforts to assess and address threats to their maritime borders and trade flows. This includes emerging threats such as those posed by cyber-attacks. In enhancing countries' ability to comply with maritime security-related treaties and standards, IMO promotes an approach based on inter-agency cooperation. To the extent possible, the Programme's activities are delivered in close collaboration with regional and United Nations entities that share with IMO the same broad objective to strengthen global maritime security. This includes the participation by IMO in joint country assessments undertaken under the auspices of the Security Council's Counter-Terrorism Committee.[93]

Recognizing the need for a more holistic approach, the IMO Integrated Technical Cooperation Programme has begun to target the strategic level too through support in developing national maritime security strategies, national maritime security committees, national maritime security risk registers, and other such materials. The strategic-level dimension, coupled with the operational support, aims to deliver a whole-of-government approach to maritime security, avoiding the silo mentality and maximizing all government resources to combat diverse maritime security risks.

In this context, a key framework is the ISPS Code. The Code is divided into two sections. Part A is mandatory and outlines detailed maritime and port security-related requirements to which parties to the SOLAS Convention, port authorities and

[92] Statement by the representative of IMO, "Security Council calls on Member States to address threats against critical infrastructure, unanimously adopting resolution 2341 (2017)", Security Council, 7782nd meeting, 13 February 2017. Available at www.un.org/press/en/2017/sc12714.doc.htm.

[93] See IMO, Integrated Technical Cooperation Programme (ITCP). Available at www.imo.org/en/OurWork/TechnicalCooperation/Pages/ITCP.aspx.

shipping companies must adhere. Part B provides a series of non-binding guidelines on how to meet the requirements and obligations set out in Part A. The objectives of the ISPS Code are the following:[94]

- To establish an international framework that fosters cooperation between government agencies, local administrations and the shipping and port industries in assessing and detecting potential security threats to ships or port facilities used for international trade, so as to implement preventive security measures against such threats.
- To determine the respective roles and responsibilities of all parties concerned with safeguarding maritime security in ports and onboard ships, at the national, regional and international levels.
- To ensure the early and efficient collation and exchange of maritime security-related information at national, regional and international levels.
- To provide a methodology for ship and port security assessments, which facilitates the development of ship, company and port facility security plans and procedures, to be utilized to respond to the varying security levels of ships or ports.
- To ensure that adequate and proportionate maritime security measures are in place on board ships and in ports.

For the management of potential security threats, the ISPS Code requires that countries, port authorities and shipping companies designate port facility security officers, ship security officers and company security officers respectively. These are responsible for elaborating and implementing specific security plans.

7.2 Aviation sector

ICAO is a United Nations specialized agency, established by States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).[95]

ICAO works with the 193 parties to the Chicago Convention and also with industry groups to reach consensus on international civil aviation standards and recommended practices (referred to in ICAO as "SARPs") and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector. These SARPs and policies are used by ICAO member States to ensure that their local civil aviation operations and regulations conform to global norms, which in turn permits more than 100,000 daily flights in the global aviation network to operate securely, safely and reliably in every region of the world.

In addition to its core work resolving consensus-driven international SARPs and policies among its member States and in the industry, and among many other priorities and programmes, ICAO also coordinates assistance and capacity-building for States in support of numerous aviation development objectives; produces global plans to coordinate multilateral strategic progress for safety and air navigation; monitors and reports on numerous air transport sector performance metrics; and audits States' civil aviation oversight capabilities in the areas of safety and security.

As for the ICAO strategic objective on aviation security and facilitation, this is essentially carried out through the following measures:

- Setting the standards and recommended practices for international civil aviation in the area of security, facilitation, identity and border management.
- Continuous auditing and monitoring of member States' aviation security performance, in order to enhance their aviation security compliance and oversight capabilities.

[94] See IMO, Maritime Security and Piracy. Available at www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx.

[95] ICAO Doc 7300/9; see also United Nations, Treaty Series, vol. 15, No. 102.

- Providing capacity-building assistance and training to improve States' capabilities in both aviation security and facilitation.

ICAO work in the sector is anchored in a number of aviation security treaties. These have been adopted over a timespan of more than fifty years and are commonly regarded as an integral part of the universal legal framework against terrorism:

1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft

1970 Convention for the Suppression of Unlawful Seizure of Aircraft

1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation

1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation

1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection

2009 Montreal Convention on Compensation for Damage to Third Parties, Resulting from Acts of Unlawful Interference Involving Aircraft

2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation

2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft

2014 Protocol to Amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft

The foundation reference document for States, industry, stakeholders and ICAO to work together with the shared goal of enhancing aviation security worldwide is the Global Aviation Security Plan. Approved in 2017 by the ICAO Council, the Plan sets forth five priority outcomes:

Enhance risk awareness and response.

Develop security culture and human capability.

Improve technological resources and foster innovation.

Improve oversight and quality assurance.

Increase cooperation and support.

A fundamental tool is the Aviation Security Manual (Doc 8973, Restricted),[96] which is designed to assist States in the implementation of standards and recommended practices included in annex 17[97] – Aviation Security–to the Chicago Convention. The latest version of the Manual, the thirteenth edition, published at the end of 2022, features new and updated guidance material. Of particular interest for CIP are best practices related to the security of landside areas of airports, staff screening and vehicle screening, cyberthreats to critical aviation systems, establishment of a risk-based prohibited item list, application of alternative security measures for lower-risk airports, and reporting of aviation security incidents.

Another relevant tool is the Aviation Security Global Risk Context Statement (Doc 10108, Restricted, which is currently in its third edition). This living document provides States with high-level information on the global threat-and-risk environment. It contains analysis of global threats to civil aviation, information on recent developments in terrorist tactics, and technical analysis on specific aviation security trends.

Acknowledging the urgency and importance of protecting the CI, information and communication technology systems and data of civil aviation against cyberthreats, ICAO is committed to developing a solid cybersecurity framework. At its 40th session, the ICAO Assembly adopted Assembly Resolution A40-10, on addressing cybersecurity in civil aviation. The

[96] Access to the Manual is classified as restricted. Its distribution is limited to State civil aviation authorities and, on request, other entities responsible for implementing aviation security measures, such as airport and aircraft operators, or other entities as validated by a State appropriate authority. The Aviation Security Manual is accessible electronically to authorized users at https://drm.icao.int/ website.

[97] Annex 17 – Security–includes, notably, the Standards and Recommended Practices for international aviation security and is constantly being reviewed and amended in the light of new threats and technological developments that have a bearing on the effectiveness of measures designed to prevent acts of unlawful interference.

resolution addresses cybersecurity through a horizontal, cross-cutting and functional approach, reaffirming the importance and urgency of protecting the CI systems and data of civil aviation against cyberthreats and calling upon States to implement the ICAO Cybersecurity Strategy.

Endorsed in 2013 by the ICAO Assembly at its 38th session, the ICAO Traveller Identification Programme (TRIP) Strategy continues to provide the framework for member States in achieving enhancements in aviation security and facilitation, and in meeting their obligations under Security Council resolutions relating to terrorism. The Strategy contains five elements, namely: evidence of identity; machine readable travel documents; document issuance and control; inspection systems and tools; and interoperable applications.

The Security Council has recognized the leadership and activities of ICAO in travel documentation policy and operational matters, which have made a significant contribution to enhancing aviation security and facilitation, notably through progressive travel document standards and specifications, and traveller identification tools to secure the borders.

The technical specifications that enable global interoperability of travel documents are found in Doc 9303, Machine Readable Travel Documents (referred to as "MRTDs"). Its eighth edition includes a new Part 13 elaborating specifications for visible digital seals (VDS) to be used for a quick reference (QR) code supporting the technologies behind the contactless processes allowing notably reliable authentication of the testing results and future vaccination certificates. In addition, with a view to ensuring a seamless journey for travellers, with fewer passenger touchpoints at the airport, resulting in a healthier and safer travel experiences, the digital travel credentials (DTC) tool and its specifications have also been endorsed, which will enable an ICAO compliant passport to be extended to a passenger's mobile device.

Moreover, ICAO is setting standards and recommended practices (SARPs) with regard to the establishment of a framework for advance passenger information (API) and passenger name record (PNR). Validation of identity is a cornerstone of efforts to hinder cross-border movements as part of terrorist activities. With a view to encouraging participation in the ICAO Public Key Directory (PKD), Amendment 26 to Annex 9 – Facilitation – has introduced a new Recommended Practice (RP), RP 3.35.5, targeted at those ICAO member States that use automated border control (ABC) systems. This RP encourages the use of the information available through the ICAO PKD as a means of validating e-passports by comparing the facial recognition to the e-passport holder's photograph.

ICAO cooperates with various United Nations offices, directorates and specialized agencies (such as the Office of Counter-Terrorism, the Counter-Terrorism Committee Executive Directorate, and the United Nations Office on Drugs and Crime), along with other international organizations (INTERPOL, IMO and the World Customs Organization) to fulfil the commitments defined in the United Nations Global Counter-Terrorism Strategy. Cooperative activities are directly related to aviation security and facilitation, identity, and border control management, as described in Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2309 (2016), 2341 (2017), 2395 (2017), 2396 (2017) and 2482 (2019). ICAO is a member of the Global Counter-Terrorism Coordination Compact and actively participates in the work of the working groups on border management and law enforcement relating to counter-terrorism, on emerging threats and on CIP.

7.3 Information technology sector

The protection of CII against cybersecurity risks is a priority goal of ITU. The Buenos Aires Action Plan, adopted at the 2017 World Telecommunication Development Conference, included as its Objective 2 "Foster the development of Infrastructure and services, including building confidence and security in the use of telecommunications/ICTs".[98] The work of ITU directly

[98] The Conference's Final Report is available at www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.

relates to enhancing the resilience of CII against cyberattacks. Its activities revolve around three major action blocks: standard setting; awareness-raising; and capacity-building. Key ongoing initiatives relating to each of these blocks and highlighted in the following paragraphs.

7.3.1 Standard setting

Standardization work is carried out by a number of technical study groups in which representatives of the ITU membership develop recommendations (standards) in the various fields of international telecommunications. Study group 17, in particular, deals with building confidence and security in the use of information and communication technologies to achieve more secure network infrastructure, services and applications. Within this study group, over 350 standards[99] (known as "ITU-T Recommendations and Supplements") have been adopted so far.

Ongoing work areas for study group 17 include, among others, cybersecurity, security management, security architectures and frameworks, identity management, application security, and security aspects of cloud computing, the Internet of things, the intelligent transport system, big data, and distributed ledger technology. A key reference for security standards is recommendation ITU-T X.509 for electronic authentication over public networks. ITU-T X.509 is regarded as a landmark tool for designing applications relating to public key infrastructure.

7.3.2 Awareness-raising

A ground-breaking tool developed by ITU is the Global Cybersecurity Index. Conceived primarily as an awareness-raising tool, the Index seeks to measure countries' commitment to cybersecurity. Each country's performance is assessed in five areas: legal measures, technical measures, organizational measures, capacity-building and cooperation.

Questions are developed to assess commitment in each pillar. Subsequently, through consultation with a group of experts, these questions are weighted in order to arrive at an overall score on the Index. The fourth edition of the Index was published in 2020.[100]

7.3.3 Capacity-building

ITU supports member States in establishing national computer incident response teams (known as "CIRTs"). These consist of national focal points for coordinating timely and effective response to cyberattacks. ITU is committed to assisting its member States along the entire process of setting up these teams, from assessing their readiness to helping with the planning and implementation phases, based on the principle of continued collaboration. ITU further organizes regular regional exercises (referred to as "cyber drills") to enhance collaboration among national teams within the same region.

To date, assessments of national computer incident response teams have been completed for more than 80 countries and such teams have been either established or enhanced in 17 countries.

Another dimension of ITU work in the capacity-building area focuses on assisting countries in the development of national cybersecurity strategies. These efforts were boosted by the publication in 2018 of the "Guide to developing a national cybersecurity strategy".[101]

[99] ITU-T Recommendations developed by ITU-T Study Group 17 are publicly available at www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17.

[100] The current version of the Index and previous editions are available at www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[101] www.itu.int/hub/publication/d-str-cyb_guide-01-2018/.

7.4 Conventional weapons sector

In its resolution 2370 (2017), the Security Council recognizes the "value of … measures aiming at achieving effective physical security and management of stockpiles of small arms and light weapons, as an important means to contribute to eliminating the supply of weapons to terrorists".[102]

In particular, in paragraph 7 of the resolution, the Council emphasizes "the importance of Member States taking appropriate measures ... to prevent … looting or acquiring small arms and light weapons from national stockpiles by terrorists, and stresses in this regard on the importance of assisting States in those regions to enable them to monitor and control stockpiles of small arms and light weapons, in order to prevent terrorists from acquiring them".

In relation to the protection of critical infrastructure, ensuring the physical security and management of stockpiles of conventional weapons is critical in a double sense. First, it reduces the risk that such weapons may be used against CI such as transport systems, government premises and any other installation deemed critical by individual countries. Second, those very stockpiles may be considered as CI in themselves, since they are instrumental in upholding countries' defence policies.

A variety of international and regional instruments form part of the international legal regime on conventional weapons. While these instruments provide the legal and operational framework for Member States to reinforce their domestic legal regimes, they do not necessarily form a homogenous set of tools. By way of example, the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition (Firearms Protocol)[103] deals with the issue from the criminal justice angle, with a view to providing measures to address the transnational nature of the phenomenon and its links to organized crime. Other instruments, although covering similar topics, address the issue from a disarmament, trade or development perspective, and focus more on measures to reduce the accumulation, proliferation, diversion and misuse of firearms. As a result, it is important for state authorities to familiarize themselves with a heterogeneous international legal framework and ensure its full implementation.

The following list is a non-exhaustive compilation of international (United Nations and regional) treaties and other guiding instruments dealing with the subject from its various angles.

United Nations

Treaties

- Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime (2001)
- Arms Trade Treaty (2013)

Other instruments

- Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (2001)
- International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (2005)

[102] These measures were already contemplated in the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects. Under this programme, Governments agreed to improve national small arms laws, import and export controls, and stockpile management – and to engage in cooperation and assistance (www.un.org/disarmament/convarms/salw/programme-of-action/).

[103] The Protocol supplements the United Nations Convention against Transnational Organized Crime.

Africa

Treaties

- Protocol on the Control of Firearms, Ammunition and Other Related Materials in The Southern African Development Community Region (2001)
- Nairobi Protocol for the Prevention, Control, and Reduction of Small Arms and Light Weapons in the Great Lakes Region and the Horn of Africa (2004)
- Economic Community of West African States Convention on Small Arms and Light Weapons, Their Ammunition and Other Related Materials (2006)
- Central African Convention for the Control of Small Arms and Light Weapons, their Ammunition and All Parts and Components That Can Be Used for Their Manufacture, Repair and Assembly (Kinshasa Convention) (2010)

Other instruments

- Bamako Declaration on an African Common Position on the Illicit Proliferation, Circulation and Trafficking of Small Arms and Light Weapons (2000)
- African Union Strategy on the Control of Illicit Proliferation, Circulation and Trafficking of Small Arms and Light Weapons (2011)
- Action Plan for The Implementation of the African Union Strategy on the Control of Illicit Proliferation, Circulation and Trafficking of Small Arms and Light Weapons

Americas

Treaties

- Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and other Related Materials (1997)

Other instruments

- Andean Plan to Prevent, Combat and Eradicate Illicit Trade in Small Arms and Light Weapons in All Its Aspects (2003)
- Model Regulations for the Control of International Movement of Firearms, Their Parts and Components and Ammunition (2000)
- Central American Integration System Code of Conduct of the Central America States on the Transfer of Arms, Ammunition, Explosives and Other Related Materials (2006)

Asia-Pacific

Instruments

- Nadi Framework (Legal Framework for a Common Approach to Weapons Control Measures)
- ASEAN Plan of Action to Combat Transnational Crime (Association of Southeast Asian Nations) (1999)

Europe

Organization for Security and Cooperation in Europe

- OSCE Plan of Action on Small Arms and Light Weapons

- Handbook of Best Practices on Conventional Ammunition, Handbook of Best Practices on Conventional Ammunition (2008);
- OSCE Principles on the Control of Brokering in Small Arms and Light Weapons (2004);
- Standard Elements of End-User Certificates and Verification Procedures for Small Arms and Light Weapons Exports (Forum for Security Cooperation) (2004)
- Handbook of Best Practices on Small Arms and Light Weapons (2003)
- OSCE Principles Governing Conventional Arms Transfers (1993)
- OSCE Document on Small Arms and Light Weapons (2000, reissued in 2012)
- OSCE Decision no. 11/08 Introducing best practices to prevent destabilizing transfers of small arms and light weapons through air transport and on an associated questionnaire (2008)

European Union

- Council Joint Action of 12 July 2002 on the European Union's contribution to combating the destabilizing accumulation and spread of small arms and light weapons
- Council Common Position 2003/468/CFSP of 23 June 2003 on the control of arms brokering
- Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment
- Regulation (EU) No. 258/2012 of the European Parliament and of the Council of 14 March 2012 implementing Article 10 of the United Nations Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against Transnational Organised Crime, and establishing export authorization, and import and transit measures for firearms, their parts and components and ammunition
- European Union Code of Conduct on Arms Exports (1998)
- European Union strategy to combat illicit accumulation and trafficking of small arms and light weapons and their ammunition (2005).

7.5 Chemical, biological, radiological and nuclear sectors

The possibility of non-State entities, including terrorist groups and their supporters, gaining access to and using weapons and materials of mass destruction is regarded as a serious threat to international peace and security. In its resolution on the seventh review of the United Nations Global Counter-Terrorism Strategy (resolution 75/291), the General Assembly called upon all Member States to "prevent the acquisition by terrorists of nuclear, chemical and biological materials and to support international efforts under the auspices of the United Nations to prevent terrorists from acquiring weapons of mass destruction and their means of delivery, and urges all Member States to take and strengthen national measures, as appropriate, to prevent terrorists from acquiring weapons of mass destruction, their means of delivery and related materials, equipment and technologies related to their manufacture" (para. 68). The Security Council has made similar pronouncements, the latest of which is included in resolution 2325 (2016) of 15 December 2016, which calls on all Member States to strengthen their national anti-proliferation regimes in the implementation of its seminal resolution 1540 (2004).

Office of Counter-Terrorism

Further to Security Council resolution 2325 (2016), the United Nations Global Counter-Terrorism Strategy calls upon Member States, international organizations and the United Nations system to:

- Combat smuggling of chemical, biological, radiological and nuclear materials
- Ensure that advances in biotechnology are not used for terrorist purposes
- Improve border and customs controls to prevent and detect illicit trafficking of CBRN weapons and materials
- Improve coordination in planning a response to a terrorist attack using CBRN weapons or materials

In response to the CBRN global threat, the Office of Counter-Terrorism, through the United Nations Counter-Terrorism Centre, developed its Programme on Preventing and Responding to Weapons of Mass Destruction/Chemical Biological, Radiological and Nuclear (WMD/CBRN) Terrorism. The Programme seeks to advance Member States' and international organizations' understanding of the level of this threat. It also supports their prevention, preparedness and response efforts at their request. Specifically, the Programme provides capacity-building support, focusing on areas such as border and export control, strategic trade control, illicit trafficking, protection of CBRN materials and critical infrastructure, CBRN forensics, emerging technologies, incident response and crisis management, through, among other measures, a global portfolio of training events.

The Programme supports the working groups of the Global Counter-Terrorism Coordination Compact, in particular those on emerging threats and critical infrastructure protection, and on border management and law enforcement relating to counter-terrorism.

Moreover, it is designed to strengthen strategic partnerships with relevant WMD and CBRN-related members of the Global Counter-Terrorism Coordination Compact and Member States' international initiatives, enabling the development of joint, complementary and mutually reinforcing projects. Close working relationships have been established with the Global Initiative to Combat Nuclear Terrorism and the Group of Seven-led Global Partnership against the Spread of Weapons and Materials of Mass Destruction.

United Nations Interregional Crime and Justice Research Institute

Action by the United Nations Interregional Crime and Justice Research Institute (UNICRI) in this field is based on the observation that existing national strategies acknowledge the importance of developing a comprehensive approach, but tend to have an isolated stance perpetuated by the divisional structuring of CBRN sectors. In the light of this observation, UNICRI supports the development of an integrated CBRN approach that incorporates all international, regional and national CBRN components into a common strategy. This entails the application of a holistic approach through which all stakeholders, while operating autonomously, can establish common goals, identify and manage resources to achieve these goals, clearly allocate responsibilities and tasks, elaborate functioning channels of communication, create a security culture based on common learning, and ensure that lessons learned are incorporated and absorbed throughout the whole system.

In line with this vision, UNICRI, with the technical support of the International Atomic Energy Agency (IAEA), the Organisation for the Prohibition of Chemical Weapons (OPCW), the Implementing Support Unit of the Biological Weapons Convention, the World Health Organization (WHO), INTERPOL, Europol and the World Customs Organisation launched the CBRN Risk Mitigation and Security Governance Programme.[104] The main objectives of the Programme are to:

- Promote and support the development of CBRN security governance in participating countries by encouraging a comprehensive CBRN approach, establishing clear channels of communication, improving information-sharing and transferring international best practices.

[104] See https://unicri.it/index.php/topics/cbrn.

- Optimize the sharing and use of accumulated international and national experience in the area of CBRN risk mitigation, including applying knowledge and lessons learned from the nuclear security field to the chemical and biological security field.
- Develop a cooperation process among network members to identify problems and possible solutions from information available to the network. Through this approach, the intent is to generate genuine ownership of policy and its implementation by national agencies.

7.5.1 INTERPOL

In 2010, at its eightieth session, the INTERPOL General Assembly took a historic decision[105] to launch a comprehensive CBRNE terrorism prevention and response capacity in support of the Organization's 192 member countries. In 2016, in the "weapons and materials" action stream of its Global Counter-Terrorism Strategy – a five-year flexible strategic framework – INTERPOL cemented its mission in the CBRNE field by undertaking to assist member countries in the identification, tracking and interception of the illicit trafficking of weapons and materials necessary for terrorist activities. The Strategy further defines the main actions to be taken by the CBRNE and Vulnerable Targets Sub-Directorate with a view to assisting member countries in the prevention of and response to non-State actor-based CBRNE global threats:

- Action 4.3: Facilitate intelligence sharing among member countries about subjects and modus operandi linked to CBRN and IED incidents.
- Action 4.4: Enhance the capacity of member countries to prevent and respond to CBRN and IED attacks by establishing programmes of countermeasures.
- Action 4.5: Design and coordinate cross-border intelligence-led interagency operations to intercept the illicit trafficking of CBRN materials and IED components.
- Action 4.7: Maintain and develop strategic CBRNE partnerships on a global scale.

In implementing the aforementioned actions – and in line with the INTERPOL Constitution[106] – the Organization exclusively focuses on addressing CBRNE threats posed by non-State actors. Accordingly, INTERPOL refrains from addressing matters related to the State-sponsored proliferation of weapons of mass destruction, which are thoroughly addressed by other international legal and institutional mechanisms. Nevertheless, the spectrum of non-State actors encompasses not only terrorist groups, lone wolves, and other criminals as potential end-users, but also the large picture of illicit trafficking in CBRNE materials and its different components. Suppliers, intermediaries, buyers and smuggling networks all fall within the purview of INTERPOL.

The explicit mention in Security Council resolution 1540 (2004) of non-State actors made the resolution a natural point of reference for the CBRNE-related activities of INTERPOL. Since it first developed its CBRNE capacity, INTERPOL has been exchanging official letters with the 1540 Committee, outlining the terms of their ongoing collaboration and designating respective points of contact. More recently, INTERPOL has played an active role within the framework of the resolution's 2016 comprehensive review. More broadly, INTERPOL is a designated "assistant provider agency" under the resolution 1540 (2004) initiative and the majority of its activities within the CBRNE field support – either directly or indirectly – implementation of the resolution.

[105] Resolution AS-2011-RES-10 of 7 November 2011.

[106] Article 3 of the INTERPOL Constitution enshrines the guiding principle of neutrality by explicitly forbidding INTERPOL from engaging in matters of a political, military, religious or racial character.

INTERPOL has been maintaining a close working relationship with the United Nations Office for Disarmament Affairs, especially in contributing to the capacity-building activities of the roster of experts participating in the Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons.

In 2020, INTERPOL and the United Nations Counter-Terrorism Centre of the Office of Counter-Terrorism have launched a joint initiative to produce a global threat study on non-State actors and their CBRNE materials. By developing strategic threat assessments against CBRNE using national law enforcement information, this five-year initiative will help the international community counter the threat posed by non-State actors' access to CBRNE materials. With law enforcement agencies worldwide leading prevention, preparedness, and response efforts against CBRNE terrorism, the threat assessments will be used to prioritize future international support and capacity building activities, including through the INTERPOL CBRNE and vulnerable targets programme.

INTERPOL has established a sub-directorate on CBRNE and vulnerable targets, supported by an analytical unit that produces country and regional assessments, compiles reports and provides information that offers direction for targeted activities. The Radiological and Nuclear Terrorism Prevention Unit within the CBRNE and Vulnerable Targets Sub-Directorate focuses on the development and delivery of projects designed to raise awareness on the availability and vulnerability of radiological and nuclear materials, and in turn improve the capability and capacity of member countries to prevent, detect, respond and investigate terrorist and criminal acts involving these materials. Using a multi-agency approach, the Unit's activities promote relationship building and information-sharing, and encourage the development of joint agency response plans. This goal is achieved by bringing together representatives from police, customs, border security agencies, science, academia, regulatory bodies, government ministries and other relevant organizations.

At INTERPOL, specialized teams focus on the prevention of three types of terrorism:

- Radiological and nuclear terrorism
- Bioterrorism
- Chemical and explosives terrorism

INTERPOL activities range from data analysis, training workshops and table-top exercises to international conferences and on-the-ground operations. The INTERPOL methodology for countering the CBRNE threats consists of three main pillars:

- The first pillar comprises information-sharing and intelligence analysis. In addition to conducting threat assessments and analysis, INTERPOL publishes a regular analytical report: the INTERPOL CBRNE Monthly Digest. Shared with member countries and other subscribers, the report summarizes open-source reporting on all aspects of CBRNE crime and terrorism and provides an analytical perspective on particular issues.
- The second pillar involves capacity building and training. The Organization assists its member countries in building their capacity, skills, and knowledge in order to counter the CBRNE threat. It works to:
    - Increase the level of CBRNE awareness in law enforcement agencies
    - Deliver training sessions in order to increase law enforcement capabilities
    - Provide prevention methodologies for use by member countries
- The third pillar consists in the provision of operational and investigative support. On request, INTERPOL can provide operational support to its member countries in the form of an incident response team. In the event of a terrorist attack, staff with expertise in CBRNE matters can be deployed in these teams. In addition, the Organization run a number of initiatives, projects and operations to support the international law enforcement community in tackling the trafficking of CBRNE materials.

7.5.2 Chemical sector

OPCW addresses the issue of CI protection from the perspective of promoting sound security management practices of processes and chemical sites. In 2016, the Organization compiled a best practices manual which collects and elaborates information received from 16 member States.[107]

OPCW notably views security issues (understood as measures addressing the "deliberate releases" of toxic chemicals) hand-in-hand with safety issues (namely, measures to confront "non-deliberate releases"). The Organization's overarching objectives in this area are to ensure member States' coverage of the following safety and security dimensions:

- Prevention: Refers to the understanding and implementation of measures to reduce the potential for a chemical accident or security incident to occur. A chemical security incident may include the theft of chemical materials for subsequent misuse or the malicious release of chemicals into the environment.
- Detection: Refers to systems and processes that support the early detection of a chemical release or loss, and the confirmation of chemical use following a suspected release (either accidental or malicious). Detection systems should incorporate risk communication processes.
- Response: Refers to both facility-level response and national-level response to a chemical accident or chemical security incident. Response systems include the engagement, equipping, and training of responders, such as fire, hazmat, emergency, and police.

Among existing international instruments and initiatives, OPCW has highlighted the following as incorporating useful elements on chemical safety and security issues:

- Security Council resolution 1540 (2004), which obliges Member States, among others, to refrain from supporting by any means non-State actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their delivery systems. Crucially, this instrument focuses on the preventive dimension elements of chemical security risk management.
- Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, which deals with the international movement of hazardous materials. While the Convention seeks to prevent the release of toxic chemicals into the environment, implementing measures can support safe handling of chemicals and reduce the volume of chemicals in transport and within the waste system, supporting both chemical safety and chemical security best practices.
- Stockholm Convention on Persistent Organic Pollutants, which seeks to reduce the production and use of persistent organic pollutants. Regulations and best practices adopted to implement this Convention are instrumental in enhancing chemical safety and security risk management.
- Rotterdam Convention on the Prior Informed Consent Procedure for Certain Hazardous Chemicals and Pesticides in International Trade, which regulates the labelling and handling of hazardous chemicals, in particular those which are internationally traded. It contains standards and guidance useful to support supply chain security practices.
- Seveso Directives (I, II, and III)[108], European Union instruments which are aimed at improving the safety of sites containing large quantities of dangerous substances.
- Globalized Harmonized System of Classification and Labelling of Chemicals (GHS), a United Nations-managed standard established to replace the plethora of hazardous material classification and labelling schemes previously

[107] See www.opcw.org/sites/default/files/documents/ICA/ICB/OPCW_Report_on_Needs_and_Best_Practices_on_Chemical_Safety_and_Security_ManagementV3-2_1.2.pdf.

[108] Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances" and the original Seveso Directive was "Directive 82/501/EC on the control of major-accident hazards involving dangerous substances"

used by countries around the world. While voluntary in nature, several country regulations have made it binding at the domestic level.

- Responsible Care, a global chemical industry initiative which is aimed, among other objectives, at enhancing security of products and processes and, as stated on its website, "commits companies, national chemical industry associations and their partners to provide help and advice to foster the responsible management of chemicals by all those who manage and use them along the product chain".[109]
- International Organization for Standardization (ISO), which has established a number of standards supporting elements of chemical safety and security, in particular: 13000 on risk management, 28000 on the chemical supply chain, 14000 on environmental management, and 9000 on quality management.

Focusing more specifically on the terrorist threat posed by non-State actors, an OPWC-convened expert workshop on international chemical security coordination was held in 2017.[110] The workshop conducted an overview exercise "aiming to take stock of existing international cooperation and coordination on chemical security, to identify gaps and to deliberate on future activities, including future coordination mechanisms". A key recommendation was the establishment of an international coordination mechanism "to enable the key international actors supporting global chemical-security capability development … to discuss priorities and methodologies, leverage each other's resources, collaborate where needed on meeting individual State needs, and raise the international profile of chemical security needs and assistance". Another key outcome of the meeting was a recommendation to set up a model chemical security delivery methodology.

OPCW capacity-building activities with direct relevance to CI in the chemical sector are implemented through the Chemical Safety and Security Management Programme.[111] Through the sharing of policies and best practices with chemistry practitioners, policymakers, national authorities and chemical industry associations, the Programme seeks to promote and disseminate a chemical safety and security management culture. It provides training to specialists on practical aspects of chemical safety and security, and forums to share and discuss best practices among stakeholders. From 2008 to 2018, capacity-building programmes on integrated chemical risk management carried out by the OPCW Technical Secretariat have been attended by over 2,000 participants from more than 130 member States.

7.5.3 Nuclear sector

The protection of nuclear and other radioactive materials and their associated facilities against terrorist attacks and other hazards is a priority goal of IAEA. Its initiatives in this field are pursued by the Nuclear Security Division, which addresses all issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear and other radioactive materials and associated facilities. The legal bases underpinning these work areas comprise a web of international instruments which include, notably:

- Convention on the Physical Protection of Nuclear Material (with its 2005 Amendment)
- Code of Conduct on the Safety and Security of Radioactive Sources
- United Nations Security Council resolutions 1373 (2001), 1540 (2004) and 2325 (2016)
- International Convention for the Suppression of Acts of Nuclear Terrorism

The IAEA Nuclear Security Series of publications complement the above by providing best practices, technical guides, training manuals and other materials for the benefit of member States. These publications include the implementing

[109] See www.cefic.org/Responsible-Care.

[110] Expert Workshop on International Chemical Security Coordination, 7 December 2017. Available at www.opcw.org/fileadmin/OPCW/Protection-Against-CW/OPCW_Chemical_Security_Workshop_-_Informal_Summary_-_October_2017_-_for_release.pdf.

[111] See www.opcw.org/resources/capacity-building/international-cooperation-programmes/chemical-safety-and-security.

guide entitled Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme (IAEA 2013). The guide provides technical guidance on the development of a nuclear security infrastructure, including a legal, regulatory and institutional framework and a national nuclear security strategy. Its rationale lies in the need, as stated in the foreword to the guide, "to ensure that nuclear and other radioactive material does not fall into the hands of parties who could use the material for criminal or terrorist acts, and to prevent acts of sabotage against facilities and associated activities, including during transport".

On 14 September 2021, the Board of Governors approved the Nuclear Security Plan for the period 2022–2025.[112] The Plan describes proposed IAEA nuclear security activities that respond to the priorities that member States have put forward through the decisions and resolutions of the Agency's policymaking bodies. The Plan identifies, in particular, a set of priority areas and sub-areas for intervention through technical assistance and capacity building activities, which include:

- Continue to promote further adherence to the Convention on the Physical Protection of Nuclear Material and its Amendment with the aim of its universalization.
- Provide assistance, upon request, in areas of prevention, detection and response, and also insider threat mitigation and nuclear security culture.
- Reinforce the protection of sensitive information and computer-based systems, recognizing the threats to nuclear security and from cyberattacks at nuclear related facilities, as well as their associated activities including the use, storage and transport of nuclear and other radioactive material.
- Assist member States, upon request, in their development of national legislative and regulatory frameworks; promote and facilitate technical exchanges of knowledge, experiences and good practices on the use and security of radioactive sources throughout their life-cycle.
- Strengthen the nuclear security culture and provide education and training opportunities in nuclear security.

[112] See www.iaea.org/sites/default/files/gc/gc65-24.pdf.

Annex I
Selected resources on CIP by country[1]

Argentina

Resolution No.1523 (2019)	Normative instrument	The resolution, which was adopted by the Government Secretariat for Modernization, with the collaboration of the Cybersecurity Committee, in the framework of the National Cybersecurity Strategy, defines the concept of critical infrastructure and critical information infrastructure. It also approves a glossary of cybersecurity terms, in which such concepts as access, threat, cyberattack, cookies and data leakage, among others, are be found. The resolution explains, in its preambular part, that the Cybersecurity Committee carried out a detailed analysis of the definitions adopted by different countries and international organizations, thus seeking to take advantage of international experience and knowledge in the matter. The resolution mandates the National Director of Cybersecurity to periodically review and update the glossary.	www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Australia

Critical Infrastructure Resilience Strategy: Plan (2015)	Strategy and policy document	The Strategy aims to support the continued operation of CI in the face of all hazards. The key outcomes that the Strategy seeks to achieve are: • Strong and effective business-government partnership • Enhanced risk management of the operating environment • Effective understanding and management of strategic issues • Mature understanding and application of organizational resilience The document outlines the core activities that will be undertaken at a national level in pursuit of these outcomes.	www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF
National Guidelines for Protecting Critical Infrastructure from Terrorism (2015)	Strategy and policy document	The Guidelines complement the CI Resilience Strategy by providing a framework for a national approach on CIP against the specific threat posed by terrorist acts.	www.police.vic.gov.au/sites/default/files/2019-03/NationalGuidelinesForProtectingCriticalInfrastructureFromTerrorismNovember2015.pdf
Security of Critical Infrastructure Act (2018)	Normative instrument	The object of this Act is to provide a framework for managing risks relating to critical infrastructure, including by: • Improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks • facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks • providing a regime for the Commonwealth to respond to serious cybersecurity incidents On 2 December 2021, the Security of Critical Infrastructure Act 2018 was amended to expand coverage from 4 sectors to 11 sectors and 22 asset classes.	www.legislation.gov.au/Details/C2021C00570
Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy (2022)	Strategy and policy document	The purpose of this strategy is to outline how the Cyber and Infrastructure Security Centre will accomplish compliance and enforcement of the entities that it regulates by ensuring that they satisfy their regulatory obligations under relevant legislation. In delivering a best-practice, industry-focused, active and engaged regulatory partnership that works with industry to improve the security and prosperity of Australia, the Centre drives an all-hazards approach across each of the 11 critical infrastructure sectors that it regulates, underpinned by a strong focus on cybersecurity. The Compliance and Enforcement Strategy explains the key principles that underpin the Centre's regulatory, compliance and enforcement approach and should be read in conjunction with the Centre's Protecting Australia Together publication and the Critical Infrastructure Resilience Strategy.	www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-compliance-enforcement-strategy-april-2022.pdf

[1] The information displayed in this annex is not intended to be an exhaustive list of existing government resources on CIP. Information has been included on the basis of relevance, web accessibility, geographical representation and the responses provided by Governments in response to a note verbale sent to Member States by the Office on Counter-Terrorism on 2 March 2022 requesting them "to share their good practices on critical infrastructure protection (in English or any other available language)".

Belgium

Act on the security and protection of critical infrastructure (2011, amended in 2018)	Normative instrument	The Act : • Partially transposes European Union Directive 2008/114 / on the designation of European critical infrastructure • Establishes the criteria and procedures for identifying and designating CI • Defines internal and external security measures for CIP • Determines the scope and modalities for information exchanges between CI operators and the competent public agencies • Sets forth the public controls and sanctions for violations of the law.	www.nbb.be/doc/cp/fr/2018/20180925_loi_du_1juillet2011.pdf

Canada

Emergency Management Framework for Canada (2011)	Strategy and policy document	Establishes a common approach for the various federal, provincial and territorial emergency management initiatives. The Framework aims to enable consolidation of federal, provincial and territorial collaborative work and ensure more coherent, complementary actions among the different government initiatives at federal, provincial and territorial levels. It underscores the key components of emergency management. It also introduces new terms and revises existing definitions for evolving terms such as "all-hazards" and "resilience" to reflect contemporary developments in the field of emergency management.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frm-wrk/mrgnc-mngmnt-frmwrk-eng.pdf
Cyber Security Strategy (2018)	Strategy and policy document	Seeks to strengthen cyber systems and CI sectors by building on three pillars: Securing Government systems; Partnering to secure vital cyber systems outside the federal Government; Helping Canadians to be secure online.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
National Strategy for Critical Infrastructure (2009)	Strategy and policy document	Based on the principles of the Emergency Management Framework, the Strategy proposes that federal, provincial and territorial governments and ten CI sectors collaborate to strengthen CI resiliency in Canada. Collaboration is predicated on the development of partnerships building upon existing mandates and responsibilities. To foster these partnerships, the Strategy outlines mechanisms for enhanced information-sharing and information protection and identifies the importance of a risk management approach.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
Action Plan for Critical Infrastructure (2021–2023)	Strategy and policy document	The Action Plan supports the advancement of the 2009 National Strategy by reaffirming the commitments by the Government of Canada to work closely with CI sector partners, provinces and territories towards a more secure and resilient Canada. The Action Plan builds upon progress made through past action plans, identifies new activities based on the changing threat environment, and will support a collaborative approach to enhance the security and resilience of the country's CI.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx

China

Critical Information Infrastructure Security and Protection Regulations (2021)	Normative instrument	The Regulations define the country's policies on the protection of CII. Specifically, the General Provisions assign to the Public Security Department of the State Council responsibility for guiding and supervising CI security protection work. The various chapters set forth rules for the identification of CI, responsibilities and duties of CI operators, and the operators' legal liability for non-compliance with the regulations.	https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/

France

Decree No. 2007-585 of 23 April 2007 on certain regulatory provisions of the first part of the Defence Code	Normative instrument	Amends the Defence Code by introducing a set of articles that establish the institutional framework for the protection of activities of vital importance ("activités d'importance vitale") (see articles R. 1332-1–1332-42).	www.legifrance.gouv.fr/affichTexte.do;jsessionid=B3D2B93BA4D5B3162AC56B149F71F4EC.tplgfr30s_3?cidTexte=JORFTEXT000000615627&dateTexte=20070424

Inter-ministerial Instruction on the Security of Activities of Vital Importance (No. 6600/ SGDSN/PSE/PS, 7 January 2014)	Normative instrument	Adopted by the General Secretariat for Defence and National Security, the Instruction contains extensive provisions for the implementation of France's institutional architecture on the protection of CI.	http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf
National Digital Security Strategy (2015)	Strategy and policy document	Sets out the strategic objectives and institutional approach to ensure the resilience of France against cyber-related threats, including threats against CII.	www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
Plan Vigipirate (2015)	Strategy and policy document	Plan Vigipirate envisages 300 measures covering 13 main areas of action such as transport, health and networks. On the basis of the assessment of the terrorist threat made by intelligence services, the General Secretariat for Defence and National Security issues guidelines determining the measures to be implemented by the entities concerned with vigilance, prevention and protection from terrorist threats. CI operators have to translate the measures of the plan into their own security plans.	www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf

Germany

National Strategy for Critical Infrastructure Protection (2009)	Strategy and policy document	Summarizes the Federal Administration's aims and objectives and its political and strategic approach. The Strategy is also the starting point for consolidating the results obtained to date and for further developing them in view of novel challenges.	www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1
Cybersecurity Strategy for Germany (2011)	Strategy and policy document	Provides the framework for cybersecurity over the next five years. Policy framework for the Government, together with industry and society, to ensure that the new technologies can be used safely and autonomously by adequately equipping security authorities, effectively protecting critical infrastructure and businesses, and making the digital sphere safer for the public	www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html

Japan

Basic Cybersecurity Act (2014 – amended in 2018)	Normative instrument	The Act seeks to ensure cybersecurity while guaranteeing the free flow of information. Owing to increased threats to cybersecurity, the Act was amended in 2018 with a view to preparing Japan to host the Tokyo 2020 Olympic and Paralympic Games. Specifically, a Cybersecurity Council has been established to enable various public and private entities to mutually cooperate in sharing cybersecurity information and discussing necessary countermeasures. Council members include representatives of national and local administrative bodies, infrastructure and cyber entities, educational and research institutions, and experts.	www.lexology.com/library/detail.aspx?g=5a1b0e44-9f84-432e-9bed-88523b2eb-b6a
Cybersecurity Strategy (2021)	Strategy and policy document	The Cybersecurity Strategy has been elaborated on the basis of the Basic Cybersecurity Act. CIP is addressed under one of the Strategy's key objectives: "Realizing a digital society in which people can live with a sense of safety and security". Under the subsection on "Advancing protection of critical infrastructure based on public-private collaboration", the Strategy makes reference to the 2017 Cybersecurity Policy for Critical Infrastructure Protection as the document on the basis of which the national Government undertakes its efforts to protect CI.	www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf
Cybersecurity Policy for Critical Infrastructure Protection (2017)	Strategy and policy document	The Policy represents the central document for the protection of CI in the country. It reflects three priorities: • Promotion of leading activities by CI operators (classification of CI operators in the light of interdependency) • Enhancement of information-sharing mechanisms in preparation for the Olympic and Paralympic Games • Promotion of incident readiness based on risk management	www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf

New Zealand

Draft Infrastructure Strategy (2021)	Strategy and policy document	Prepared by the Infrastructure Commission, the draft strategy describes the infrastructure issues that New Zealand is facing. These include long-term challenges, including security-related challenges, and also the opportunities posed by changing technology. It sets out several objectives and recommendations. Under the heading "Strengthening resilience to shocks and stresses", it identifies the need for a coordinated approach to CI, in particular: • Need to define and identify the country's CI • Best practice approach to manage cybersecurity threats • Need to include security of supply for essential infrastructure materials in risk management planning	www.tewaihanga.govt.nz/assets/Uploads/211012-Draft-New-Zealand-Infrastructure-Strategy.pdf
Civil Defence and Emergency Management Act (2002)	Normative instrument	The Act provides the legislative foundation for ensuring that national infrastructure is resilient by : • Setting out the requirements on and responsibilities of providers of lifeline infrastructure services, such as water and electricity, in the central Government, local government, and the private sector. • Identifying lifeline utilities as providers of CI services, and setting out requirements for coordinated preparedness and continuity of these lifeline services in the event of an emergency, and information disclosure requirements. • Requiring preparation of the National Disaster Resilience Strategy and the National Emergency Management Plan, which cascade in to coordinated local plans. Oversight of the Act is carried out by the National Emergency Management Agency.	www.legislation.govt.nz/act/public/2002/0033/51.0/DLM149789.html
National Security System Handbook (2016)	Strategy and policy document	The Handbook sets out the country's arrangements with regard to both the governance of national security and in response to a potential, emerging or actual national security crisis. It is divided into four sections: part 1: The national security system; part 2: National security governance structures; part 3: Response to a potential, emerging or actual event; part 4: Supporting annexes.	https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf
Cyber Security Strategy (2019)	Strategy and policy document	The Strategy identifies five areas for priority actions. It specifically mentions CI under the priority area on "responsive and resilient New Zealand". The Strategy is accompanied by an annual work programme outlining a range of steps to advance each priority area. The responsible minister releases a public annual report on progress under each area.	https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019

Poland

National Critical Infrastructure Protection Programme (2020)	Strategy and policy document	The programme defines: • National priorities, goals, requirements and standards to ensure the efficient functioning of CI • Competent government authorities responsible for the CIP systems • Criteria employed to distinguish objects, installations, devices and services included in the CIP systems	www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej
National Security Strategy (2020)	Strategy and policy document	The Strategy makes explicit reference to CIP under its pillar dealing with "Resilience of the State and consolidated civic defence". Section 2.8 envisages the implementation of a "model of critical infrastructure protection, ensuring its continued operation and uninterrupted provision of services". The Strategy also contains guidelines for CIP in specific sectors such as health, and economic and energy security.	www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Portugal

Counter Terrorism Strategy (2015)	Strategy and policy document	The National Strategy is based on five pillars: detect, prevent, protect, pursue and respond. Under the "Protect" pillar, the purpose includes to "strengthen the security of priority targets". The Strategy requests the development of an action plan for the protection and increase of the resilience of CI, both national and European.	PM of Portugal (request weblink)
National Cybersecurity Strategy (2019–2023)	Strategy and policy document	The Strategy is based on three strategic objectives, which translate into six axes of intervention. Specifically, axis 3 deals with the "Protection of cyberspace and infrastructure."	PM of Portugal (request weblink)

Republic of Moldova

Government Decision No. 701 on the approval of the Regulation on the protection of the critical infrastructure against terrorism (2018)	Normative instrument	The Regulation establishes the process for planning, organizing and implementing the antiterrorist protection measures of CI facilities by streamlining use of the available human, financial and material resources and taking into account specific vulnerabilities of CI. The Regulation was adopted in the framework of Act No. 120 on preventing and combating terrorism (see case study)	Information received from Permanent Mission of the Republic of Moldova to the United Nations

Russian Federation

Act on security of critical information infrastructure (2017)	Normative instrument	Sets out key principles, definitions and arrangements for ensuring the security of the CII of the Russian Federation. It outlines elements and principles of the State system for detecting, preventing and mitigating the impact of cyberattacks against information resources of the Russian Federation, a system which includes, among other elements, a national coordination centre for computer incidents (see https://cert.gov.ru/index.html). The Federal Act also identifies the criteria for defining certain information assets as critical infrastructure (such as social, economic, defence, political and environmental), and also the roles and responsibilities of State bodies, key requirements for security and protection of CII assets, rights and obligations of CII operators and owners, and the consequences of failure to comply with those requirements and obligations . Lastly, the Act sets up a national CII register and specifies principles of regular State oversight and threat assessments.	http://kremlin.ru/acts/bank/42128

Senegal

National Cybersecurity Strategy (2017)	Strategy and policy document	The Strategy includes the following elements: • Assessment of the strategic context of cybersecurity in Senegal, including current and future threats • Government vision for cybersecurity and strategic objectives to be attained • Institutional framework for its implementation Strategic Objective 2 deals specifically with strengthening infrastructure protection for CII and the State's information systems.	www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf

Singapore

Infrastructure Protection Act (2018)	Normative instrument	The Infrastructure Protection Act forms part of the country's counter-terrorism framework. The Act seeks to strengthen building security and enhance the protection of sensitive locations by ensuring that: • Major developments are designed with security in mind, notably through the incorporation of security measures upfront in building design. • Crowded places are protected against terrorist threats through the issuance of specific security measures (directives and orders). • Sensitive locations and their surroundings are protected through enhanced powers (such as enforcement against unauthorized photography). The Act is accompanied by a guide setting out its statutory requirements for the benefit of owners and persons responsible for special developments and special infrastructure designated under the Act.	https://sso.agc.gov.sg/Acts-Supp/41-2017/Published/20171031?DocDate=20171031&WholeDoc=1
Cybersecurity Act (2018)	Legislative instrument	The Act formalizes the country's policy in the field and articulates the protection of CII in specific cybersecurity concepts and protective measures (see the case study for further details)	www.csa.gov.sg/legislation/cybersecurity-act
Cybersecurity Strategy (2021)	Strategy/ Policy document	The Strategy comprises three strategic pillars. Under pillar 1 ("Build resilient infrastructure"), it is envisaged that the Cybersecurity Agency of Singapore cooperate closely with CII owners and sector leads to strengthen the cybersecurity of operational technology systems – such as industrial controls systems – where cyberattacks could pose physical and economic risks.	www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021

South Africa

Critical Infrastructure Protection Act (2019)	Normative instrument	The Act provides for: • Identification and declaration of infrastructure as CI • Factors to be taken into account to ensure transparent identification and declaration of CI • Measures for CI protection, safeguarding and resilience • Establishment of the Critical Infrastructure Council and its functions; • Functions of the National Commissioner under the Act • Designation and functions of inspectors • Powers and duties of persons in control of CI • Reporting obligations	www.gov.za/sites/default/files/gcis_document/201911/42866 28-11act8of2019criticalinfraprotectact.pdf

Spain

Act No. 8/2011 establishing measures for the protection on CI (2011)	Normative instrument	The Act coordinates the actions of all competent public bodies and promotes the collaboration and involvement of CI owners and operators. It transposes into national legislation the measures included in EC Directive 2008/114 / EC, in particular the identification and classification of European CI.	www.boe.es/buscar/act.php?id=BOE-A-2011-7630
Royal Decree 704/2011 approving Regulations for the protection of critical infrastructure (2011)	Normative instrument	The Decree implements the framework provisions set forth in Act No. 8/2011.	www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf
National Security Strategy (2021)	Normative instrument	Threats to CI are fully integrated into the document as threats to national security.	www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

Sweden

Protective Security Act (2019)	Normative instrument	The Act is designed to better protect information and activities of importance for the security of Sweden from cyberattacks (including those designed to steal sensitive data and those designed to disrupt critical operations).	https://rkrattsbaser.gov.se/sfst?bet=2018:585

Switzerland

National Strategy for CIP 2018–2022 (2017)	Strategy and policy document	Adopted by the Federal Office for Civil Protection, the Strategy updates the original strategy (issued in 2012) by setting forth higher objectives. The revised strategy is aimed at translating accomplished work into an institutionalized process, fixing it in legislation and supplementing it on an ad hoc basis.	www.babs.admin.ch/fr/aufgabenbabs/ski.html
National Strategy on Protection against Cyber Risks (2018-2022) (2018)	Strategy and policy document	Building on the previous strategy for the period 2012–2017, the revised strategy for 2018–2022 views CI operators as the main target group for its measures. The new strategy sets forth ten spheres of action addressing different aspects of cyber risks. A total of 29 measures are formulated within these spheres of action, based on a set of overarching principles such as "decentralized implementation", the "subsidiary role of the State" and a "risk-based approach".	www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html

United Kingdom of Great Britain and Northern Ireland

National Security Strategy (2015)	Strategy and policy document	The National Security Strategy is the overarching document outlining the pillars and objectives of the country's vision for the protection of CI.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
Sector Security and Resilience Plan 2018 (2019)	Strategy and policy document	Sector security and resilience plans are commissioned annually by the Cabinet Office for the lead government departments for the country's 13 critical sectors The plans describe: • Lead government departments' approaches to critical sector security and resilience • Their assessments of significant risks to their sectors • Their approach to security and resilience in the United Kingdom • Activities that they plan to undertake to mitigate and respond to those risks The full sector security and resilience plans are classified documents, as they contain sensitive security information. Each year, however, the Government publishes unclassified summaries to provide members of the public with information on activity being undertaken in each sector to improve security and resilience. Individual plans are classified, but the Cabinet Office summarizes each version into one overall sector resilience plan for CI.	www.gov.uk/government/collections/sector-resilience-plans
National Risk Register of Civil Emergencies (2017)	Strategy and policy document	Provides an overview of the key risks that have the potential to cause significant disruption in the United Kingdom over the next five years. The document illustrates the types of emergencies that might occur, what the Government and partners are doing to mitigate them, and how members of the public and small businesses can protect themselves. A number of sections directly address the protection of CI against terrorist acts.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

Ukraine

Critical Infrastructure Act (2021)	Normative instrument	The Act determines the legal and organizational basis for the creation and functioning of the national system for CIP and its legislative component in the domain of homeland security.	https://cis-legislation.com/document.fwx?rgn=136781

United States of America

National Infrastructure Protection Plan (2013)	Strategy and policy document	Outlines how government and private sector participants in the CI community work together to manage risks and achieve security and resilience outcomes. The 2013 Plan meets the requirements of Presidential Policy Directive 21, on CI security and resilience, signed in February 2013. It was developed through a collaborative process involving stakeholders from all 16 CI sectors, all 50 states, and from all levels of government and industry.	www.cisa.gov/national-infrastructure-protection-plan
Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013)	Normative instrument	The Directive instructs the Executive Branch to: • Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time • Understand the cascading consequences of infrastructure failures • Evaluate and mature the public-private partnership • Update the National Infrastructure Protection Plan • Develop comprehensive research and development plans	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)	Normative instrument	The Order instructs the Executive Branch to: • Develop a technology-neutral voluntary cybersecurity framework • Promote and incentivize the adoption of cybersecurity practices • Increase the volume and improve the timeliness and quality of cyberthreat information-sharing • Incorporate strong privacy and civil liberties protections into every initiative to secure critical infrastructure • Explore the use of existing regulation to promote cybersecurity	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Annex II
Security Council resolution 2341 (2017)

The Security Council,

Recalling its resolutions 1373 (2001), 1963 (2010), 2129 (2013) and 2322 (2016),

Reaffirming its primary responsibility for the maintenance of international peace and security, in accordance with the Charter of the United Nations,

Reaffirming its respect for the sovereignty, territorial integrity and political independence of all States in accordance with the United Nations Charter,

Reaffirming that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever, wherever and by whomsoever committed, and remaining determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level,

Reaffirming that terrorism poses a threat to international peace and security and that countering this threat requires collective efforts on national, regional and international levels on the basis of respect for international law, including international human rights law and international humanitarian law, and the Charter of the United Nations,

Reaffirming that terrorism should not be associated with any religion, nationality, civilization or ethnic group,

Stressing that the active participation and collaboration of all States and international, regional and sub-regional organizations is needed to impede, impair, isolate, and incapacitate the terrorist threat, and emphasizing the importance of implementing the United Nations Global Counter-Terrorism Strategy (GCTS), contained in General Assembly resolution 60/288 of 8 September 2006, and its subsequent reviews,

Reiterating the need to undertake measures to prevent and combat terrorism, in particular by denying terrorists access to the means to carry out their attacks, as outlined in Pillar II of the UN GCTS, including the need to strengthen efforts to improve security and protection of particularly vulnerable targets, such as infrastructure and public places, as well as resilience to terrorist attacks, in particular in the area of civil protection, while recognizing that States may require assistance to this effect,

Recognizing that each State determines what constitutes its critical infrastructure, and how to effectively protect it from terrorist attacks,

Recognizing a growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy of the concerned States as well as wellbeing and welfare of their population,

Recognizing that preparedness for terrorist attacks includes prevention, protection, mitigation, response and recovery with an emphasis on promoting security and resilience of critical infrastructure, including through public-private partnership as appropriate,

Recognizing that protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information-sharing; interdiction and disruption; screening, search and detection;

access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply chain integrity and security,

Acknowledging a vital role that informed, alert communities play in promoting awareness and understanding of the terrorist threat environment and specifically in identifying and reporting suspicious activities to law enforcement authorities, and the importance of expanding public awareness, engagement, and public-private partnership as appropriate, especially regarding potential terrorist threats and vulnerabilities through regular national and local dialogue, training, and outreach,

Noting increasing cross-border critical infrastructure interdependencies between countries, such as those used for, inter alia, generation, transmission and distribution of energy, air, land and maritime transport, banking and financial services, water supply, food distribution and public health,

Recognizing that, as a result of increasing interdependency among critical infrastructure sectors, some critical infrastructure is potentially susceptible to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns,

Expressing concern that terrorist attacks on critical infrastructure could significantly disrupt the functioning of government and private sector alike and cause knock-on effects beyond the infrastructure sector,

Underlining that effective critical infrastructure protection requires sectoral and cross-sectoral approaches to risk management and includes, inter alia, identifying and preparing for terrorist threats to reduce vulnerability of critical infrastructure, preventing and disrupting terrorist plots against critical infrastructure where possible, minimizing impacts and recovery time in the event of damage from a terrorist attack, identifying the cause of damage or the source of an attack, preserving evidence of an attack and holding those responsible for the attack accountable,

Recognizing in this regard that the effectiveness of critical infrastructure protection is greatly enhanced when based on an approach that considers all threats and hazards, notably terrorist attacks, and when combined with regular and substantive consultation and cooperation with operators of critical infrastructure and law enforcement and security officials charged with protection of critical infrastructure, and, when appropriate, with other stakeholders, including private sector owners,

Recognizing that the protection of critical infrastructure requires cooperation domestically and across borders with government authorities, foreign partners and private sector owners and operators of such infrastructure, as well as sharing their knowledge and experience in developing policies, good practices, and lessons learned,

Recalling that the resolution 1373 (2001) called upon Member States to find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups and to cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks,

Noting the work of relevant international, regional and sub-regional organizations, entities, forums and meetings on enhancing protection, security, and resilience of critical infrastructure,

Welcoming the continuing cooperation on counter-terrorism efforts between the Counter-Terrorism Committee (CTC) and International Criminal Police Organization (INTERPOL), the United Nations Office on Drugs and Crime, in particular on technical assistance and capacity-building, and all other United Nations bodies, and strongly encouraging their further engagement with the United Nations Counter-Terrorism Implementation Task Force (CTITF) to ensure overall coordination and coherence in the counter-terrorism efforts of the United Nations system,

1. *Encourages* all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure;

2. *Calls upon* Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management, and facilitating effective interaction of all stakeholders involved;

3. *Recalls* its decision in resolution 1373 (2001) that all States shall establish terrorist acts as serious criminal offences in domestic laws and regulations, and calls upon all Member States to ensure that they have established criminal responsibility for terrorist attacks intended to destroy or disable critical infrastructure, as well as the planning of, training for, and financing of and logistical support for such attacks;

4. *Calls upon* Member States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to or recovery from terrorist attacks planned or committed against critical infrastructure;

5. *Further calls upon* States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks;

6. *Urges* all States to ensure that all their relevant domestic departments, agencies and other entities work closely and effectively together on matters of protection of critical infrastructure against terrorist attacks;

7. *Encourages* the United Nations as well as those Member States and relevant regional and international organizations that have developed respective strategies to deal with protection of critical infrastructure to work with all States and relevant international, regional and sub-regional organizations and entities to identify and share good practices and measures to manage the risk of terrorist attacks on critical infrastructure;

8. *Affirms* that regional and bilateral economic cooperation and development initiatives play a vital role in achieving stability and prosperity, and in this regard calls upon all States to enhance their cooperation to protect critical infrastructure, including regional connectivity projects and related cross-border infrastructure, from terrorist attacks, as appropriate, through bilateral and multilateral means in information-sharing, risk assessment and joint law enforcement;

9. *Urges* States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, technical assistance, technology transfers and programmes, where it is needed to enable all States to achieve the goal of protection of critical infrastructure against terrorist attacks;

10. *Directs* the CTC, with the support of the Counter-Terrorism Committee Executive Directorate to continue as appropriate, within their respective mandates, to examine Member States efforts to protect critical infrastructure from terrorist attacks as relevant to the implementation of resolution 1373 (2001) with the aim of identifying good practices, gaps and vulnerabilities in this field;

11. *Encourages* in this regard the CTC, with the support of CTED, as well as the CTITF to continue working together to facilitate technical assistance and capacity building and to raise awareness in the field of protection of critical infrastructure from terrorist attacks, in particular by strengthening its dialogue with States and relevant international, regional and sub-regional organizations and working closely, including by sharing information, with relevant bilateral and multilateral technical assistance providers;

12. *Encourages* the CTITF Working Group on the Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security to continue its facilitation, and in cooperation with other specialized United Nations agencies, assistance on capacity-building for enhancing implementation of the measures upon request by Member States;

13. *Requests* the CTC to update the Council in twelve months on the implementation of this resolution;

14. *Decides* to remain seized of the matter.

Annex III
Addendum to the Madrid Guiding Principles (excerpts)

V. Protecting critical infrastructure, vulnerable or soft targets and tourism sites[2]

49. In its resolution 2341 (2017), the Security Council called upon States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, including by, inter alia, assessing and raising awareness of the relevant risks; taking preparedness measures, including implementing effective responses to such attacks and promoting better interoperability in security and consequence management; and facilitating effective interaction among all stakeholders involved.

50. In its resolution 2396 (2017), the Security Council stressed the need for States to develop, review or amend national risk and threat assessments to take into account soft targets, in order to develop appropriate contingency and emergency-response plans for terrorist attacks. It also called upon States to establish or strengthen national, regional and international partnerships with public and private stakeholders on the sharing of information and experience, in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against soft targets.

51. Critical infrastructure and soft targets are especially vulnerable and appealing as targets of terrorism. Vulnerabilities may be increased by the interconnectivity, interlinkage and interdependence of critical infrastructure. The appeal of soft targets to terrorists derives not only from their open format and limited security to facilitate access, but also from the potential to generate civilian casualties, chaos, publicity and economic impact.

52. Member States bear the primary responsibility for the protection of critical infrastructure and soft targets. Each State defines critical infrastructure and soft targets in accordance with its specific national context. There is a growing need, however, to increase cooperation between States and with private companies that own, operate and manage critical infrastructure and soft targets in order to address security needs, reduce vulnerabilities and share information on threats, vulnerabilities and measures, with a view to mitigating the risk of attack. Joint training sessions, communications networks, information-sharing (for example, on methodologies, best practices and exercises) and early warning mechanisms should be utilized and improved.

53. In order to maximize the potential to protect soft targets, public-private partnerships should be developed or strengthened at all levels of Government, including State, local and provincial. Member States should encourage and support such partnerships with companies that can contribute to all aspects of preparedness, namely protection from, mitigation of, response to and recovery from terrorist attacks, as well as the investigation of such incidents.

[2] See www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-on-foreign-terrorist-fighters.pdf.

54. Protection efforts entail multiple streams of effort, such as planning; public information and warning; operational coordination; intelligence and information-sharing; interdiction and disruption; screening, search and detection; access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply-chain integrity and security.

Guiding principle 50[3]

In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should:

(a) Identify, assess and raise awareness of the relevant risks and threats of terrorist attacks on critical infrastructure and soft targets;

(b) Determine what constitutes critical infrastructure and soft targets in the national context, on the basis of ongoing analysis of terrorist capabilities, intentions and past attacks, and regularly conduct risk assessments to keep pace with the evolving nature of the threat and the adversary, including by utilizing existing tools and guidance developed by international and regional organizations;[4]

(c) Develop, implement and practice strategies and action plans for reducing the risks of terrorist attacks on critical infrastructure and soft targets that integrate and leverage the capabilities of relevant public and private stakeholders;

(d) Take preparedness measures, including to ensure effective protection of and responses to such attacks, that are informed by comprehensive risk assessments;

(e) Promote better interoperability in security and crisis management;

(f) Promote risk-based and mutually reinforcing efforts to protect critical infrastructure and soft targets;

(g) Establish or strengthen mechanisms to share information, expertise (such as tools and guidance) and experience among public and private stakeholders to investigate and respond to terrorist attacks on such targets.[5]

Guiding principle 51[6]

In their further efforts to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider:

---

[3] The issue of protecting critical infrastructure, vulnerable or soft targets and tourism sites is not specifically addressed in the Madrid Guiding Principles. The guidance provided in guiding principles 50 and 51 are aimed at supporting the implementation of resolution 2341 (2017) on the protection of critical infrastructure, complemented by resolution 2396 (2017) and its provisions on protecting soft targets. They also build on the guidance provided in the following documents: Executive Directorate, Technical Guide; and Executive Directorate and Office of Counter-Terrorism, The Protection of Critical Infrastructure against Terrorist Attacks: Compendium of Good Practices (2018).

[4] In its Aviation Security Manual, ICAO provides guidance on how to apply the standards and recommended practices covered in annex 17 to the Convention on International Civil Aviation. Published in 2017, the tenth edition of the Manual features new and updated guidance material. Of particular interest with respect to critical-infrastructure protection are the materials relating to the security of landside areas of airports, staff and vehicle screenings and cyberthreats to critical aviation systems. See ICAO, Aviation Security Manual, 10th ed., document 8973; and ICAO, Annex 17 to the Convention on International Civil Aviation: Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference, 10th ed., International Standards and Recommended Practices (April 2017).

[5] Resolution 2396 (2017), paras. 27 and 28.

[6] The issue of protecting critical infrastructure, vulnerable or soft targets and tourism sites is not specifically addressed in the Madrid Guiding Principles. The guidance provided in guiding principles 50 and 51 are aimed at supporting the implementation of resolution 2341 (2017) on the protection of critical infrastructure, complemented by resolution 2396 (2017) and its provisions on protecting soft targets. They also build on the guidance provided in the following documents: Executive Directorate, Technical Guide; and Executive Directorate and Office of Counter-Terrorism, The Protection of Critical Infrastructure against Terrorist Attacks. See also resolution 2396 (2017), paras. 27 and 28.

(a) Updating contingency planning, such as guidance, exercises and training for law enforcement, other relevant ministries and industry actors, in order to keep pace with actual threats, refine strategies and ensure that stakeholders adapt to evolving threats;

(b) Putting in place national frameworks and mechanisms to support risk-based decision-making, information-sharing and public-private partnering for both Government and industry, including with a view to working together to determine priorities, and jointly developing relevant products and tools, such as general guidelines on surveillance or specific protective measures suggested for different types of facilities (for example, stadiums, hotels, malls or schools);

(c) Establishing processes for the exchange of risk assessments between Government, industry and the private sector, to promote and increase situational awareness and strengthen soft target security and resilience;

(d) Establishing processes for sharing relevant information with industry and private sector partners by, for example, issuing security clearances and increasing awareness;

(e) Promoting public-private partnerships by developing cooperation mechanisms, supporting business owners and operators and infrastructure managers and by sharing plans, policies and procedures, as appropriate;

(f) Assisting in the delivery of effective and targeted capacity development, training and other necessary resources, as well as technical assistance, where such delivery is needed to enable all States to develop appropriate capacity to implement contingency and response plans with regard to attacks against soft targets.

Annex IV
United Nations Global Counter-Terrorism Strategy (excerpts)

United Nations Global Counter-Terrorism Strategy (resolution 60/288, annex)

II–Measures to prevent and combat terrorism

We resolve to undertake the following measures to prevent and combat terrorism, in particular by denying terrorists access to the means to carry out their attacks, to their targets and to the desired impact of their attacks:

…

18. To step up all efforts to improve the security and protection of particularly vulnerable targets, such as infrastructure and public places … while recognizing that States may require assistance to this effect.

III. Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard

We recognize that capacity-building in all States is a core element of the global counter-terrorism effort, and resolve to undertake the following measures to develop State capacity to prevent and combat terrorism and enhance coordination and coherence within the United Nations system in promoting international cooperation in countering terrorism:

…

13. To encourage the United Nations to work with Member States and relevant international, regional and sub-regional organizations to identify and share best practices to prevent terrorist attacks on particularly vulnerable targets. We invite the International Criminal Police Organization to work with the Secretary-General so that he can submit proposals to this effect. We also recognize the importance of developing public-private partnerships in this area.

United Nations Global Counter-Terrorism Strategy: Seventh Review (General Assembly resolution 75/291)

The General Assembly,

…

Expressing concern over terrorist attacks against vulnerable targets, including critical infrastructure and public places ("soft" targets), recognizing that each Member State determines what constitutes its critical infrastructure or public places, assesses their level of vulnerability and identifies means to effectively protect them from terrorist attacks,

Expressing particular concern that terrorist attacks on critical infrastructure could significantly disrupt the functioning of government and the private sector alike and cause knock-on effects beyond the infrastructure sector, and therefore

underlining the growing importance of protecting critical infrastructure from terrorist attacks and of fostering comprehensive preparedness for such attacks, including through public-private partnership, as appropriate,

…

69. *Strongly condemns* all terrorist acts against critical infrastructure, including critical energy facilities, and against other vulnerable targets, and urges all Member States to take all necessary measures to prevent such attacks, as well as their possible radiological, radioactive and environmental consequences, and to counter such terrorist acts, including the prosecution of perpetrators;

…

71. *Calls upon* Member States to strengthen efforts to improve the security and protection of particularly vulnerable targets, including religious sites, educational institutions, tourist sites, urban centres, cultural and sport events, transport hubs, rallies, processions and convoys, as well as to enhance their resilience to terrorist attacks, in particular in the area of civil protection, and encourages Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management and facilitating the effective interaction of all stakeholders involved;

…

73. *Further calls* upon Member States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect against, mitigate, investigate, respond to and recover from terrorist attacks, and emphasizes the need for States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, and technical assistance, where it is needed, to enable all States to develop appropriate capacity to implement contingency and response plans with regard to attacks on critical infrastructure and public places (“soft” targets), and calls upon Global

Counter- Terrorism Coordination Compact entities to continue providing capacity-building support to requesting Member States for the resilience of vulnerable targets;

74. *Encourages* the Office of Counter-Terrorism and the Global Counter-Terrorism Coordination Compact entities to work closely with Member States and relevant international, regional and subregional organizations to identify and share best practices to prevent terrorist attacks on particularly vulnerable targets, including critical infrastructure and public places ("soft" targets), and recognizes the importance of developing public-private partnerships in this area;

Annex V
United Nations Global Counter-Terrorism Coordination Compact

The United Nations Global Counter-Terrorism Coordination Compact is the largest coordination framework across the three pillars of work of the United Nations: peace and security, sustainable development, human rights and humanitarian affairs. It aims to strengthen a common United Nations action approach to support Member States, at their request, in the balanced implementation of the United Nations Global Counter-Terrorism Strategy and other relevant United Nations resolutions and mandates. The Counter-Terrorism Compact was developed as part of the Secretary-General's reform of the United Nations counter-terrorism architecture, following the establishment of the , which serves as secretariat of the Counter-Terrorism Compact.

As of April 2022, the Counter-Terrorism Compact brings together 45 entities, as members or observers, including 41 United Nations entities, as well as INTERPOL, the World Customs Organization, the Inter-Parliamentary Union and the Financial Action Task Force. The following are members and observers of the Counter-Terrorism Compact:

Members:

1267 Committee Monitoring Team

1540 Committee Expert Group

Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO)
Counter-Terrorism Committee Executive Directorate
Department of Safety and Security
Department of Peace Operations
Department of Political and Peacebuilding Affairs
Department of Global Communications
Executive Office of the Secretary-General, Rule of Law Unit
International Civil Aviation Organization (ICAO)
International Criminal Police Organization (INTERPOL)
International Labour Organization (ILO)
International Maritime Organization (IMO)
Office of Counter-Terrorism
Office of the Special Adviser on Africa
Office for Disarmament Affairs

Office of Information and Communications Technology
Office of Legal Affairs
Office of the United Nations High Commissioner for Human Rights (OHCHR)
Office of the Secretary-General's Envoy on Youth
Office on Genocide Prevention and the Responsibility to Protect
Office of the Special Representative of the Secretary-General for Children and Armed Conflict
Office of the Special Representative of the Secretary-General on Sexual Violence in Conflict
Office of the Special Representative of the Secretary-General on Violence against Children
Organisation for the Prohibition of Chemical Weapons (OPCW)
Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism
United Nations Alliance of Civilizations
United Nations Development Programme (UNDP)
United Nations Educational, Scientific and Cultural Organization (UNESCO)
United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women)
United Nations Interregional Crime and Justice Research Institute (UNICRI)
United Nations Institute for Disarmament Research (UNIDIR)
United Nations Institute for Training and Research (UNITAR)
United Nations Office on Drugs and Crime
United Nations System Staff College
World Customs Organization (WCO)
World Health Organization (WHO)

Observers:

Department of Economic and Social Affairs
International Organization for Migration (IOM)
Inter-Parliamentary Union (IPU)
Office for the Coordination of Humanitarian Affairs
Office of the United Nations High Commissioner for Refugees (UNHCR)
United Nations Children's Fund (UNICEF)

22-25521

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

INTERPOL